



070-296

Planning, Implementing, and Maintaining
a Microsoft Windows Server 2003 Environment
for an MCSE Certified on Windows 2000

Version 9.0

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 test TestKing also provides:

* Online Testing. Check out an Online Testing Demo at <http://www.testking.com/index.cfm?pageid=724>

For this test TestKing plans to provide:

* Study Guide (Concepts and Labs)

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 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 family, including Windows Server 2003 Standard Edition, Windows Server 2003 Enterprise Edition, Windows Server 2003 Datacenter Edition, and Windows Server 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: 2

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 run Windows XP Professional. Client computers in the engineering department run Windows 2000 Professional. Client computers in the Sales department run either Windows NT Workstation 4.0 or Windows 98. All client computers access data files on the application server.

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.

Methods
Select from these

Server Message Block
(SMB) signing

IPSec encryption

Kerberos version 5
protocol

NTLMv2 authentication

Clients computers
Place here



Answer:

Methods
Select from these

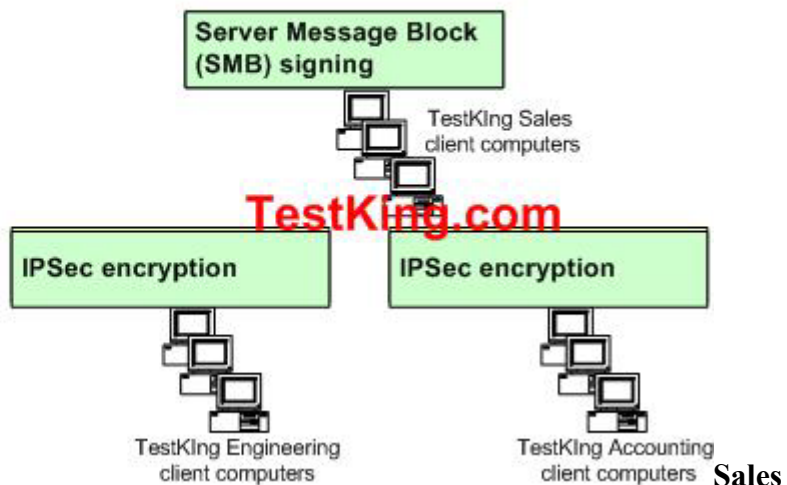
Server Message Block
(SMB) signing

IPSec encryption

Kerberos version 5
protocol

NTLMv2 authentication

Clients computers
Place here



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 and 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>

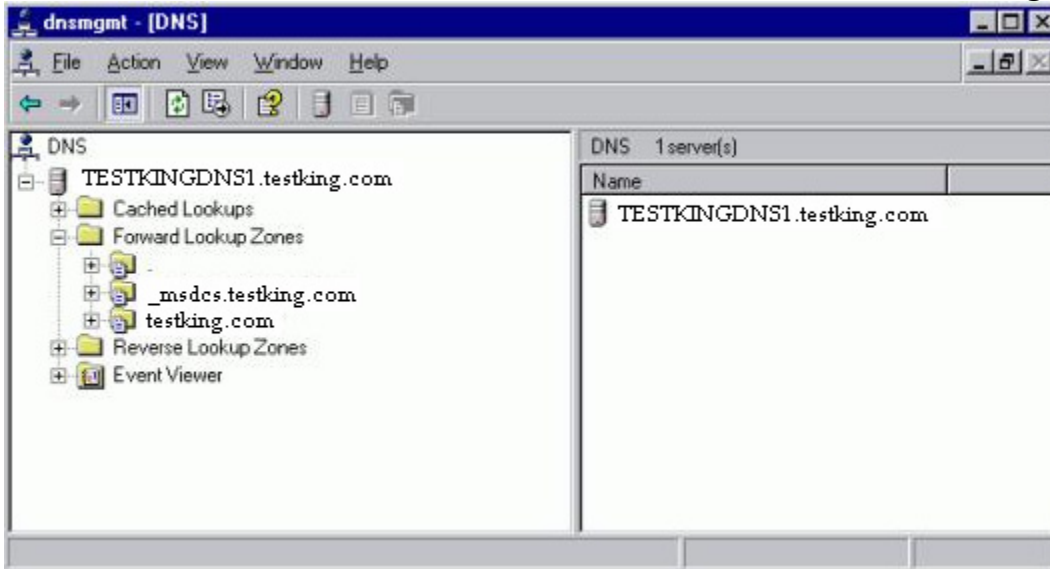
Microsoft L2TP/IPSec VPN Client is a free download that allows computers running Windows 98, Windows Millennium Edition (Me), or Windows NT® Workstation 4.0 to use Layer Two Tunneling Protocol (L2TP) connections with Internet Protocol security (IPSec).

- 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: 3

Leading the way in IT testing and certification tools, www.testking.com

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 zones 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: 4

You are the system engineer for TestKing. The network consists of a single Active Directory domain named testking.com. All servers run Windows Server 2003. The network is connected to the Internet by a dedicated T3 line.

TestKing enters into a partnership with another company for a new project. The partner company's network consists of a single Active Directory forest that contains two domains. All servers in the network run Windows 2003 Server. The partner network is also connected to the Internet by a dedicated T3 line.

The partner network is accessible by a VPN connection that was established between the two networks. The VPN connection was tested and was verified to provide a functional connection between the two networks.

Users from both companies need to connect to resources located on another network. A forest trust relationship exists between the two companies' forests to allow user access to resources. Users in your company report that they can access resources on the partner network, but that it can take up to several minutes for the connection to be established. This problem is most pronounced during the morning.

You verify that there is sufficient available bandwidth on the connection between the two networks to provide access. You also verify that both network's routing tables are configured correctly to route requests to the appropriate destinations. When you attempt to connect to a server in the partner network by host name by using the ping command, the connection times out. However, when you attempt to connect to the server a second time by IP address by using the ping command, you receive a response within a few seconds.

You need to improve the performance of the network connection between the two networks.

What should you do?

- A. Add the partner network's domain names and DNS server addresses to the forwarders list on your DNS servers.
- B. Update the root hints list on your DNS servers to include the host names and IP addresses of the partner network's DNS servers.
- C. Disable recursion on the DNS servers in both companies' networks.
- D. Add the partner network's DNS server addresses to the **006 DNS Servers** scope option in your DHCP scope.

Answer: A

Explanation: It is taking a long time to locate resources on the other network. This is because name resolution requests are being passed to the internet root servers, then down through the internet DNS hierarchy before the request finally reaches the appropriate DNS server. We can speed up this process by using conditional forwarding. This would enable resolution requests for resources in the partner network to be forwarded directly to the partner's DNS server.

Conditional forwarders

A conditional forwarder is a DNS server on a network that is used to forward DNS queries according to the DNS domain name in the query. For example, a DNS server can be configured to forward all the queries it receives for names ending with widgets.example.com to the IP address of a specific DNS server or to the IP addresses of multiple DNS servers.

Incorrect Answers:

B: The root hints are used to locate internet root DNS servers.

C: This won't help. It would mean that the internal DNS servers wouldn't forward external resolution requests to other DNS servers such as the root servers.

D: The partner network's DNS servers would never be used unless the local DNS server failed.

QUESTION NO: 5

You are the network administrator for Contoso, Ltd. The network consists of a single Active Directory forest. The functional level of the forest is Windows Server 2003. The forest root domain is contoso.com.

Contoso, Ltd., recently merged with another company named TestKing, whose network consists of a single Active Directory forest. The functional level of the TestKing forest is Windows Server 2003. The forest root domain for TestKing is testking.com. You need to create a forest trust relationship between the two forests. Each company has dedicated connections to the Internet.

You need to configure DNS to support the forest trust relationship. You want to maintain Internet name resolution capability for each company's network.

What should you do?

- A. Configure the contoso.com DNS servers to forward to the testking.com DNS servers.
Configure the testking.com DNS servers to forward to the contoso.com DNS servers.
- B. Configure conditional forwarding of testking.com on the contoso.com DNS servers to the testking.com DNS servers.
Configure conditional forwarding of contoso.com on the testking.com DNS servers to the contoso.com DNS servers.
- C. Configure a standard primary zone for testking.com on one of the contoso.com DNS servers.
Configure a standard primary zone for contoso.com on one of the testking.com DNS servers.
- D. Configure an Active Directory-integrated zone for testking.com on the contoso.com DNS servers.
Configure an Active Directory-integrated zone for contoso.com on the testking.com DNS servers.

Answer: B

Explanation: This is a typical scenario for conditional forwarding

Conditional forwarders. A conditional forwarder is a DNS server on a network that is used to forward DNS queries according to the DNS domain name in the query. For example, a DNS server can be configured to forward all the queries it receives for names ending with widgets.example.com to the IP address of a specific DNS server or to the IP addresses of multiple DNS servers.

Incorrect Answers:

- A: We don't want ALL resolution requests to be forwarded to the other DNS servers.
- C: We can't host primary zones on multiple servers.
- D: We can't host AD integrates zones on DNS servers in a different forest.

QUESTION NO: 6

You are the network administrator for TestKing. The network consists of a single Active Directory forest that contains three domains. Each domain contains domain controllers that run Windows 2000 Server and domain controllers that run Windows Server 2003. The DNS Server service is installed on all domain controllers. All client computers run Windows XP Professional.

You need to add an additional DNS zone that is hosted on at least one DNS server on each domain. You want to configure the zone to allow secure updates only.

What should you do?

- A. Configure the new zone on DNS servers in the root domain.
Configure stub zones that refer to DNS servers in another two domains.
- B. Configure the new zone as a primary zone on one DNS server.
Configure other DNS servers in the three domains as secondary servers for this zone.
Enable the DNS Security Extensions (DNSSEC) protocol.
- C. Configure the new zone as an Active Directory-integrated zone on DNS servers in the three domains.
Store the zone data in the DNS directory partition named DomainDNSZones.
- D. Configure the new zone as an Active Directory-integrated zone on DNS servers in the three domains.
Store the zone data in the DNS directory partition named ForestDNSZones.

Answer: D

Explanation: To enable secure updates, we need an Active Directory integrated zone. To replicate to the DNS servers in the other domains, the zone must be installed on a Windows 2003 domain controller in each domain. During the configuration of the zone, you can select the option to replicate the zone information to all domain controllers in the forest; this will store the zone data in the DNS directory partition named ForestDNSZones.

Incorrect Answers:

A: We need Active Directory integrated zones, not stub zones.

B: Secondary zones are not writeable and so cannot accept updates.

C: If we store the zone data in the DNS directory partition named DomainDNSZones, it will only be replicated in a single domain, not the entire forest.

QUESTION NO: 7

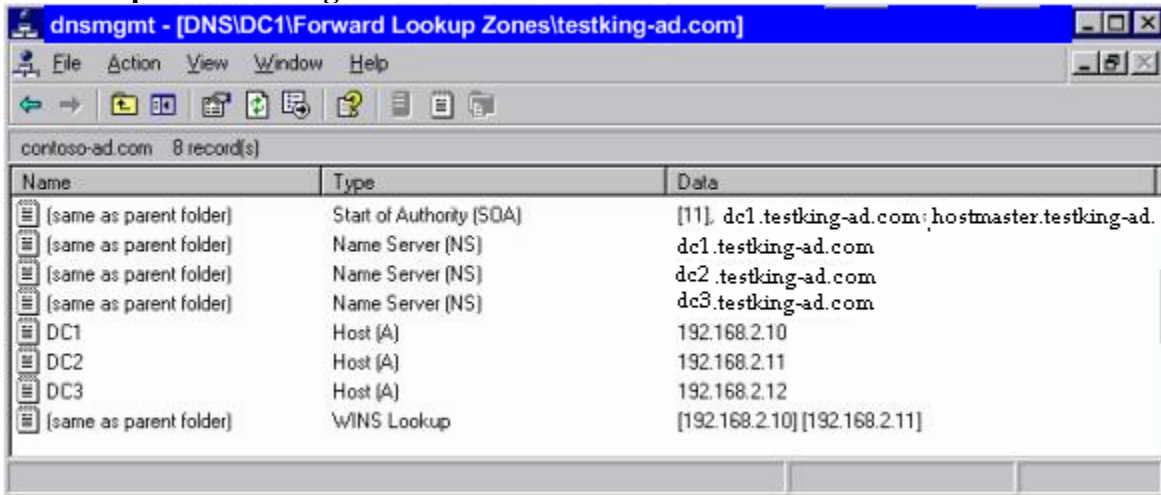
You are the systems engineer for TestKing GmbH. The network consists of three Windows NT 4.0 domains in a master domain model configuration. The servers on the network run either Windows NT Server 4.0 or Windows 2000 Server. All domain controllers run Windows NT Server 4.0.

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: 8

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 accessed 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: 9

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 simplify the task.

QUESTION NO: 10

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

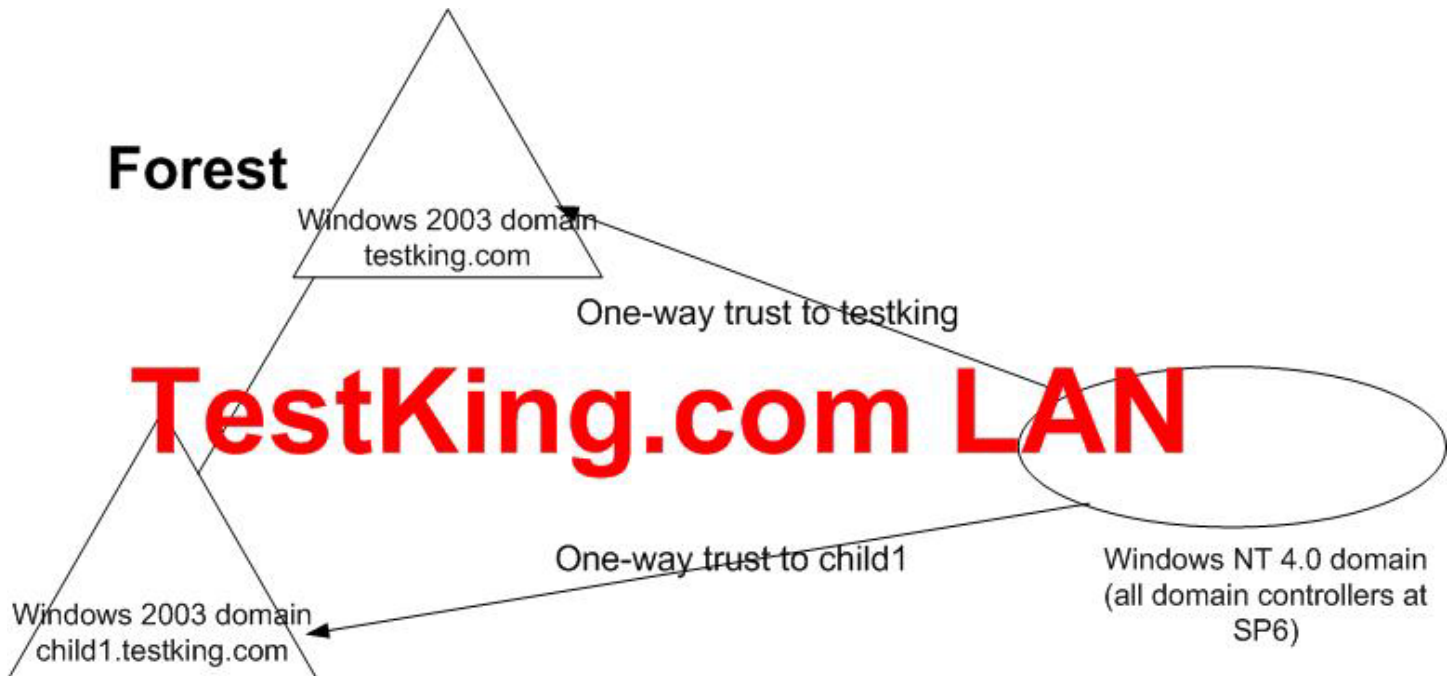
Explanation: Short for Secure Sockets Layer, a protocol developed by Netscape for transmitting private documents via the Internet. SSL works by using a private key to encrypt data that's transferred over the SSL connection. Both Netscape Navigator and Internet Explorer support SSL, and many Web sites 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: 11

You are a network administrator for TestKing Inc. The network consists of a single Active Directory forest as shown in the exhibit.



Your company'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: 12

You are a network administrator for Testking. The network consists of a single Active Directory domain named testking.com. The domain name is testking.com. The network contains three Windows Server 2003 domain controllers.

You are creating the recovery plan for the company. According to the existing backup plan, domain controllers are backed up by using normal backups each night. The normal backups of the domain controllers include the system state of each domain controller.

Your recovery plan must incorporate the following organization requirements:

- Active Directory objects that are accidentally or maliciously deleted must be recoverable.
- Active Directory must be restored to its most recent state of quickly as possible.
- Active Directory database replication must be minimized.

You need to create a plan to restore a deleted organizational unit (OU).

Which two actions should you include in your plan? (Each correct answer presents part of the solution. Choose two)

- A. Restart a domain controller in Directory Services Restore Mode.
- B. Restart a domain controller in Safe Mode.
- C. Use the Ntdsutil to perform an authoritative restore operation of the Active Directory database.
- D. Restore the system state by using the **Always replace the file on my computer** option.
- E. Use the Ntdsutil utility to perform an authoritative restore operation of the appropriate subtree.

Answer: A, E

Explanation: If an OU gets deleted from the Active Directory, we can restore it from a backup of the system state data. Directory Services Restore Mode is a sort of safe mode in which we can boot a domain controller without loading the Active Directory. This will enable us to restore all or part of the Active Directory database. To ensure that the deleted OU isn't deleted again by replication from another domain controller, we must use the Ntdsutil utility to mark the restored subtree as authoritative.

Incorrect Answers:

B: To restore part of the Active Directory, we must start a domain controller in Directory Services Restore Mode, not safe mode.

C: We don't need to restore the entire Active Directory database; we can just restore part of it.

D: This will overwrite the existing Active Directory database.

QUESTION NO: 13

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 seccedit 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: 14

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 Cert Administrators group to the Cert Publishers 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: 15

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 Hisecws.inf templates.

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 an 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: 16

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: 17

You are the security analyst 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 perimeter network contains an application server, which is accessible to external users.

You view the logs on your intrusion-detection system (IDS) and on the router and discover that very large numbers of TCP SYN packets are being sent to the application server. The application server is responding with SYN-ACK packets to several different IP addresses, but is not receiving ACK responses. You note that all incoming SYN packets appear to be originating from IP addresses located within the perimeter network's subnet address range. No computers in your perimeter network are configured with these IP addresses. The router logs show that these packets are originating from locations on the Internet.

You need to prevent this type of attack from occurring until a patch is made available from the application vendor. Because of budget constraints, you cannot add any new hardware or software to the network. Your solution cannot adversely affect legitimate traffic to the application server.

What should you do?

- Relocate the application server to the company intranet.
Configure the firewall to allow inbound and outbound traffic on the ports and protocols used by the application.
- Configure network ingress filters on the router to drop packets that have local addresses but that appear to originate from outside the company network.
- Create access control lists (ACLs) and packet filters on the router to allow perimeter network access to only authorized users and to drop all other packets originating from the Internet.
- Configure the IDS on the perimeter network with a response rule that sends a remote shutdown command to the application server in the event of a similar denial-of-service attack.

Answer: B

Explanation: This type of attack is known as a Denial of Service Attack.

Dropping spoofed packets

In an ideal world, each router would be configured with ingress filters that would drop packets arriving from "internal" networks whose source address was not a member of the set of network addresses that this router serves. The majority of routers could be so configured. Backbone routers and edge routers for complex topologies probably could not be configured with such filters. These ingress filters should be required as part of a "good neighbor policy." **Ingress filters would not totally eliminate denial of service attacks but could greatly reduce such attacks.** An attacker could still spoof an address within a local subnet, but that would permit backtracking the packets to the source subnet. Cisco's unicast reverse path forwarding also can be used to block spoofed packets at edge routers. **Routers that implement ingress filtering will not forward the packets sent by a mobile host in a foreign network.**

QUESTION NO: 18

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: C

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: 19

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 child1.testking.com and child2.testking.com. The child1.testking.com domain contains a member server named TestKingSrvC. You configure TestKingSrvC 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 child1.testking.com and the child2.testking.com domains to enroll for user certificates.

You discover that the certificates for user accounts in the child1.testking.com domain are being published to Active Directory, but the certificates for user accounts in the child2.testking.com domain are not.

You want certificates issued by TestKingSrvC to child2.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.

- B. Configure user certificate autoenrollment for all domain user accounts in the child2.testking.com domain.
- C. Add TestKingSrvC to the Cert Publisher group in the testking.com domain.
- D. Add TestKingSrvC to the Cert Publisher group in the child2.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: 20

You are a 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. All domain controllers run Windows Server 2003. The domain controllers are configured as shown in the following table.

Server name	Server role
TestKingSrvA	Global catalog server, schema master, domain naming master
TestKingSrvB	Domain controller, infrastructure master, PDC emulator
TestKingSrvC	Domain controller
TestKingSrvD	Global catalog server, relative ID (RID) master

You plan to take TestKingSrvD offline for maintenance. Another network administrator plans to add 1,250 new user accounts while TestKingSrvD is offline.

You need to ensure that the network administrator can add the user accounts while TestKingSrvD is offline. You also need to ensure that there is no disruption of user account creation after TestKingSrvD is brought back online.

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

- A. Connect to TestKingA by using the Ntdsutil utility.
- B. Connect to TestKingSrvD by using the Ntdsutil utility.
- C. Remove the global catalog server role from TestKingSrvD.
- D. Add the global catalog server role to TestKingSrvD.
- E. Transfer the RID master role.

Answer: A, E

Explanation: The RID master is assigned to allocate unique sequences of relative IDs to each domain controller in its domain. As the domain controllers use the IDs allocated, they contact the RID master and are allocated additional sequences as needed. At any time, the RID master role can be assigned to only one domain controller in each domain. The Relative ID is part of a security ID (SID) that uniquely identifies an account or group within a domain. We will be creating 1250 new user accounts so the domain controller will need to contact the RID master to obtain more RIDs.

We can transfer the RID master role using the ntdsutil utility.

Incorrect Answers:

B: We need to connect to the computer we will be transferring the role to, not from.

C: We have a Global Catalog on TestKingSrvA. We don't need another one.

D: TestKingSrvD is already a global catalog server.

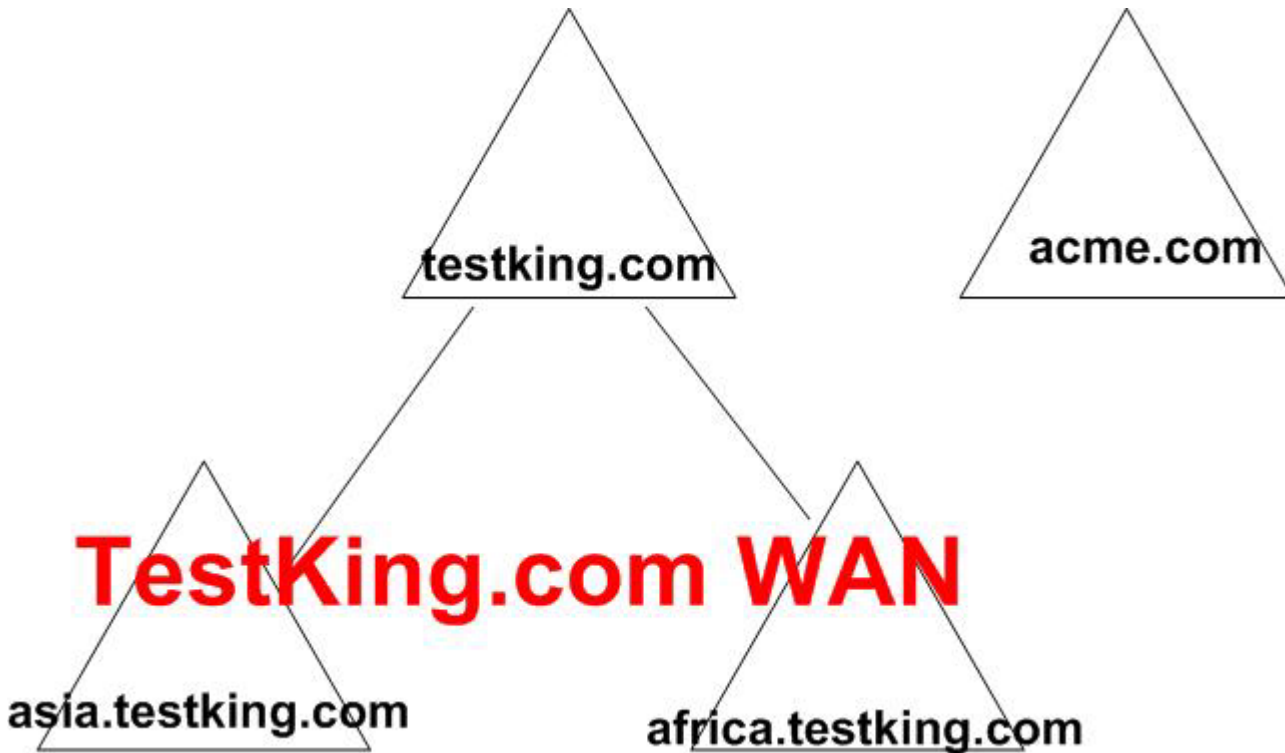
Reference:

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/proddocs/entserver/sag_adTransRIDMaster.asp

QUESTION NO: 21

You are the network administrator for TestKing. The network consists of a single Active Directory forest that contains three domains. The functional level of all three domains is Windows 2000 native.

Your company is merging with a company named Acme. The Acme., network consists of a single Active Directory forest that contains one domain named acme.com. The functional level of the domain is Windows 2000 native. The forests of both companies are shown in the exhibit.



You need to allow users in each forest to fully access resources in the domains of the other forest. In addition, users must be able to log on between domains by using Kerberos authentication. You need to ensure that users can continue to access all resources by using their existing user accounts.

What should you do?

- A. Demote the Windows 2000 domain controllers in the acme.com domain to become member servers. Promote these servers into the testking.com domain.
- B. Demote the Windows 2000 domain controllers in the acme.com domain to become member servers. Upgrade these servers to Windows Server 2003. Promote the upgraded computers to become domain controllers for a new domain tree in the TestKing forest.
- C. Upgrade the Windows 2000 domain controllers in the acme.com domain to Windows Server 2003. Create external trust relationships between the root domains of each forest.
- D. Upgrade all domain controllers in both forests to Windows Server 2003. Raise the functional level of both forests to Windows Server 2003. Create a forest trust relationship between the root domains of each forest.

Answer: D

Explanation: To enable users in each forest to fully access resources in the domains of the other forest and log on to either domain with Kerberos authentication, we need to create a forest trust between the two forests. To

create a forest trust, the forests must be in Windows 2003 domain functional level. This requires that all domain controllers in each domain are running Windows server 2003.

Incorrect Answers:

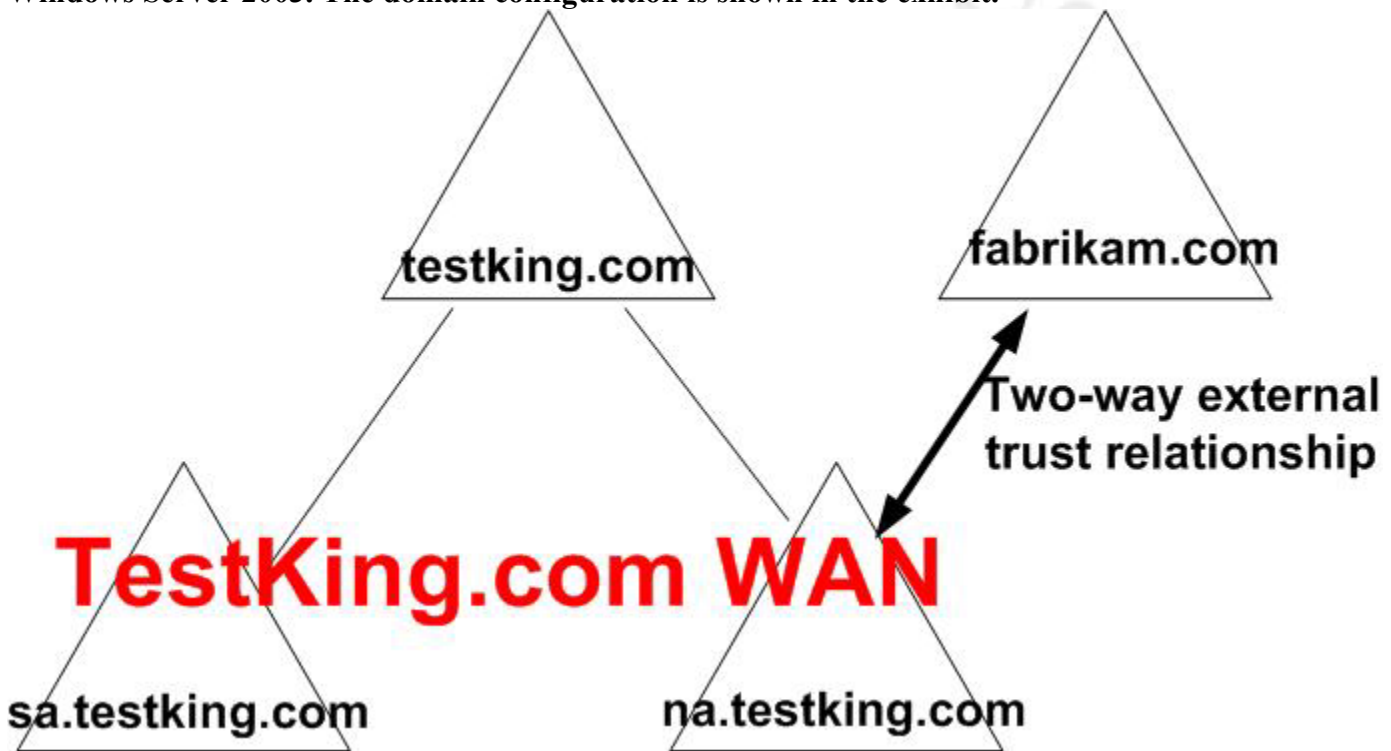
A: This will decommission the acme.com domain/forest. This isn't a requirement.

B: This will decommission the acme.com forest. This isn't a requirement.

C: We need a forest trust to enable Kerberos authentication across the trust link.

QUESTION NO: 22

You are the network administrator for your company. The company consists of two subsidiaries named TestKing., and Fabrikam, Inc. The network consists of two Active Directory forests. All servers run Windows Server 2003. The domain configuration is shown in the exhibit.



The North American department in the company is renamed to Northwind Traders. You rename the NA.testking.com domain to northwindtraders.com. You change the NetBIOS name for the domain to northwindtraders. The northwindtraders.com domain is a second tree in the testking.com forest.

After the domain is renamed, users in the northwindtraders.com domain report that they cannot access any shared resources in the fabrikam.com domain. In addition, users in the fabrikam.com domain report that they cannot access shared resources in the northwindtraders.com domain.

You need to re-enable the sharing of resources between the northwindtraders.com domain and the fabrikam.com domain.

What should you do?

- A. Change the NetBIOS name for the northwindtraders.com domain to NA.
- B. Delete and re-create the two one-way trust relationships between the northwindtraders.com domain and the fabrikam.com domain.
- C. Configure conditional forwarding on the DNS server in the fabrikam.com domain to forward requests for the northwindtraders.com domain to the DNS servers in the testking.com domain.
- D. Reset the computer account passwords on all of the domain controllers in the northwindtraders.com domain.

Answer: B

Explanation: After renaming the domain, the external trust relationships will need to be recreated.

Creating Necessary Shortcut Trust Relationships

You can reposition any domain within the domain tree hierarchy of a forest, with the exception of the forest-root domain. Remember that although the forest root domain can be renamed (its DNS and NetBIOS names can change), it cannot be repositioned in such a way that you designate a different domain to become the new forest root domain. If your domain rename operation involves restructuring the forest through repositioning of the domains in the domain tree hierarchy as opposed to simply changing the names of the domains in-place, you first need to create the necessary shortcut trust relationships between domains such that the new forest structure has two-way transitive trust paths between every pair of domains in the target forest, just as your current forest does.

Forest restructuring

Using domain rename, you can also restructure the hierarchy of domains in your forest so that a domain residing in one domain tree

In DNS, the inverted hierarchical tree structure that is used to index domain names. Domain trees are similar in purpose and concept to the directory trees used by computer filing systems for disk storage. For example, when numerous files are stored on disk, directories can be used to organize the files into logical collections. When a domain tree has one or more branches, each branch can organize domain names used in the namespace into logical collections.

In Active Directory, a hierarchical structure of one or more domains, connected by transitive, bidirectional trusts, that forms a contiguous namespace. Multiple domain trees can belong to the same forest.

Domains can be moved to another domain tree. Restructuring a forest allows you to move a domain anywhere within the forest in which it resides (except the forest root domain). This includes the ability to move a domain so that it becomes the root of its own domain tree.

You can use the domain rename utility (Rendom.exe) to rename or restructure a domain. The Rendom.exe utility can be found in the Valueadd\Msft\Mgmt\Domren directory on the operating system installation CD. A

domain rename will affect every domain controller in your forest and is a multistep process that requires a detailed understanding of the operation.

Renaming a domain controller requires that you first provide a FQDN as a new computer name for the domain controller. All of the computer accounts for the domain controller must contain the updated SPN attribute and all the authoritative DNS servers for the domain name must contain the host (A) resource record for the new computer name. Both the old and new computer names are maintained until you remove the old computer name. This ensures that there will be no interruption in the ability of clients to locate or authenticate to the renamed domain controller, except when the domain controller is restarted

Renaming domain controllers

The SPN value of the computer account must be replicated to all domain controllers for the domain and the DNS resource records for the new computer name must be distributed to all the authoritative DNS servers for the domain name. If the updates and registrations have not occurred prior to removing the old computer name, then some clients may be unable to locate this computer using the new or old name.

References:

Server Help
Window Server 2003
MS White paper Step-by-Step Guide to Implementing Domain Rename

QUESTION NO: 23

You are the network administrator for TestKing. The company needs to implement a Web application that uses two Microsoft SQL Server 2000 database instances.

You expect the size of each database instance to be between 200 GB and 300 GB at any given time. Several tables in each database contain data that is updated once every few seconds, on average. You estimate that each database instance requires 7 GB of memory, and that each instance requires 70 percent usage of four CPUs, on average.

Using two servers TestKingSQL1 and TestKingSQL2, you need to plan the minimum highly available server infrastructure for the databases that meets the requirements. You also want to minimize the costs and administrative effort required to maintain the infrastructure.

What should you do?

To answer, drag the appropriate configuration settings to the Cluster Configuration.

	Select from these	Place here
Operating systems:	Windows Server 2003, Web Edition	Put Operating system here
Clustering Technologies:	Cluster service server cluster	Put Clustering Technology here
Number of CPUs:	4 CPUs per cluster node	Put Number of CPUs here
Amount of RAM:	8 GB of RAM per cluster node	Put Amount of RAM here

Answer:

	Select from these	Place here
Operating systems:	Windows Server 2003, Web Edition	Windows Server 2003 Enterprise Edition
Clustering Technologies:	Cluster service server cluster	Cluster service server cluster
Number of CPUs:	4 CPUs per cluster node	8 CPUs per cluster node
Amount of RAM:	8 GB of RAM per cluster node	16 GB of RAM per cluster node

Explanation:

We are running two different databases so we need a Cluster Service Cluster rather than a Network Load Balancing cluster (We can only use NLB if the two servers are hosting identical content). For a Cluster Service Cluster, we need to use Windows Server 2003 Enterprise Edition.

We need to ensure that the database will still run if one of the cluster nodes fails. Therefore each cluster node will need enough resources to run both databases. Each database requires four CPUs, so each cluster node must have 8 CPUs in order to run both databases in the event of a cluster node failure. Each database requires 7 GB of RAM so each cluster node must have at least 14 GB of RAM in order to run both databases in the event of a cluster node failure (our only option above 14GB of RAM is to put 16GB of RAM in each cluster node).

QUESTION NO: 24

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 secure site and a main office site, as shown in the exhibit.



All domain controllers are configured as shown in the following table.

Drive	Contents
C	Boot partition, system partition, Active Directory database log files
D	Active Directory database
E	Files and folders

The motherboard on TESTKING2 fails and TESTKING2 is taken offline. One week later, an administrator connects to TESTKING3 and seizes the schema master role.

You need to access files on drive E on TESTKING2. You replace the motherboard on TESTKING2 and bring TESTKING2 online on an isolated subnet.

You need to be able to bring TESTKING2 back into the secure site as quickly as possible in order to access the files.

What should you do?

- A. Perform a full format of drive D on TESTKING2.
Transfer the schema master role to a domain controller in the MainOffice site.
Remove references to TESTKING2 from Active Directory by using the Ntdsutil utility and the ADSIEdit utility on TESTKING1.
- B. Perform a full format of drive C on TESTKING2.
Reinstall the operating system on TESTKING2.
Remove references to TESTKING2 from Active Directory by using the Ntdsutil utility and the ADSIEdit utility on TESTKING1.
- C. Perform a full format of drive E on TESTKING2.
Run the **deprmo** command on TESTKING2.
Transfer the schema master role to a domain controller in the MainOffice site.
Join TESTKING2 to the domain.
- D. Perform a full format of drive C on TESTKING2.
Transfer the schema master role to a domain controller in the MainOffice site.

Remove references to TESTKING2 from Active Directory by using the Ntdsutil utility and the ADSIEDut utility on TESTKING1.

Answer: B

Explanation: We have seized the schema master role from Testking2 on Testking3. Therefore, we don't want to bring Testking2 back online with its old schema master role. Having two schema masters will cause problems in the forest. To bring Testking2 back online, we should format the C drive and reinstall the operating system. We should also 'clean' the Active Directory database by removing references to TESTKING2 from Active Directory by using the Ntdsutil utility and the ADSIEdit utility on another domain controller.

Incorrect Answers:

A: We need to reinstall the operating system, so we should format drive C, not drive D.

C: Formatting drive E will erase the data we want to access.

D: The schema master role has already been transferred. We need to reinstall the operating system after formatting drive C.

QUESTION NO: 25

You are a network administrator for TestKing. Your network consists of a single Active Directory domain named testking.com. All servers run Windows Server 2003.

A help desk user reports that a user object was accidentally deleted and the user can no longer log on to the domain and access resources. You confirm that the user object was included in the most recent backup.

You need to enable the user to log on to the domain. You must ensure that the user retains access to resources.

What should you do?

- A. Install a new domain controller.
Install Active Directory from media by using the most recent backup.
Manually initiate replication.
- B. Decrease the garbage collection interval.
Perform a nonauthoritative restoration of Active Directory by using the most recent backup.
- C. Perform a nonauthoritative restoration of Active Directory by using the most recent backup.
Authoritatively restore the user object that was deleted.
- D. Re-create a user object that has the same user principal name (UPN) as the user object that was deleted.
Authoritatively restore this user object.

Answer: C

Explanation: If you inadvertently delete or modify objects stored in the Active Directory directory service, and those objects are replicated or distributed to other servers, you will need to authoritatively restore those objects so they are replicated or distributed to the other servers. If you do not authoritatively restore the objects, they will never get replicated or distributed to your other servers because they will appear to be older than the objects currently on your other servers. Using the Ntdsutil utility to mark objects for authoritative restore ensures that the data you want to restore gets replicated or distributed throughout your organization. On the other hand, if your system disk has failed or the Active Directory database is corrupted, then you can simply restore the data nonauthoritatively without using the Ntdsutil utility.

Active Directory gives network users access to permitted resources anywhere on the network using a single logon process. It provides network administrators with an intuitive, hierarchical view of the network and a single point of administration for all network objects. Active directory service data can be restored using one of three restore methods:

- **Primary restore**
- **Normal (nonauthoritative) restore**
- **Authoritative restore**

In Backup, a type of restore operation performed on an Active Directory domain controller in which the objects in the restored directory are treated as authoritative, replacing (through replication) all existing copies of those objects.

We need to restore the Active Directory database non-authoritatively, then from the restored copy of the database, we need to authoritatively restore the user object.

Incorrect Answers:

A: It isn't necessary to install a new domain controller.

B: We need to authoritatively restore the user object, otherwise AD replication will delete the user object again.

D: Creating a new user account won't work because the new user account will have a different SID from the deleted account.

QUESTION NO: 26

You are the network administrator for Fabrikam, Inc. The network consists of a single Active Directory domain that contains one domain controller. All servers run Windows Server 2003. All client computers run Windows XP Professional. The company uses Group Policy objects (GPOs) to configure user and computer settings.

A new user named Dr. King reports that his Windows desktop is different from others in the company and that he does not have access to the same applications as other users. You discover that none of the user settings from any GPOs are in effect in Dr. King's computer after Dr. King logs on. You instruct Dr.

King to run the gpresult command, and he reports that he receives the following error message: “INFO: The group policy object does not exist”.

You run the gpoutil command on the domain controller and receive the output shown in the exhibit.

```

C:\Documents and Settings\Administrator.FABRIKAM-DC>gpoutil /gpo:E0E11
Validating DCs...
Available DCs:
FABRIKAM-DC.fabrikam.com
Searching for policies...
Found 1 policies
=====
Policy <E0E11C04-370D-470A-B301-C1EC92FD6086>
Error: Cannot access \\FABRIKAM-DC.fabrikam.com\\sysvol\\fabrikam.com\\policies\\<E0E11C04-370D-470A-B301-C1EC92FD6086>, error 2
Details:
=====
DC: FABRIKAM-DC.fabrikam.com
Friendly name: User Settings
Created: 4/23/2003 6:52:12 AM
Changed: 4/23/2003 7:04:24 AM
DS version: 2(user) 0(machine)
Sysvol version: not found
Flags: 0
User extensions: [(35378EAC-683F-11D2-A89A-00C04FBBCEFA2)<0F6B957E-509E-11D1-A7CC-0000F87571E3>]
Machine extensions: not found
Functionality version: 2
=====
Errors found
C:\Documents and Settings\Administrator.FABRIKAM-DC>

```

You need to ensure that Group Policy settings can be applied correctly.

What should you do?

- A. Run the **gpupdate /force** command on the domain controller.
- B. Run the **gpupdate /force** command on Dr. King's computer.
- C. Restore the system state on the domain controller from a valid backup.
- D. Restore the backup state on Dr. King's computer from a valid backup.

Answer: C

Explanation: We can see from the exhibit that there is a problem with the group policy. It seems to have become corrupted. To restore the group policy, we'll need to restore the system state data on a domain controller.

The gpoutil is the Group Policy Object verification tool

Usage: gpoutil [options]

Options:

/gpo:GPO[,GPO...] Preferred policies. Partial GUID and friendly name match accepted. If not specified, process all policies in the domain.

/domain:name Specify the DNS name for the domain hosting the policies. If not present, assume user's domain.

/dc:DC[,DC...] Preferred list of domain controllers. If not specified, find all controllers in the domain.

/checkacl Verify sysvol ACL. For faster processing, this step is skipped

/verbose Display detailed information.

Identifying the File-Based GPO Structure on the System Volume

1. On a domain controller in the domain identified above, determine which drive hosts the system volume (Sysvol).
2. Using Windows Explorer, open the Sysvol folder.
3. The following folders exist: Domain, Staging, Staging Areas, and Sysvol. Change to the Sysvol folder.
4. A folder with the name of the domain that the local domain controller is a member of should exist.

Change to the following folder:

*Path to Sysvol*Sysvol\DomainName\Policies.

A folder for each GPO created in the domain, each identified by its GUID, should exist.

5. Open the folder identified by the GUID of the GPO that you recorded in the previous section of this article.

Note: The Group Policy structure on the system volume contains a Gpt.ini file that contains version information (of the GPO) and other optional data. Additionally, the file-based policy is broken into Machine and User folders with the appropriate policy for each. An Adm folder may also be present when software policies (administrative templates) are being used.

Without access to the properties of a given GPO, the administrator can use other methods of attaining either the GUID for a known GPO or the friendly name of a GPO of which the administrator has the associated GUID.

Reference:

Troubleshooting Group Policy Application Problems. **Microsoft Knowledge Base Article – 216359**

Troubleshooting Group Policy Application Problems. **Microsoft Knowledge Base Article - 250842**

QUESTION NO: 27

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 the 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 or RSoP.

Gpresult

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

RSoP overview Resultant 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: Gpupdate, 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: 28

You are the network administrator for TestKing. The network consists of a single Active Directory domain named testking.com. You are testing Group Policy object (GPOs) on an organizational unit (OU) named Test. The Test OU contains a Windows XP Professional client computer that you use as a test computer.

The domain contains a group named Security. You create a new GPO and configure the Computer Configuration section to grant the Security group the Change the system time user right.

You log on to the test computer and discover that the setting you set through the GPO is not in effect.

You need to apply the GPO settings immediately.

What should you do?

- A. Log off the test computer and log on again.
- B. Log off the test computer.
Create a test user account in the Test OU and then log on as the test user account.
- C. On the test computer, run the **gpresult** command.
- D. On the test computer, run the **gpupdate /force** command.

Answer: D

Explanation: We need to apply the group policy immediately, rather than wait for the next group policy refresh interval. We can do this using the gpupdate /force command.

Gpupdate

Refreshes local Group Policy settings and Group Policy settings that are stored in Active Directory, including security settings. This command supersedes the now obsolete /refreshpolicy option for the secedit command.

The switch **/force**

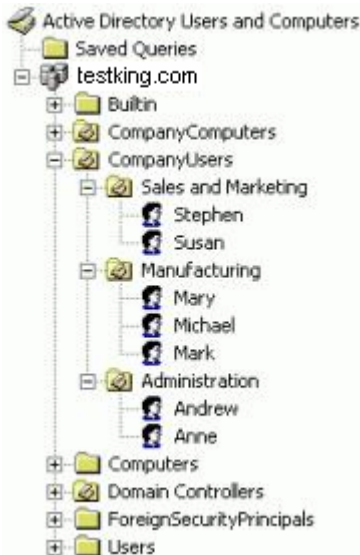
Ignores all processing optimizations and reapplies all settings.

Incorrect Answers:

- A:** We need to apply a computer policy, so we would need to restart the computer rather than just logging off.
B: There is no need to create another user account.
C: Gpresult is used to display the effective group policy settings. It does not apply group policy settings.

QUESTION NO: 29

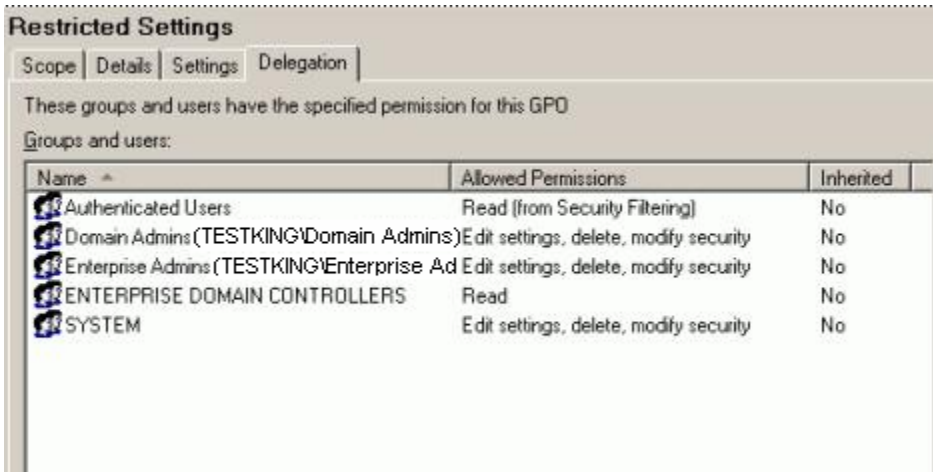
You are the network administrator for TestKing GmbH. The network consists of a single Active Directory domain named testking.com. All servers run Windows Server 2003. All client computers run Windows XP Professional. The Active Directory structure is shown in the Active Directory exhibit.



The company's written policy states that users in the manufacturing department are given only restricted access to settings and applications on their computers. The written policy also states that this limitation does not apply to members of a security group named Managers.

You create a Group Policy object (GPO) named Restricted Settings and link the GPO to the domain. This GPO contains the policy settings required by the written company policy.

You discover that the restricted settings apply to all users. You examine the Restricted Settings GPO by using the Group Policy Management Console (GPMC). The relevant information is shown in the GPMC exhibit.



You need to configure the network so that the written policy is enforced correctly.

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

- A. Unlink the Restricted Settings GPO from the domain.
Link it to the Manufacturing organizational unit (OU).
- B. Unlink the Restricted Settings GPO from the domain.
Link it to the Company Users organizational unit (OU).
- C. Assign the Authenticated Users group to the **Deny – Apply Group Policy** permission for the Restricted Settings GPO.
- D. Assign the Managers group the **Deny – Apply Group Policy** permission for the Restricted Settings GPO.

Answer: A, D

Explanation: The question states that the restricted settings should apply to users in the Manufacturing OU. The policy is currently linked to the domain which is why it is being applied to all users in the domain. We should unlink the policy from the domain and link it to the Manufacturing organizational unit (OU). Members of the Managers group should not receive the settings from the OU. We can fulfil this requirement by assigning the Managers group the **Deny – Apply Group Policy** permission for the Restricted Settings GPO.

Incorrect Answers:

- B:** The restricted settings should apply to users in the Manufacturing OU, not the Company Users OU.
- C:** This would prevent the policy applying to all users. The policy should apply to users in the Manufacturing OU.

QUESTION NO: 30

Leading the way in IT testing and certification tools, www.testking.com

You are the network administrator for TestKing. The company has a main office and six branch offices. Each branch office employs fewer than 15 users.

The network consists of a single Active Directory domain configured as a single site. All servers run Windows Server 2003. Domain controllers are located in the main office. All branch offices are connected to the main office by WAN connections.

All users are required to change their password every 10 days. They are further restricted from reusing a password until after they have used five different passwords. You discover that users in the branch office can log on by using recently expired passwords and access local resources during a WAN connection failure that lasts for 24 hours or longer.

You need to ensure that users can log on to the domain only by using a current password.

What should you do?

- A. Enable universal group membership caching in the site.
- B. Instruct all users to log on by using their principal names (UPNs).
- C. In Active Directory Users and Computers, require all users to change their passwords to the next time they log on to the domain.
- D. Configure the Default Domain Policy Group Policy object (GPO) to prevent logon attempts that use cached credentials.

Answer: D

Explanation: When the client computers are unable to contact a domain controller at the main office, the users are being logged on using 'cached credentials'. This means that the client computer remembers that the user successfully authenticated with the domain controller recently, so the client computer assumes it is ok to log the user on again after failing to contact a domain controller. We can disable this behaviour using a group policy.

Incorrect Answers:

- A:** Enabling universal group caching won't prevent the logons.
- B:** This won't prevent the users' ability to log on.
- C:** This won't prevent the users' ability to log on.

QUESTION NO: 31

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. Most of the client computers are located in the offices of individual users. Some client computers are located in publicly accessible locations.

The company's written security policy includes the following requirements.

- All users must use smart cards to log on to a client computer.
- Users using the publicly accessible client computers must be logged off if the smart card is removed from the smart card reader.

You configure all user accounts to require smart cards for interactive logon. You create an organizational unit (OU) named Public.

You need to ensure that the appropriate result occurs on each client computer when a smart card is removed.

You must achieve this goal without affecting other computers.

What should you do?

- Place all computer accounts for the publicly accessible client computers in the Public OU. Create a new Group Policy object (GPO) and link the GPO to the Public OU. Configure the **Interactive Logon: Smart card removal behavior** setting to **Force Logoff**.
- Place the user accounts of all users who use the publicly accessible client computers in the Public OU. Create a new Group Policy object (GPO) and link the GPO to the Public OU. Configure the **Interactive logon: Smart card removal behavior** setting to **Force logoff**.
- On the Default Domain Policy Group Policy object (GPO), configure the **Interactive logon: Smart card removal behavior** setting to **Force logoff**.
- On the Default Domain Controllers Policy Group Policy object (GPO), configure the **Interactive logon: Smart card removal behavior** setting to **Force Logoff**.

Answer: A

Explanation: We can place the public computers in the Public OU; this will enable us to apply a group policy to the public computers. The question states that users must be logged off if the smart card is removed from the smart card reader. There is a specific setting in group policy for this. We can configure the Interactive Logon: Smart card removal behaviour setting to Force Logoff.

MS White Paper

Planning a Smart Card Deployment

Selecting Group Policy Settings to Manage Smart Card Use

Several Group Policy settings are specific to smart card management. You can use these Group Policy settings to manage smart cards in your organization.

Note Other security policy settings, such as lockout policy or restricted logon times, can also impact smart card users if they use their cards for account logon.

Smart card required for interactive logon

When you set this policy on a user account, the user cannot log on to the account by using a password. They can only log on by using a smart card.

The advantage of using this policy setting is that it enforces strict security. However, if users are unable to log on by using conventional passwords, you must provide an alternate solution in the event that smart cards become unusable.

Note This policy setting applies to interactive and network logons only. It does not apply to remote access logons, which are managed by policy settings that are configured on the remote access server.

The **Smart card required for interactive logon** policy is not recommended for users who need to:

- Join a computer to a domain.
- Perform administrative tasks such as installing Active Directory on a member server.
- Configure a network connection for remote access.

If you choose not to use this security policy setting, users can revert to their standard network passwords if their smart cards are damaged or unavailable. However, this weakens security. In addition, users who use their passwords infrequently might forget them, and either write them down, or call the help desk for a password reset, increasing help desk costs to the organization.

On smart card removal

Users who walk away from computers that are running an active logon session create a security risk. To enforce the security of your system, it is best if users either log off or lock their computers when they leave. The **On smart card removal** policy allows you to force users to log off or lock their computers when they remove their smart cards.

Note If you select the forced logoff option, users need to make sure they have saved changes to documents and other files before they remove their smart cards. Otherwise, they lose any changes they have made.

Whether or not you set the **On smart card removal** policy depends on how your users interact with their computers. For example, this policy is a good choice if using computers in an open floor or kiosk environment. This policy might not be necessary when users have dedicated computers or exclusive use of multiple computers. You can use a password-protected screensaver or other means to lock the computers of these users.

Note The **On smart card removal** policy is a local computer policy that is administered on a per computer basis. Set the **On smart card removal** policy on a per user account basis, along with other domain security policy settings.

Incorrect Answers:

B: This is a computer setting, not a user setting.

C: This will force logoff all users in the domain. Only users of the public computers should be logged off when they remove their smart cards.

D: This will force logoff all users who log on to a domain controller. Only users of the public computers should be logged off when they remove their smart cards.

QUESTION NO: 32

You are a network administrator for TestKing. Your network consists of a single Active Directory domain named testking.com. All servers run Windows Server 2003.

The company has users who work in the main office and users who work remotely by connecting to a server running Routing and Remote Access. The company's written security policy requires that administrators in the main office log on by using smart cards. The written security policy also requires that remote users use smart cards to access network resources. No other users are required to use smart cards.

You issue portable computers that contain smart card readers to administrators and remote users. You issue smart cards to administrators and remote users. Administrators and remote users report that they can log on without using a smart card.

You need to ensure that only administrators are required to use smart cards when working in the main office. You must also ensure that remote users are required to use smart cards when accessing network resources.

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

- A. In the computer configuration settings of the Default Domain Policy Group Policy object (GPO), enable the **Interactive logon: Require smart card** setting.
- B. On the server running Routing and Remote Access, select the **Extensible authentication protocol (EAP)** check box and require smart card authentication.
- C. In the properties of each administrator account, select the **Smart Card Required for Interactive Logon** check box.
- D. In the computer configuration settings of the Default Domain Controllers Policy Group Policy object (GPO), enable the **Interactive logon: Requires smart card** setting.
- E. In the properties of each user account that requires remote access, select the **Smart Card Required for Interactive Logon** check box.

Answer: B, C

Explanation: We can require remote users to log on using smart cards only by configuring the RRAS server that the remote users connect to to require smart card authentication.

We can configure the administrators' user accounts to require smart cards for interactive logons. This setting is defined in the user properties in Active Directory Users and Computers.

TestKing1 Properties

Member Of | Dial-in | Environment | Sessions

Remote control | Terminal Services Profile | COM+

General | Address | Account | Profile | Telephones | Organization

User logon name:
 @TestKing.com

User logon name (pre-Windows 2000):

☐ Account is locked out

Account options:

☐ Account is disabled

☒ Smart card is required for interactive logon

☐ Account is trusted for delegation

☐ Account is sensitive and cannot be delegated

Account expires:

☒ Never

☐ End of:

Incorrect Answers:

A: This would require that all users log on using a smart card.

D: This would require that users use a smart card to log on to only the domain controllers. The administrators must use smart cards to log on to any machine in the domain.

E: This would require that the remote users log on using a smart card to any machine. They don't need a smart card logon if they are using a machine in the office.

QUESTION NO: 33

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

In a test lab that contains a separate forest, you develop and test a Group Policy object (GPO) that you need to apply to all computers and users in the domain.

You need to implement the new GPO on the network. You want to accomplish this task by using the minimum amount of administrative effort.

What should you do?

- A. Use a Distributed File System (DFS) to replicate the GPO information in the SYSVOL shared folder from the test lab to the domain.
- B. Use the Group Policy Management Console (GPMC) to back up the GPO from the test lab and import it into the domain.
- C. Copy the Group Policy Template (GPT) files in the SYSVOL shared folder from the test lab to the domain.
- D. Use Active Directory Users and Computers to create a new GPO linked to the domain.
In the new GPO, include all of the settings that exist in the GPO in the test lab.

Answer: B

Explanation: We can use the Group Policy Management Console (GPMC) to back up the GPO from the test lab and import it into the domain.

MS White Paper

Migrating GPOs Across Domains with GPMC

<http://www.microsoft.com/windowsserver2003/docs/MigGPOs.doc>

The GPMC lets administrators manage Group Policy for multiple domains and sites within one or more forests, all in a simplified user interface (UI) with drag-and-drop support. Highlights include new functionality such as backup, restore, import, copy, and reporting of Group Policy objects (GPOs). These operations are fully scriptable, which lets administrators customize and automate management.

QUESTION NO: 34

You are a network administrator for TestKing. All client computers run Windows XP Professional.

You administer a Windows Server 2003 file server named TestKingSrvC. TestKingSrvC contains two volumes configured as drive G and Drive H. Shared folders for the accounting department are stored on drive G. Shared folders for the marketing department are stored on drive G and on drive H. Drive H has sufficient space to store all of the shared folders with 400 GB of free space.

The design team specifies the following requirements for the files in the marketing shared folders on TestKingSrvC:

- The files must be backed up, even if they are open.

Leading the way in IT testing and certification tools, www.testking.com

- Backups can be performed during business hours, if required.
- Users must be able to restore the files.

You need to create a plan that will allow the backup and recovery of folders and files in accordance with the requirements. You need to minimize data loss.

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

- A. Customize all shared folders by using the Documents template.
- B. Place all marketing shared folders on drive H.
Enable Shadow Copies of Shared Folders on the volume.
- C. Configure all backups by selecting the **Disable volume shadow copy** check box.
- D. Install the Previous Versions client software on all marketing client computers.
- E. Assign all users the **Allow – Full Control** NTFS permissions for the marketing shared folders.

Answer: B, D

Explanation: The question states that drive H has sufficient space to hold all the files, and will have enough space left over to hold shadow copies of the files. The client computers will need the previous versions client software to access the previous versions of the files.

Deploying the client software for shadow copies.

The client software for Shadow Copies of Shared Folders is installed on the server in the \\%systemroot%\system32\clients\twclient directory.

You can distribute the client software in a variety of ways; consider the various options before deployment. There are several tools included in the Windows Server 2003 family, such as Group Policy, that can make deploying and maintaining the clients software easier.

Recover files that were accidentally deleted.

If you accidentally delete a file, you can open a previous version and copy it to a safe location.

Recover from accidentally overwriting a file. If you accidentally overwrite a file, you can recover a previous version of the file.

Compare versions of file while working.

You can use previous versions when you want to check what has changed between two versions of a file.

Incorrect Answers:

A: This is not necessary.

C: This option should be enabled, not disabled, in order to back up the open files.

E: It is not necessary to change the permissions on the marketing shared folders.

QUESTION NO: 35

You are the network administrator for TestKing. The network consists of a single Active Directory domain named testking.com. The domain contains Windows Server 2003 computers and Windows XP Professional client computers. The domain contains two organizational units (OUs) named Sales and Marketing. Both OUs have multiple Group Policy Objects (GPOs) linked to them.

The Sales OU needs to be moved under the Marketing OU.

You need to find out which objects in the Sales OU are adversely affected by GPOs linked to the Marketing OU.

You need to achieve this goal without disruption to users.

What should you do?

- A. Use Resultant Set of Policy (RSoP) in logging mode for the Marketing OU.
Review the policy results for the users in the OU.
- B. Use Resultant Set of Policy (RSoP) in logging mode for the Sales OU.
Review the policy results for the users in the OU.
- C. Use Resultant Set of Policy (RSoP) in planning mode for the Marketing OU.
Choose the Sales OU to simulate policy settings.
- D. Use Resultant Set of Policy (RSoP) in planning mode for the Sales OU.
Choose the Marketing OU to simulate policy settings.

Answer: D

Explanation: We need to view the effective group policy without actually applying the group policy and disrupting the users. For this, we can use RSoP in planning mode.

RSoP Modes

Planning Mode

In planning mode, you can determine how policy settings are applied to a target, and then analyze the results before deploying a change to Group Policy. For example, you can use planning mode to simulate moving a user to a different group, or to see the effects of placing the user in different security groups.

In planning mode, the Group Policy Data Access Service mimics the function of the Windows logon service. Planning mode simulates calling each Group Policy client-side extension to allow the extension to write policy data to the Common Information Model Object Manager (CIMOM) database.

Logging Mode

In logging mode, you can assess which policy settings have been applied or failed to apply to a particular target (users or computers in Active Directory). Group Policy client-side extensions have a WMI interface that writes information (known as *logging mode data*) about their policy settings to a CIMOM database. You can use the RSoP user interface to query the CIMOM database for policy information

RSOP logging is enabled by default. You can use a policy setting to disable this option. To do so, disable the Turn off Resultant Set of Policy Logging policy under the Computer Configuration\Administrative Templates\System\Group Policy node for computers or disable the Disallow Interactive Users from generating Resultant Set of Policy setting under the User Configuration\Administrative Templates\System\Group Policy node for users.

Incorrect Answers:

A: We need to use planning mode, not logging mode.

B: We need to use planning mode, not logging mode.

C: We need to test the effects of applying the Marketing OU policies to the Sales OU, not vica versa.

Reference:

MS Knowledge Base article 323276: HOW TO: Install and Use RSoP in Windows Server 2003
Server Help: RSoP overview

QUESTION NO: 36

You are the network administrator for Acme. The company consists of two subsidiaries named Litware Inc., and TestKing. Litware, Inc., has an office in Los Alamos. TestKing has two offices, one in New Delhi and the other in Berlin.

The network consists of two Active Directory forests. A forest trust relationship exists between the two forests. One forest contains one domain named LosAlamos.litwareinc.com. The other forest contains two domains named NewDelhi.testking.com and Berlin.testking.com. All three offices are connected by two 128-Kbps connections. All servers run Windows Server 2003.

The network uses roaming profiles and Group Policy objects (GPOs). Occasionally, users need to work at an office other than their usual office. Users must have the same desktop, no matter where they log on to the network.

You need to ensure that the user's profile and the GPO settings that apply to the user's account will apply wherever the user logs on to the network.

What should you do?

To answer, drag the appropriate configuration or configurations to the correct policy or policies in the work area.

Configuration Select from these		Place here
Enabled		Wait for remote user profile
Disabled		Group Policy slow link detection
Not configured		Allow Cross-Forest User Policy and User Roaming Profiles

Answer:

Configuration Select from these		Place here
Enabled		Wait for remote user profile
Disabled		Group Policy slow link detection
Not configured		Allow Cross-Forest User Policy and User Roaming Profiles

Explanation: The question states that when a user logs on in the other forest to the one where his user account resides, the user MUST have his desktop settings and group policy settings. The first setting, “Wait for remote user profile” should be enabled so that the client computer waits to load the remote profile, no matter how long it takes. To enable the roaming profiles and group policy settings to apply to the user across a forest link, we should enable the third setting, “Allow Cross-Forest User Policy and User Roaming Profiles”.

We need to prevent the speed of the link affecting the policies that are applied. However, we can’t do this by simply disabling the slow link detection, because a disabled slow link detection policy will use a default setting of 512Kbps (our link is slower than that, so some group policy settings won’t apply). We need to enable the policy and enter a connection speed of 0. This disables the setting in such a way that all group policies will be applied across the slow link, no matter how long they take to load.

Reference:

Designing a Group Policy Infrastructure

Roaming Users

Leading the way in IT testing and certification tools, www.testking.com

Roaming users access the corporate network through LAN links. They have permanent LAN connections when working locally, but if they roam between sites, they might have restricted network bandwidth back to some servers. They need to access their data from multiple workstations from many different areas in the same physical location.

Mobile Users

Mobile users need to access the network at different times and locations by using dial-up connections, varying LAN connections, or across a wide area network (WAN) link. Therefore, network services must be accessible at any time.

The following characteristics apply:

- Their computers are often connected by slow or intermittent network links.
- The bandwidth, quality, and consistency of their network connections are highly variable.
- Users need to save data and settings locally when working offline (their data and settings might be synchronized to a file server).
- The availability of different types of services depends on whether the users are connected to the corporate network and the speed and reliability of their connections.

Optional Settings for Mobile Users

Mobile users might require additional flexibility to configure their systems, for example, they need to configure virtual private network (VPN) connections. In such cases, enable the following settings:

- Enable deletion of remote access connections (belonging to the user).
- Enable renaming of connections belonging to the current user.
- Display and enable the Network Connection wizard.
- Allow access to the current user's remote access connection properties.
- Enable access to the properties of the components of a local area network (LAN) connection.
- Enable access to the properties of the components of a remote access connection.
- Enable status statistics for an active connection.
- Enable the Dial-up Preferences item on the Advanced menu.

Consider using a separate Group Policy object for users who work mostly away from the office, and modify the following policy settings, which are located in the Computer Configuration\Administrative Templates\System\Logon node.

- Slow network connection timeout for user profiles: Defines a slow connection for roaming user profiles.
 - Defines a slow connection for roaming user profiles. If the server on which the user's roaming user profile resides takes longer to respond than the thresholds that are set by this policy permit, the system considers the connection to the profile to be slow. This policy and related policies in this folder together determine how the system responds when roaming user profiles are slow to load.
- Wait for remote user profile: Directs the system to wait for the remote copy of the roaming user profile to load, even when loading is slow.
 - Directs the system to wait for the remote copy of the roaming user profile to load even when loading is slow. The system waits for the remote copy when the user is notified about a slow connection but does not respond within the time allowed.

- If you enable the **Wait for remote user profile** policy, the system loads the remote copy without prompting the user.
- Prompt user when slow link is detected: Notifies users when their roaming profile is slow to load.
- Timeout for dialog boxes: Determines how long the system waits for a user response before it uses a default value.

Special Considerations for Site-linked GPOs

Multiple domains (within a forest) can get the same Group Policy object (and included policies), although the Group Policy object only lives on a single domain and must be read from that domain when the affected clients read their site policy.

If child domains are set up across wide area network (WAN) boundaries, the site setup typically reflects this. If it does not, the computers in a child domain might be accessing a site Group Policy object across a WAN link.

By default, to manage site GPOs, you need to be either an Enterprise Administrator or domain administrator of the forest root domain.

Replication between domain controllers in different sites occurs less frequently than replication between domain controllers in the same site, and during scheduled periods only. The replication schedule and frequency are properties of the site links that connect sites. The default inter-site replication frequency is three hours. To change it, go to the appropriate site link, into the IP link, and change the replication frequency or schedule as desired.

Allow Cross-Forest User Policy and Roaming User Profiles

Requirements: At least Microsoft Windows Server 2003

Location: Computer Configuration\System\Group Policy\

Description:

Allows User based policy processing, Roaming User Profiles and User Object logon scripts for cross forest interactive logons.

This setting affects all user accounts interactively logging on to a computer in a different forest when a Cross Forest or 2-Way trust exists.

QUESTION NO: 37

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.

A Group Policy object (GPO) named Software Restrictions prevents users from running unauthorized applications. This restriction does not apply to users who are local administrators on their client computers.

Developers at the company create a new application for internal users. An administrator installs the application on a number of computers by running the Setup.exe file supplied by the developers. However, when users try to run the new application, they report that they cannot do so.

You need to ensure that all users can run the new application. You also need to ensure that unauthorized applications cannot run.

What should you do?

- A. Install the application on computers that require its use.
Create a VMI filter on the Software Restrictions GPO that detects where the software is installed and prevents the GPO from being applied.
- B. Create a security group that contains all users who need to use the application.
Modify the security settings on the Software Restrictions GPO so that its effects are bypassed for members of this group.
- C. Create a hash value for the application's executable code file, and revise the Software Restrictions GPO to allow executable code files that match the hash value to run.
- D. Repackage the application as an .msi package and use a new GPO to assign the package to the computers that require the application.

Answer: C

Explanation: We have a software restrictions policy that only allows authorised applications to run. The new application isn't authorised, so we need to authorise it by creating a hash value of the program file and modify the software restrictions policy to permit the users to run the application.

Reference:

MS knowledge Base Article Q 324036 HOW TO: Use Software Restriction Policies in Windows Server 2003

How to Create a Hash Rule

1. Click Start, click Run, type mmc, and then click OK.
2. Open Software Restriction Policies.
3. In either the console tree or the details pane, right-click Additional Rules, and then click New Hash Rule.
4. Click Browse to find a file, or paste a precalculated hash in the File hash box.
5. In the Security level box, click either Disallowed or Unrestricted.
6. In the Description box, type a description for this rule, and then click OK.

NOTES:

- You may have to create a new software restriction policy setting for this GPO if you have not already done so.
- You can create a hash rule for a virus or a Trojan horse to prevent the malicious software from running.
- If you want other users to use a hash rule so that a virus cannot run, calculate the hash of the virus by using software restriction policies, and then e-mail the hash value to other users. Never e-mail the virus itself.
- If a virus has been sent through e-mail, you can also create a path rule to prevent users from running mail attachments.
- A file that is renamed or moved to another folder still results in the same hash.
- Any change to a file results in a different hash.
- The only file types that are affected by hash rules are those that are listed in designated file types. There is one list of designated file types that is shared by all rules.
- For software restriction policies to take effect, users must update policy settings by logging off from and then logging on to their computers.
- When more than one rule is applied to policy settings, there is a precedence of rules for handling conflicts.

Incorrect Answers:

A: The GPO prevents users running unauthorized software. Therefore, this GPO must be applied at all times – we cannot use a WMI filter to prevent the application of the GPO.

B: The GPO prevents users running unauthorized software. Therefore, this GPO must be applied at all times – we cannot use security filtering to prevent the application of the GPO to the users who require access to the new application.

D: Windows clients support setup.exe files. As long as the setup.exe file is written correctly, the users would be able to use the application. The users in this scenario cannot run the program because the software restrictions group policy is preventing them running the application.

QUESTION NO: 38

You are the network administrator for TestKing. The network consists of two Active Directory forests, each consisting of a single domain. The functional level of both forests is Windows Server 2003. One forest is used for testing and the other forest is used for production. The test forest contains a single domain controller.

You are using the test forest to test Group Policy objects (GPOs) that manage administrative templates before they are implemented in the production forests. This testing includes changes to the Default Domain Policy GPO and the Default Domain Controllers Policy GPO.

You need to be able to restore the Default Domain Policy and Default Domain Controllers Policy GPOs for the test domain to the settings used in the production forest. You want to accomplish this task 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. Run the **dcgpofix /both** command in the test domain.
- B. Back up the Default Domain Policy and Default Domain Controllers Policy GPOs from the production domain by using the Group Policy Management Console (GPMC).
- C. Import the Default Domain Policy and Default Domain Controllers Policy GPOs into the test domain by using the Group Policy Management Console (GPMC) and a migration table.
- D. Back up the original GptTmpl.inf files for the Default Domain Policy and Default Domain Controllers Policy GPOs from the production forests.
- E. Restore the backed up GptTmpl.inf files to the test domain.
- F. Increment the version in the Gpt.ini files for the Default Domain Policy and Default Domain Controllers Policy GPOs.

Answer: B, C

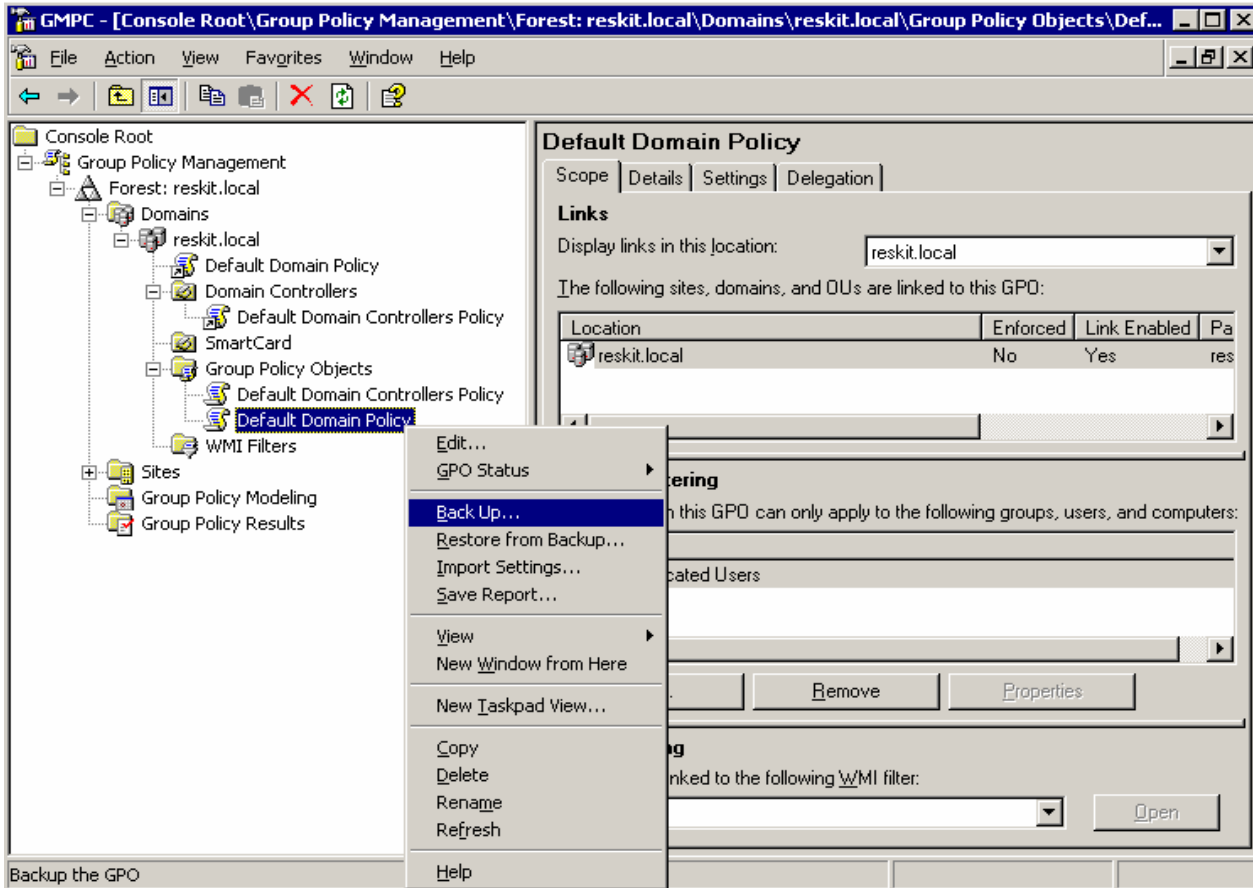
Explanation: We can use the Group Policy Management Console (GPMC) to back up the GPOs from the production domain and import them into the test lab.

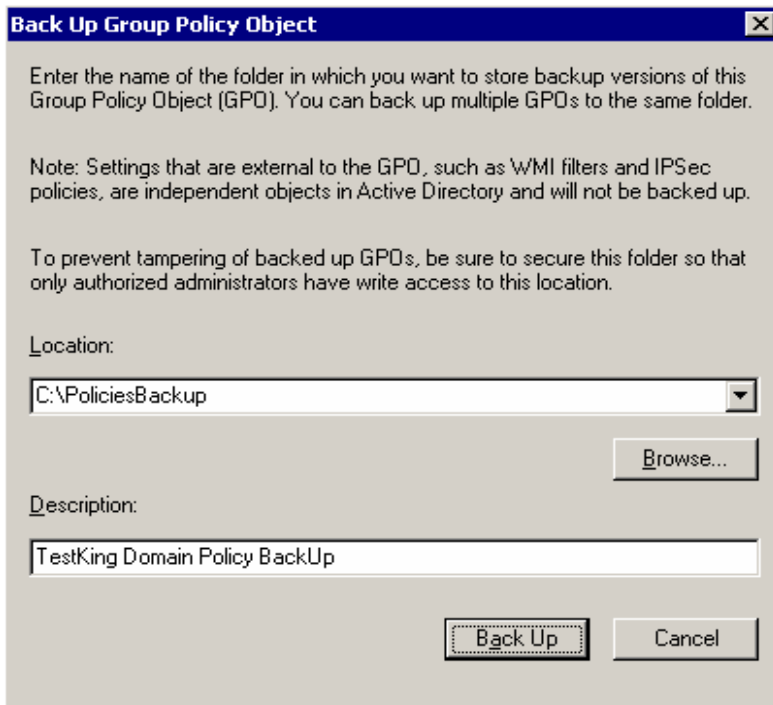
MS White Paper

Migrating GPOs Across Domains with GPMC

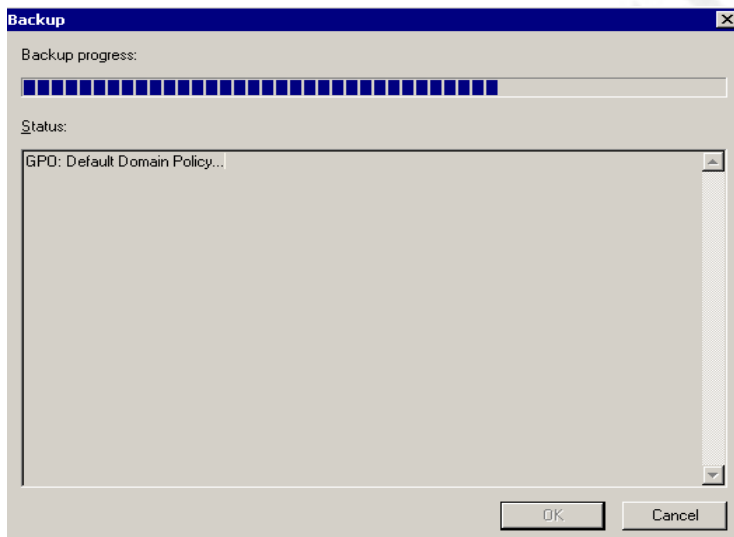
<http://www.microsoft.com/windowsserver2003/docs/MigGPOs.doc>

The GPMC lets administrators manage Group Policy for multiple domains and sites within one or more forests, all in a simplified user interface (UI) with drag-and-drop support. Highlights include new functionality such as backup, restore, import, copy, and reporting of Group Policy objects (GPOs). These operations are fully scriptable, which lets administrators customize and automate management.





The path must exist already



When we do the restore process, we need to restore both policies Domain and DCS. Therefore, for the DC's we will need to use a migration table, to migrate the security principals.

Migration Table TOOL

Leading the way in IT testing and certification tools, www.testking.com

Migration Table Editor - C:\MigrationTable.migtable		
File Edit Tools Help		
Source Name	Source Type	Destination Name
► Enterprise Admins@reskit.local	Domain Global Group	<Same As Source>
Server Operators	Free Text or SID	Server Operators
Account Operators	Free Text or SID	Account Operators
ENTERPRISE DOMAIN CONTROLLERS	Free Text or SID	ENTERPRISE DOMAIN CONTROLLERS
Everyone	Free Text or SID	Everyone
NETWORK SERVICE	Free Text or SID	NETWORK SERVICE
Authenticated Users	Free Text or SID	Authenticated Users
Pre-Windows 2000 Compatible Access	Free Text or SID	Pre-Windows 2000 Compatible Access
Administrators	Free Text or SID	Administrators
Print Operators	Free Text or SID	Print Operators
SUPPORT_388945a0@reskit.local	User	<Same As Source>
Backup Operators	Free Text or SID	Backup Operators
LOCAL SERVICE	Free Text or SID	LOCAL SERVICE
Domain Admins@reskit.local	Domain Global Group	<Same As Source>
*		

Import Settings Wizard

Migrating References
Specify how you want to transfer references to security principals (groups, users, computers) and UNC paths.

The GPO backup contains references to security principals and/or UNC paths. Transfer these references by:

☐ Copying them identically from the source.

☒ Using this migration table to map them in the destination GPO:

Browse...

☒ Use migration table exclusively. If any security principals or UNC paths in the GPO backup are not found in the migration table, do not perform the import operation.

Edit
New

< Back Next > Cancel Help

Import Settings Wizard

Migrating References
Specify how you want to transfer references to security principals (groups, users, computers) and UNC paths.

The GPO backup contains references to security principals and/or UNC paths. Transfer these references by:

☐ Copying them identically from the source.

☒ Using this migration table to map them in the destination GPO:

C:\MigrationTable.migtable Browse...

☒ Use migration table exclusively. If any security principals or UNC paths in the GPO backup are not found in the migration table, do not perform the import operation.

Edit
New

< Back Next > Cancel Help

If we install GPMC in the default path we need to execute from C:\Program Files\GPMC\Scripts
The script **CreateMigrationTable.wsf**. This script Creates migration tables that can be edited and used to map paths and security principals to new values when importing and copying GPOs across domains.

Sample:

```
C:\>cscript "C:\Program Files\GPMC\Scripts\CreateMigrationTable.wsf"
```

Creates a migration table that can be edited and used for mapping paths and security principals when performing import and copy operations.

The scripts can optionally pre-populate the table from various sources, including individual GPOs, a backup location containing GPO backups and all GPOs in the specified domain.

If you specify the /MapByName switch, the entries will use the "MapByRelativeName" option, which will expect a corresponding account with the same name as the original in the destination domain.

Usage: CreateMigrationTable.wsf TableName [/GPO:value] [/BackupLocation:value] [/AllGPOs] [/Overwrite] [/MapByName] [/Domain:value]

Options:

TableName : The file name of the migration table to be created
GPO : The name of a GPO to process when building the migration table
BackupLocation : File system location where backups are located
AllGPOs : Flag specifying to process all GPOs in the domain
Overwrite : If specified, will overwrite an existing XML instead of appending to it
MapByName : If specified, will set the default destination to map by relative name
Domain : DNS name of domain

Example switches

```
C:\>cscript "C:\Program Files\GPMC\Scripts\CreateMigrationTable.wsf" MigrationTable.migtable  
/BackupLocation:c:\PoliciesBackUP /OverWrite /MapByName
```

OUTPUT message

Processing backed up GPO 'Default Domain Controllers Policy'

Processing backed up GPO 'Default Domain Policy'

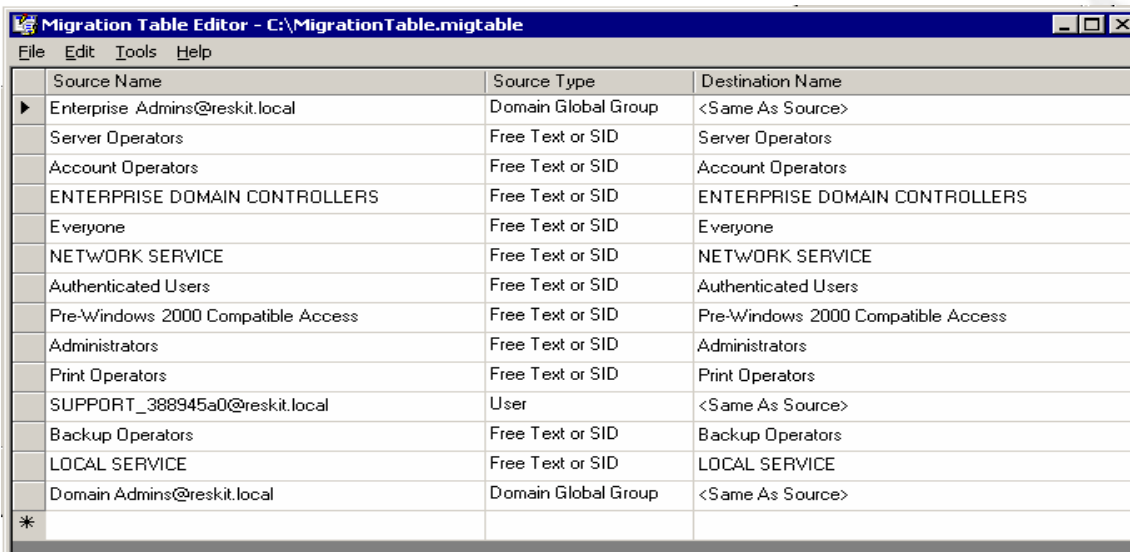
Entry 'Enterprise Admins@reskit.local' is defined in an external domain. This will not be mapped by name and will be set to be copied as is.

Entry 'SUPPORT_388945a0@reskit.local' is defined in an external domain. This will not be mapped by name and will be set to be copied as is.

Entry 'Domain Admins@reskit.local' is defined in an external domain. This will not be mapped by name and will be set to be copied as is.

Done. Migration table 'MigrationTable.migtable' was created.

Migration Table TOOL



Source Name	Source Type	Destination Name
Enterprise Admins@reskit.local	Domain Global Group	<Same As Source>
Server Operators	Free Text or SID	Server Operators
Account Operators	Free Text or SID	Account Operators
ENTERPRISE DOMAIN CONTROLLERS	Free Text or SID	ENTERPRISE DOMAIN CONTROLLERS
Everyone	Free Text or SID	Everyone
NETWORK SERVICE	Free Text or SID	NETWORK SERVICE
Authenticated Users	Free Text or SID	Authenticated Users
Pre-Windows 2000 Compatible Access	Free Text or SID	Pre-Windows 2000 Compatible Access
Administrators	Free Text or SID	Administrators
Print Operators	Free Text or SID	Print Operators
SUPPORT_388945a0@reskit.local	User	<Same As Source>
Backup Operators	Free Text or SID	Backup Operators
LOCAL SERVICE	Free Text or SID	LOCAL SERVICE
Domain Admins@reskit.local	Domain Global Group	<Same As Source>
*		

Notes

- You must have **Edit, delete, and modify security** permissions on the GPO and **Read** permissions on the folder containing the GPO backup to restore an existing GPO.
- You must have privileges to **create** GPOs in the domain and **Read** permissions on the file system location of the backed up GPO to restore a GPO that has been deleted.
- You can also restore an existing or deleted GPO using the **Manage backups** function by right-clicking **Domains** or **Group Policy Objects**.
- The **Manage Backups** dialog box can be used to restore either an existing or deleted GPO. The **Manage Backups** dialog box can be opened either by right-clicking **Domains** or **Group Policy Objects** in a given domain. When **Manage Backups** is opened by right clicking **Group Policy Objects**, only GPO backups from that domain are shown. In contrast, when **Manage Backups** is opened by right clicking **Domains**, all GPO backups are shown, regardless of domain.

QUESTION NO: 39

You are the network administrator for TestKing. The network consists of a single Active Directory forest. The functional level of the forest is Windows 2000. The forest consists of a forest root domain named testking.com and two child domains named asia.testking.com and europe.testking.com.

The functional level of all the domains is Windows 2000 mixed. Each domain contains one domain controller running Windows Server 2003. All of the other domain controllers in the forest run Windows 2000 Server.

TestKing recently acquired another company named Acme that has an Active Directory forest named acme.com. The functional level of the forest is Windows Server 2003.

You need to be able to establish a forest trust relationship between testking.com and acme.com.

What should you do?

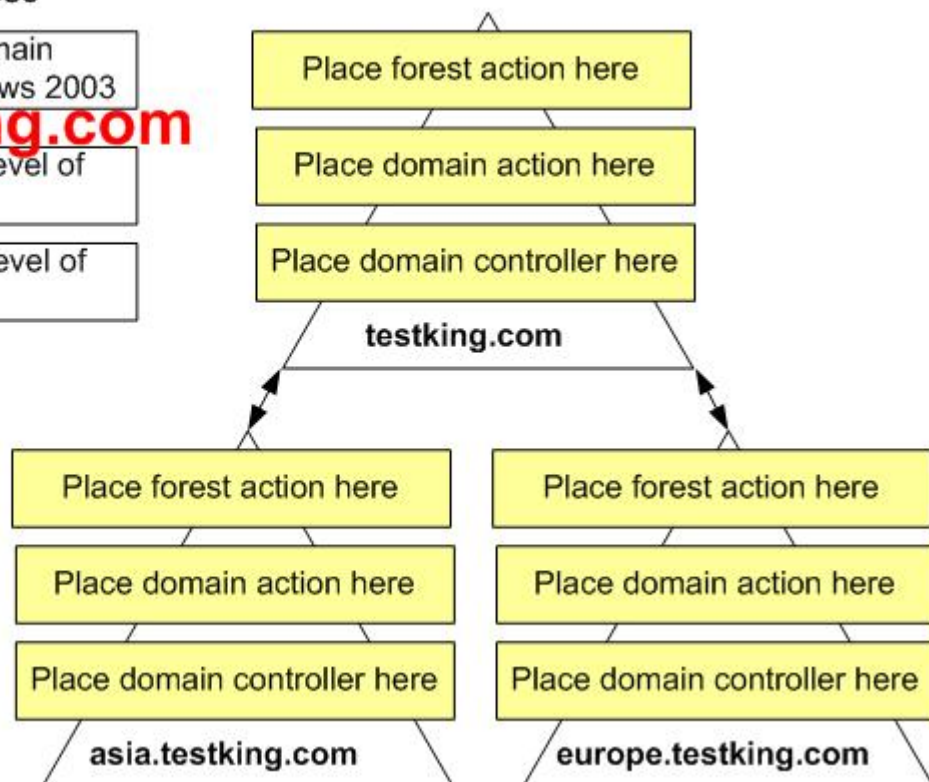
To answer, drag the appropriate action or actions to the correct location or locations in the work area.

Possible Domain Controller Action

Select from these

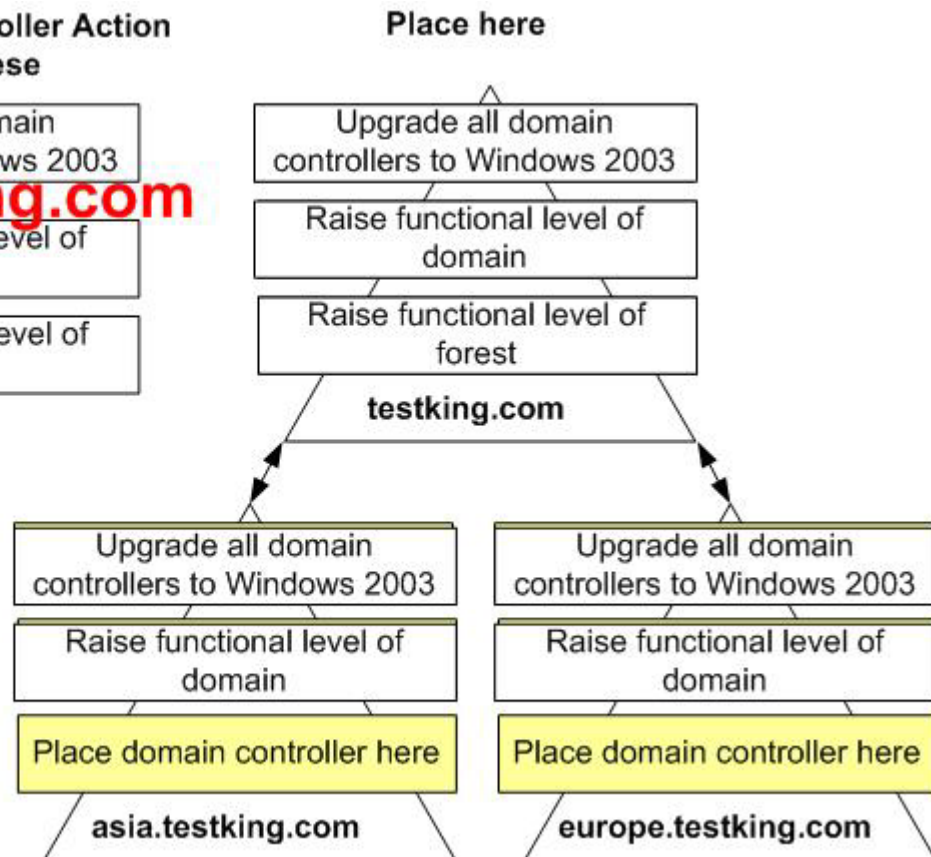
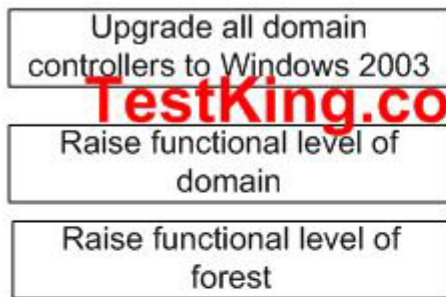
- Upgrade all domain controllers to Windows 2003
- Raise functional level of domain
- Raise functional level of forest

Place here



Answer:

Possible Domain Controller Action
Select from these



Explanation: The question explicitly asks for a “Forest Trust Relationship”, rather than just an external trust. To create a forest trust relationship, both forests must be in Windows 2003 functional level. For this functional level, all domains must be in Windows 2003 functional level which requires that all domain controllers are running Windows 2003 Server.

QUESTION NO: 40

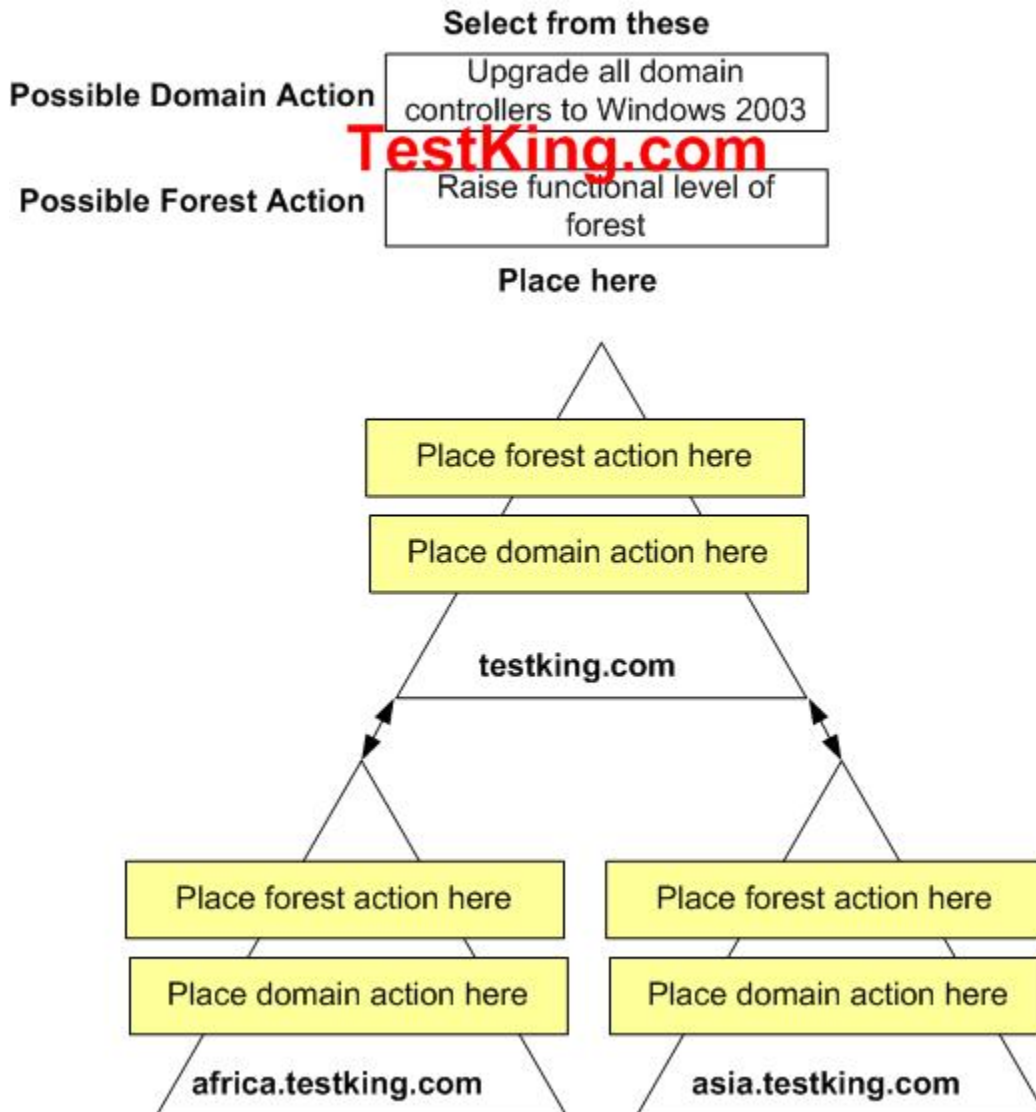
You are the network administrator for TestKing. The network consists of a single Active Directory forest testking.com. The functional level of the forest is Windows 2000. The forest consists of a root domain named testking.com and two child domains named africa.testking.com and asia.testking.com.

The functional level of the domains is Windows 2000 native. All domain controllers in the testking.com domain run Windows Server 2003. All domain controllers in the africa.testking.com and asia.testking.com domains run Windows 2000 Server.

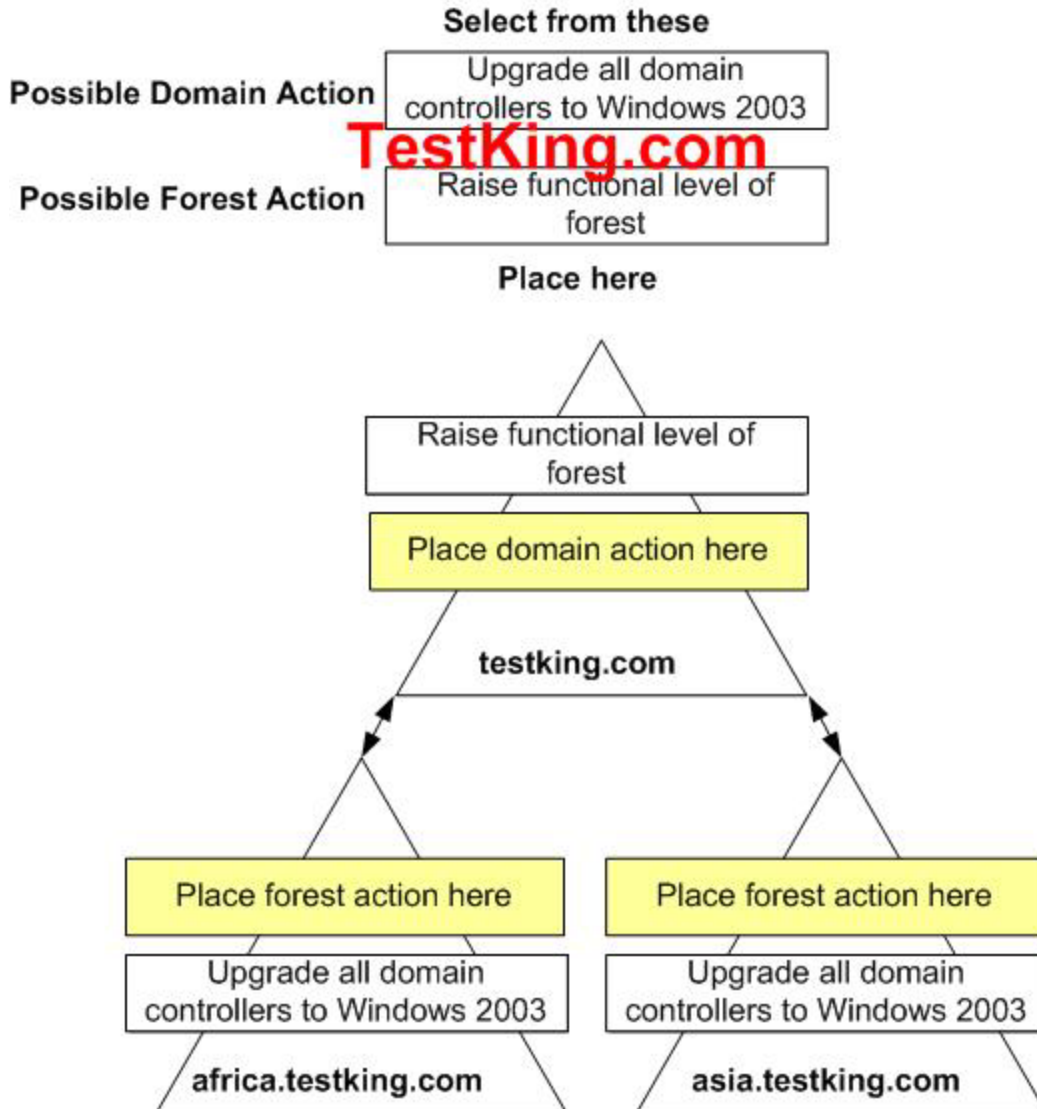
You need to be able to rename all domain controllers in testking.com. You want to minimize impact to the network.

What should you do?

To answer, drag the appropriate action or actions to the correct location or locations in the work area.



Answer:



Explanation: To rename domain controllers, the domains have to be in Windows 2003 functional level. We don't have the option to raise the domain functional levels, but upgrading the forest functional level will automatically upgrade the domain functional levels if the domains are in Windows 2000 native functional level.

To rename a Windows Server 2003 domain controller,

You must be a member of the Domain Admins group or the Enterprise Admins group in Active Directory.
Domain functional level is set to Windows Server 2003

NOTE: YOU do not need to raise the forest level, just domain level.

Note :

Before you rename a domain controller in a domain with multiple domain controllers, make sure that the computer that you want to rename is not the global catalog server and that it does not hold other Flexible Single Master Operations (FSMO) roles.

TO Rename a Domain Controller in a Domain that Contains a Single Domain Controller

To rename a domain controller in a domain that contains a single domain controller:

1. Install a second Windows Server 2003 computer in the same domain with the server that you want to rename.

Raising the forest functional level to Windows Server 2003 is not possible if there is any domain controller in the forest that remains to be upgraded to Windows Server 2003 or if any domain in the forest still has Windows 2000 mixed domain functionality. Assuming these requirements are satisfied, you can raise the forest level to Windows Server 2003.

NOTE:

Remember that although the forest root domain can be renamed (its DNS and NetBIOS names can change), it cannot be repositioned in such a way that you designate a different domain to become the new forest root domain. If your domain rename operation involves restructuring the forest through repositioning of the domains in the domain tree hierarchy as opposed to simply changing the names of the domains in-place, you first need to create the necessary shortcut trust relationships between domains such that the new forest structure has two-way transitive trust paths between every pair of domains in the target forest, just as your current forest does

Reference:

MS white paper

Step-by-Step Guide to Implementing Domain Rename

MS Knowledge base article

Q814589 HOW TO: Rename a Windows 2003 Domain Controller

QUESTION NO: 41

You are a network administrator for TestKing. The network consists of 20 Active Directory domains. All servers run Windows Server 2003. TestKing has 240 offices. Each office is configured as an Active Directory site.

TestKing has a branch office that contains four users. User objects for these users are stored in the australia.testking.com domain. The branch office is connected to the corporate network by a 56-Kbps WAN connection. The branch office contains a domain controller named TestKing17 that is configured as an additional domain controller for the australia.testking.com domain. An Active Directory site is configured for the branch office. TestKing17 is a member of this site. An IP site link exists between the branch office and the main office.

The WAN connection is available only during business hours. Users in the branch office report slow response times on the WAN connection. You examine the WAN connection and discover that the problem is caused by Active Directory replication.

You need to improve the performance of the WAN connection.

What should you do?

- A. Configure TestKing17 as a global catalog server.
- B. Enable universal group membership caching in the branch office.
- C. Remove Active Directory from TestKing17 and configure TestKing17 as a member server.
- D. On the site link that connects the branch office to the corporate network, increase the replication interval.

Answer: D

Explanation: The branch office contains a domain controller from the australia.testking.com domain. Replication between this domain controller and a domain controller at the main office is using up the bandwidth of the 56Kbps link between the two sites. We can reduce the WAN link usage by increasing the replication interval, thus ensuring that replication across the WAN link occurs less frequently.

Incorrect Answers:

- A:** Configuring TestKing17 as a global catalog server will increase the bandwidth used by the replication.
- B:** Enabling universal group membership caching in the branch office won't decrease the bandwidth used the replication.
- C:** It is not necessary to demote TestKing17 to a member server. Furthermore, this would cause logon authentication traffic to go over the WAN link.

QUESTION NO: 42

You are the network administrator for Testking Ltd. The network consists of a single Active Directory forest. The functional level of the forest is Windows Server 2003. The forest contains a root domain named testking.com and two child domains named scotland.testking.com and wales.testking.com. All domain controllers run Windows Sever 2003.

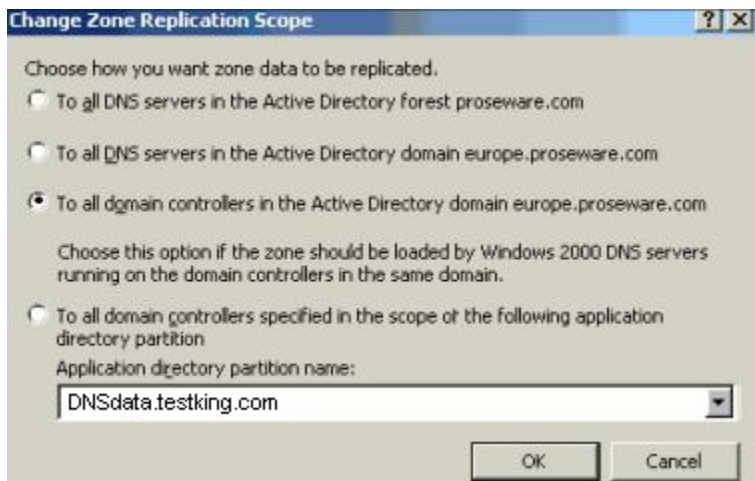
Each domain contains a DNS server. The DNS server in testking.com is named TESTKINGDNS1, the DNS server in scotland.testking.com is named TESTKINGDNS2, and the DNS server in wales.testking.com is named TESTKINGDNS3. Each DNS server in a child domain is responsible for name resolution in only its domain. The TCP/IP properties of all client computers in the child domains are configured to use only the DNS server in the domain. All records of all DNS servers are stored in Active Directory.

You create a new application directory partition named `DSNdata.testking.com`. You enlist `TESTKINGDNS1` and `TESTKINGDNS2` in this application directory partition.

You need to enable all users in `testking.com` to access resources in the `scotland.testking.com` domain by using host names. Users in the `testking.com` domain do not need to access resources in the `wales.testking.com` domain. You need to configure the zone replication scope of the `scotland.testking.com` domain at `TESTKINGDNS2`.

What should you do?

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



Answer: Select the fourth radio button.

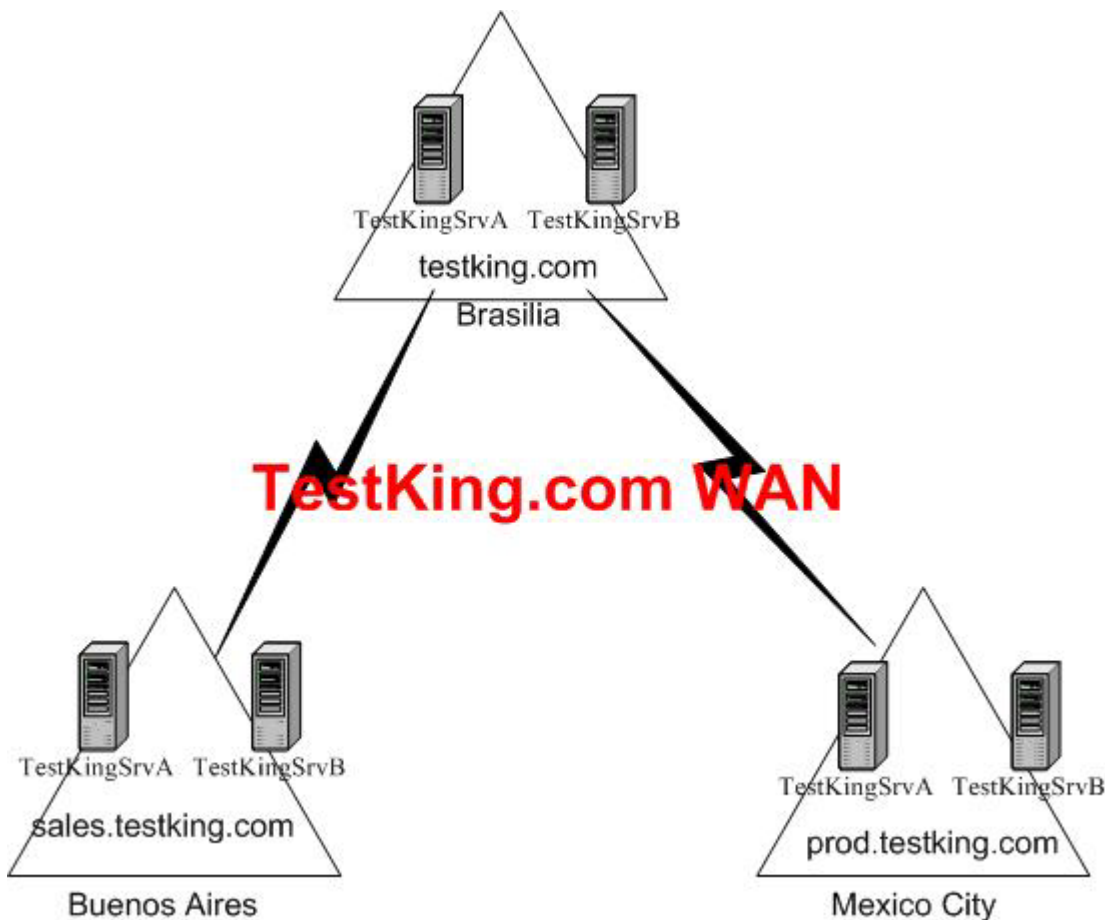
Explanation: The application directory partition `DSNdata.testking.com` contains a DNS server from `testking.com` and `Scotland.testking.com`. By configuring the DNS information from the DNS server in `Scotland.testking.com` to be replicated to the DNS server in `testking.com`, we will enable users in `testking.com` to locate resources in `Scotland.testking.com`.

QUESTION NO: 43

You are the network administrator for TestKing. The company has offices in Brasilia, Buenos Aires, and Mexico City. Each office employs 500 people.

The network consists of a single Active Directory forest with one domain in each office. Each domain contains two domain controllers named `TestKingSrvA` and `TestKingSrvB`. All domain controllers run

Windows Server 2003. Each office is configured as an Active Directory site. The domain structure is shown in the exhibit.



The Windows Server 2003 computer named TestKingSrvA.testking.com holds all operations master roles for its domain, and it holds both forest-level operations master roles. The Windows Server 2003 computers named TestKingSrvA.sales.testking.com and TestKingSrvA.prod.testking.com hold all operations master roles for their respective domains. WAN connectivity between the offices is unreliable.

You need to plan the placement of global catalog servers for the network. You need to ensure that each user can log on in the event of the failure of a single domain controller and WAN connection. You need to ensure that the consistency of universal group membership information remains intact.

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

- A. Configure both domain controllers in testking.com as global catalog servers.
- B. Configure only TestKingSrvA in each domain as a global catalog server.
- C. Configure only TestKingSrvB in each domain as a global catalog server.

- D. Enable universal group membership caching for each site.
- E. Enable universal group membership caching for the Buenos Aires office.
- F. Enable universal group membership caching for the Mexico City office and the Buenos Aires office.

Answer: A, F

Explanation: We need to ensure that the consistency of universal group membership information remains intact in the event of a WAN failure or a single domain controller failure. We can do this by having two global catalog servers in the same place. In order for the users in the other offices to log on in the event of a WAN failure, we should enable universal group membership caching for the Mexico City office and the Buenos Aires office.

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

Incorrect Answers:

B: With a global catalog server in each domain, we could lose the consistency of universal group membership information if the WAN link fails. For example, we could add someone to a universal group in one domain, but the other domains won't know about it if that information cannot be replicated due to a WAN link failure.

C: With a global catalog server in each domain, we could lose the consistency of universal group membership information if the WAN link fails. For example, we could add someone to a universal group in one domain, but the other domains won't know about it if that information cannot be replicated due to a WAN link failure.

D: We don't need universal group caching in the testking.com domain because there are global catalog servers in that domain.

E: We need to enable universal group membership caching for the Mexico City office and the Buenos Aires office, not just Buenos Aires.

QUESTION NO: 44

You are the network administrator for Acme Ltd. The company has a subsidiary named TestKing. The Acme Ltd network consists of a single Active Directory forest. The forest contains one domain named acme.com. The functional level of the domain is Windows Server 2003. The TestKing network consists of a single Windows NT 4.0 domain named TESTKING.

A file server named Server4 is a member of the acme.com domain. All users in both domains need to save files on Server4 every day.

You need to allow users in the TESTKING domain to access files on Server4. You need to ensure that the domain administrators of the TESTKING domain cannot grant users in the acme.com domain permissions on servers in the TESTKING domain.

What should you do?

- A. Upgrade the TESTKING domain to Windows Server 2003 and make this domain the root domain of a second tree in the existing forest.
- B. Upgrade the TESTKING domain to Windows Server 2003 and make this domain the root domain of a new forest.
Create a two-way forest trust relationship.
- C. Create a one-way external trust relationship in which the acme.com domain trusts the TESTKING domain.
- D. Create a one-way external trust relationship in which the TESTKING domain trusts the acme.com domain.

Answer: C

Explanation: We need a one-way external trust relationship in which the acme.com domain trusts the TESTKING domain. This will ensure that users who log on in the TESTKING domain will be able to access resources on server4 in the acme.com domain.

Incorrect Answers:

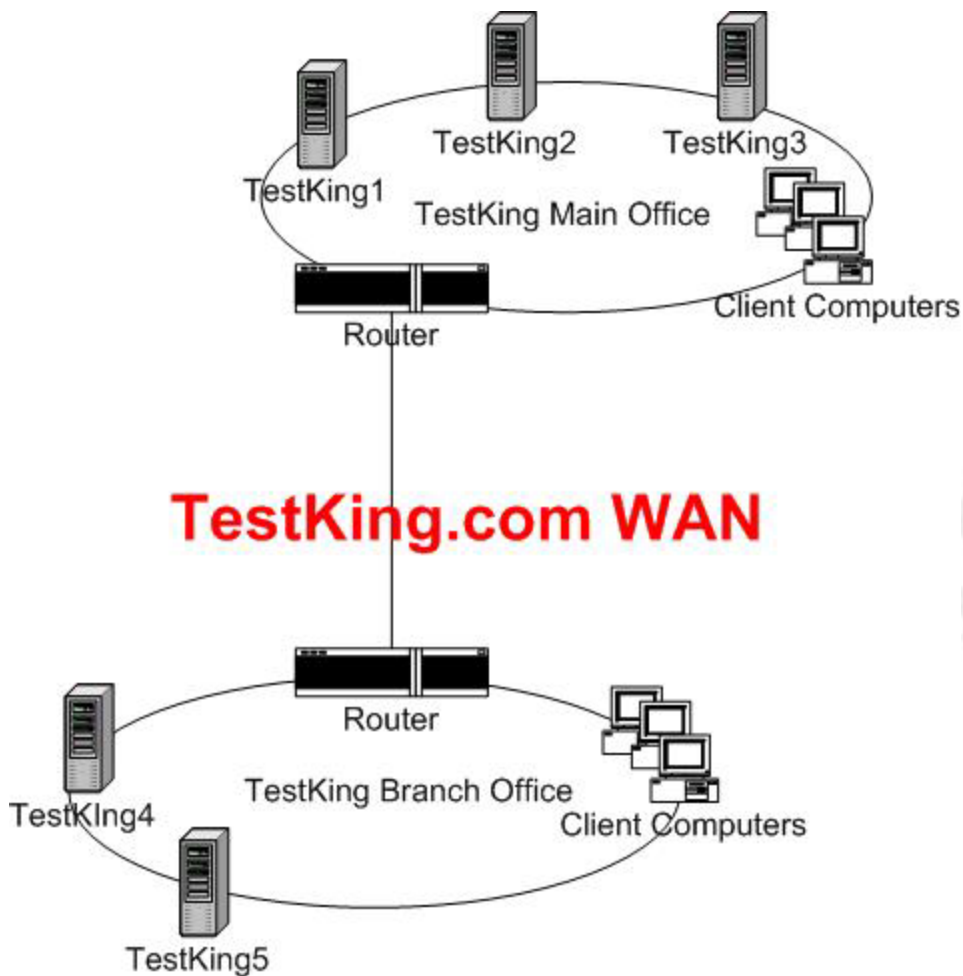
A: It is unnecessary to upgrade the Windows NT domain. Furthermore, this solution would establish two way transitive trusts with the acme.com domain. This means that the TESTKING domain administrator will be able to assign permissions to resources in the TESTKING domain to users from the acme.com domain.

B: It is unnecessary to upgrade the Windows NT domain. Furthermore, this solution would establish two way transitive trusts with the acme.com domain. This means that the TESTKING domain administrator will be able to assign permissions to resources in the TESTKING domain to users from the acme.com domain.

D: This trust is going in the wrong direction. This would enable the TESTKING domain administrator to assign permissions to resources in the TESTKING domain to users from the acme.com domain.

QUESTION NO: 45

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. The network contains three Windows Server 2003 domain controllers: TestKing1, TestKing2, and TestKing4. You configure two Active Directory sites, one for the main office and one for the branch office. The network is shown in exhibit.



The domain controllers are backed up each night by using a normal backup that also captures the system state.

You are responsible for creating a domain controller recovery plan to be used if a domain controller fails in either office. The design team specifies that the domain controller recovery plan must minimize replication traffic across the link between the network in the main office and the network in the branch office. The plan must also minimize restoration time.

You need to include in your recovery plan the process for restoring Active Directory services if any of the domain controllers suffers a hardware failure.

Which two actions should you include in your plan? (Each correct answer presents part of the solution. (Choose two))

- A. Restore the system state of any domain controller to an available member server in the same network subnet.

- B. Perform an authoritative restore operation on a functioning domain controller.
- C. On an available member server in the same network subnet as the failed domain controller, run the **dcpromo /adv** command and select the **Over the network** option.
- D. On an available member server in the same network subnet as the failed domain controller, run the **dcpromo /adv** command and select the **From these restored backup files** option.

Answer: A, D

Explanation: 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.

Incorrect Answers:

B: We don't want to authoritatively restore the data. There is also no need to restore anything to a functioning domain controller.

C: The **Over the network** option is incomplete. The full option is **Over the network from a domain controller**. We want to create a domain controller from the restored files.

QUESTION NO: 46

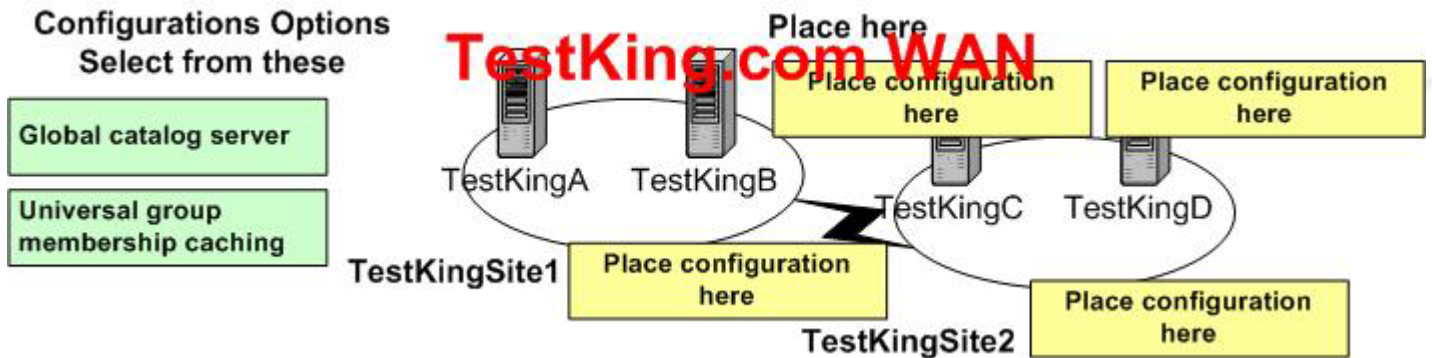
You are the network administrator for TestKing. The network consists of a single Active Directory forest that contains multiple domains. The functional level of the forest is Windows Server 2003.

The forest includes two Active Directory sites named TestKingSite1 and TestKingSite2. TestKingSite1 contains two domain controllers that are global catalog servers named TestKingA and TestKingB. TestKingSite2 contains two domain controllers that are not global catalog servers named TestKingC and TestKingD. The two sites are connected by a WAN connection. Users in TestKingSite2 report that logon times are unacceptably long.

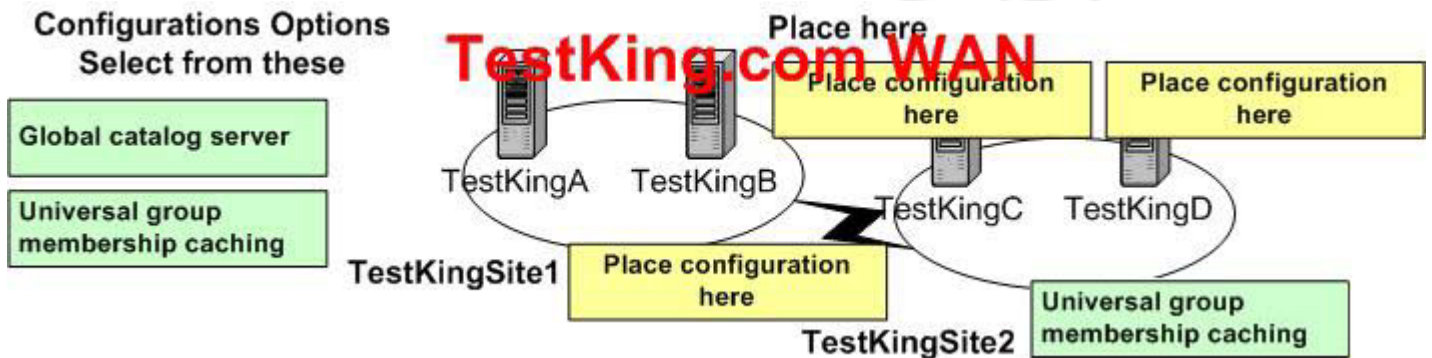
You need to improve logon times for the users in TestKingSite2 while minimizing replication traffic on the WAN connection.

How should you configure the network?

To answer, drag the appropriate configuration option or options to the correct location or locations in the work area.



Answer:



Explanation:

We need to improve logon times for the users in TestKingSite2 while minimizing replication traffic on the WAN connection. Logon times in TestKingSite2 are slow because the domain controllers need to contact a global catalog server in TestKingSite1 for universal group information. We can prevent this by enabling Universal group membership caching in TestKingSite2. Enabling Universal group membership caching at the site level will ensure that all the domain controllers in TestKingSite2 will be able to cache the information. We could improve logon times by placing a global catalog server in TestKingSite2 but this will increase replication between the two sites; therefore enabling Universal group membership caching is a better solution.

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.

QUESTION NO: 47

You are the network administrator for TestKing. The company is deploying a network that consists of a single Active Directory domain named testking.com. All client computers run Windows XP Professional.

You are planning the data transmission security for the sales department.

You need to monitor the data transmissions to and from the client computers in the sales department at all times. You need to ensure the integrity of the data transmissions to and from the client computers. You also need to be able to implement intrusion detection on the sales department traffic.

What should you do?

- A. Assign a custom IPSec policy with the Integrity and Encryption security method to the sales department client computers.
- B. Assign a custom IPSec policy with the Integrity only security method to the sales department client computers.
- C. Assign a custom IPSec policy with a custom security method and the 3DES encryption algorithm to the sales department client computers.
- D. Assign the Client (Respond Only) IPSec policy to the sales department client computers.

Answer: B

Explanation: We want to monitor IPSEC traffic. We can not use ESP; if we did, we wouldn't be able to monitor the IPSEC traffic because it is encrypted. **If you need to diagnose ESP software-encrypted communication, you must disable ESP encryption and use ESP-null encryption by changing the IPSec policy on both computers.**

We need to use AH; this way we can monitor network traffic and preserve the integrity of messages.

Using both AH and ESP is the only way to both protect the IP header and encrypt the data. However, this level of protection is rarely used because of the increased overhead that AH would incur for packets that are already adequately protected by ESP. ESP protects everything but the IP header, and modifying the IP header does not provide a valuable target for attackers. Generally, the only valuable information in the header is the addresses, and these cannot be spoofed effectively because ESP guarantees data origin authentication for the packets

Protocol	Requirement	Usage
AH	The data and the header need to be protected from modification and authenticated, but remain readable.	Use for data integrity in situations where data is not secret but must be authenticated — for example, where access is enforced by IPSec to trusted computers only, or where network intrusion detection, QoS, or firewall filtering requires traffic inspection.

ESP	Only the data needs to be protected by encryption so it is unreadable, but the IP addressing can be left unprotected.	Use when data must be kept secret, such as file sharing, database traffic, RADIUS protocol data, or internal Web applications that have not been adequately secured by SSL.
Both AH and ESP	The header and data, respectively, need to be protected while data is encrypted.	Use for the highest security. However, there are very few circumstances in which the packet must be so strongly protected. When possible, use ESP alone instead.

IPSEC MONITOR

Use the IP Security Monitor snap-in to gather information you can use to identify problems and optimize performance where IPsec is deployed. For example, you can view details about IPsec policies and filters, statistics about performance, and SAs.

IP Security Monitor allows you to view details about the active IPsec policies that are applied to the domain, the local computer, or a remote computer.

Viewing IPsec and other network communication with Network Monitor

You can install and use Network Monitor to view IPsec and other network communication. Note that the version of Network Monitor that is provided with the Windows Server 2003 family can be used only to view the network traffic that is sent to or from the computer on which it is installed. To view network traffic that is sent to or from another computer and is routed through your computer (using the Routing and Remote Access service), you must use the Network Monitor component that is provided with Microsoft Systems Management Server.

The Network Monitor component that is provided with the Windows Server 2003 family includes parsers for the ISAKMP (IKE), AH, and ESP protocols. The Network Monitor parsers for ESP can parse inside the ESP packet only if null-encryption is being used and the full ESP packet is captured. Network Monitor cannot parse the encrypted portions of IPsec-secured ESP traffic when encryption is performed in software. However, if encryption is being performed by an IPsec hardware offload network adapter, the ESP packets are decrypted when Network Monitor captures them and as a result, can be parsed and interpreted into the upper-layer protocols. **If you need to diagnose ESP software-encrypted communication, you must disable ESP encryption and use ESP-null encryption by changing the IPsec policy on both computers.**

References:

Server HELP

- Troubleshooting tools
- Viewing details about active IPsec policies in IP Security Monitor

MS Windows Server 2003 Deployment

Choosing the IPSec Protocol

QUESTION NO: 48

You are a system engineer for TestKing. The network consists of four Active Directory domains. All servers on the network run Windows Server 2003. The Windows Server 2003 computers are distributed among three offices. All servers support out-of-band management by means of serial connections to terminal concentrators in each office's data center. Each office maintains its own separate connection to the Internet.

The company adopts a new written security policy, which includes the following requirements:

- Physical access to all servers is restricted to authorized personnel and only for the purpose of installing or maintaining hardware.
- All in-band remote administration connections must be authenticated by the Kerberos version 5 protocol.
- Administrators in each office must be able to access their servers for remote administration or troubleshooting even when the operating system is not running or experiences a Stop error.
- Services or programs that are not essential for remote administration or server operation must not be installed on any computer.

You need to plan a remote administration strategy for the network that compiles with the new policy. You are not responsible for permissions management in the domains.

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

- A. Configure each server to accept Remote Desktop connections.
- B. On each server, enable the Telnet service with a startup parameter of **Automatic**.
- C. Install Terminal Services on each server.
- D. On each server, enable Emergency Management Services.
- E. Install IIS on each server.

Select the **Remote Administration (HTML)** check box in the properties for the Wide World Web Service.

Answer: A, D

Explanation:

Emergency Management Services is a new feature in Windows Server 2003 that permits you to perform remote management and system recovery tasks when the server is not available by using the standard remote

administration tools and mechanisms. Emergency Management Services provides alternative access to a server when the server is not accessible through the standard connection methods, typically a network.

With Emergency Management Services, combined with the appropriate hardware, you can perform remote management and system recovery tasks, even when the server is not available through the standard remote administration tools and mechanisms.

To manage a server from a remote computer when the server is not available on the network, you must enable Emergency Management Services. Emergency Management Services is a Windows Server 2003 service that runs on the managed server. This service is not enabled by default when you install the Windows Server 2003 operating system, but you can enable it during installation or at any later time.

Emergency Management Services features are available when the Windows Server 2003 loader or kernel is at least partially running. You can access all Emergency Management Services output by using terminal emulator software that supports VT100, VT100+, or VT-UTF8 protocols on the management computer, although VT-UTF8 is the preferred protocol. For more information about terminal emulator software and the supported protocols

Management Software for Out-of-Band Connections

Typically, you use terminal emulation software on the management computer to connect to and communicate with a server through an out-of-band connection. The two most common methods are the following:

- Use Telnet — or a secure alternative such as SSH — to connect to a terminal concentrator through an in-band connection, which then connects to the server through an out-of-band connection.
- Use HyperTerminal to connect directly to the server

When Emergency Management Services is enabled:

- Console redirection automatically sends output to the out-of-band port for any supported operating state,

Task

Selecting operating system during system load

Running Recovery Console

Viewing text mode setup messages

Viewing GUI mode setup messages

Viewing RIS loading messages

Viewing Stop error messages

Monitoring and managing with out-of-band connections

Performing last-resort system recovery

Feature

Console redirection

Console redirection

Console redirection

SAC, including setup logs

Console redirection

Console redirection

SAC

!SAC

- You can use SAC to issue supported commands or switch to the command shell (cmd.exe) whenever the kernel is running.
- You can view logs during the GUI-mode phase of Setup.
- !SAC automatically becomes available whenever a system failure occurs.

Remote Administration using Terminal Services

In Microsoft® Windows® Server 2003 family operating systems, Terminal Services technology is the basis for several features that enable you to connect to remote computers and perform administrative tasks.

- **Remote Desktop for Administration** (formerly known as Terminal Services in Remote Administration mode) provides remote server management capabilities for Windows Server 2003 family operating systems. Using this feature, you can administer a server from virtually any computer on your network. **No license is required for up to two simultaneous remote connections in addition to the server console session.** A corresponding desktop version of Remote Desktop for Administration is available on Microsoft® Windows® XP Professional, and is called Remote Desktop.
- The Remote Desktops MMC snap-in allows you to create remote connections to the console session of multiple terminal servers, as well as computers running Windows 2000 or Windows Server 2003 family operating systems.

- Remote Desktop Connection, available on Windows Server 2003 family operating systems as well as on Microsoft® Windows® XP operating systems, enables you to log on to a remote computer and perform administrative tasks, even from a client computer that is running an earlier version of Windows.

References:

MS Knowledge Base article 815273

HOW TO: Perform an Unattended Emergency Management Services Installation of Windows Server 2003

MS Windows Server 2003

Planning Server Deployments

Emergency Management Services

Server help

QUESTION NO: 49

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

You install a wireless network. You discover that the coverage for the executive offices is very poor. You need to improve wireless coverage for the executive team in their office area.

The design team specifies the following requirements for the executive team:

- Executives must be able to access the wireless network in all locations in the building, including their offices.
- Non executive employees may use wireless access points in the executive office area only if other access points are unavailable.

You need to develop a plan to improve the coverage in the executive offices. You need to implement your plan by using the minimum amount of administrative effort.

What should you do?

- A. Use the Connection Manager Administration Kit (CMAC) wizard to create new service profiles. One profile will be used for executives only. Send an e-mail message that contains the proper profiles to the proper users.
- B. Use the Windows Management Instrumentation command-line tool with the NIC and the NICCONFIG aliases.
- C. Install new access points for the executive team with a new dedicated service set identifier (SSID).

Use wireless network policies to control use of the SSIDs on the wireless network.

D. Install new access points for the executive team with a new dedicated service set identifier (SSID).

Use wireless network policies to control access for ad hoc networks.

Answer: C

Explanation

The **Network name (SSID)** specifies the name for the specified wireless network. Under the IEEE 802.11 standard, the network name is also known as the Service Set Identifier (SSID).

We will need to setup two different **Network name (SSID)s**, one for users and one for executives. Also we can to enhance the deployment and administration of wireless networks, using a Group Policy to centrally create, modify, and assign wireless network policies for Active Directory clients.

Reference:

MS Windows Server 2003 Deployment Kit: Designing a Managed Environment

QUESTION NO: 50

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. 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 out-of-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}	Comx (where <i>x</i> 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= <i>value</i>	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: 51

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.

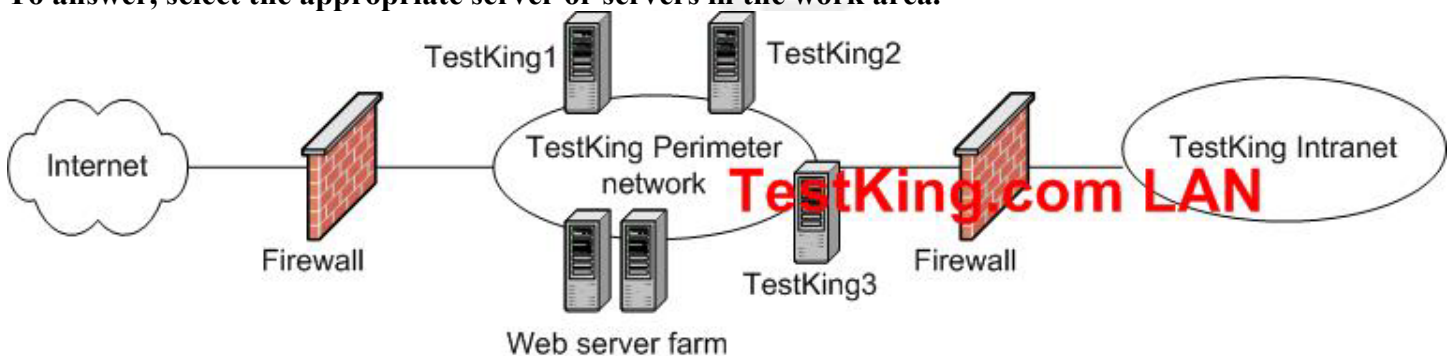
All servers on the perimeter network are members of the same workgroup.

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: 52

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: 53

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		
Bytes Total/sec	AMD PCNET Family PCI Ethernet Adapter	21230,359
Paging File		
% Usage	\\??\C:\pagefile.sys	86,670
PhysicalDisk		
% Disk Time	_Total	93,610
Processor		
% Processor Time	_Total	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	15%	
	Logical Disk\%		

Leading the way in IT testing and certification tools, www.testking.com

	Free Space		
	Physical Disk\\%		
Disk	Disk Time	90%	
	Logical Disk\\%		
	Disk Time		
	Physical	Depends	
Disk	Disk/Disk	on	
	Reads/sec,	manufactu	Check the specified transfer rate for your disks to verify that this rate
	Physical	rer's	does not exceed the specifications. In general, Ultra Wide SCSI disks
	Disk/Disk	specificati	can handle 50 to 70 I/O operations per second.
	Writes/sec	ons	
	Physical		
Disk	Disk/Current	Number of	This is an instantaneous counter; observe its value over several intervals.
	Disk Queue	spindles	For an average over time, use Physical Disk/Avg. Disk Queue Length.
	Length	plus 2	
Memor	Memory\Availabl	Less than	
y	e Bytes	4 MB	Research memory usage and add memory if needed.
Memor	Memory\Pages/se	20	Research paging activity.
y	c		
Paging	Paging File\\%	Above	Review this value in conjunction with Available Bytes and Pages/sec to
File	Usage	70%	understand paging activity on your computer.
Process	Processor\\%		
or	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.
		Depends	
		on	
Process	Processor\Interru	processor;	
or	pts/sec	1000	A dramatic increase in this counter value without a corresponding
		interrupts	increase in system activity indicates a hardware problem. Identify the
		per second	network adapter causing the interrupts. You might need to install an
		is a good	additional adapter or controller card.
		starting	
		point	
Server	Server\Bytes		If the sum of Bytes Total/sec for all servers is roughly equal to the
	Total/sec		maximum transfer rates of your network, you might need to segment the
			network.
			If the value reaches this threshold, consider adding the DWORD entries
Server	Server\Work Item	3	InitWorkItems (the number of work items allocated to a processor
	Shortages		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\Lan
			manServer\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: 54

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 adapter. The cluster has converged successfully.

You notice that the nodes in the cluster run at almost full capacity most of the time. You want to add a fourth node to the cluster. You enable and configure Network Load Balancing on the fourth node.

However, the cluster does not converge to a four-node cluster. In the System log on the existing three nodes, you find the exact same TCP/IP error event. The event has the following description: "The system detected an address conflict for IP address 10.50.8.70 with the system having network hardware address 02:BF:0A:32:08:46."

In the System log on the new fourth node, you find a similar TCP/error event with the following description: "The system detected an address conflict for IP address 10.50.8.70 with the system having network hardware address 03:BF:0A:32:08:46." Only the hardware address is different in the two descriptions.

You verify that IP address 10.50.8.70 is configured as the cluster IP address on all four nodes.

You want to configure a four-node Network Load Balancing cluster.

What should you do?

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

Answer: A

Explanation: This normally happens when you don't enable the network load balancing service in TCP/IP of the server when adding two IP's (one for the server and one for the load balancing IP).

When you want to manage a NLB cluster with one network adapter you use multicast option.

My idea is since reload/suspend and remove the IP are all garbage answers could be that the other nodes are using multicast and this new node is using unicast that's why on a single network adapter configuration it will cause an IP conflict.

Reference: Syngress 070-293, Page 689

QUESTION NO: 55

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: 56

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

Place third action here

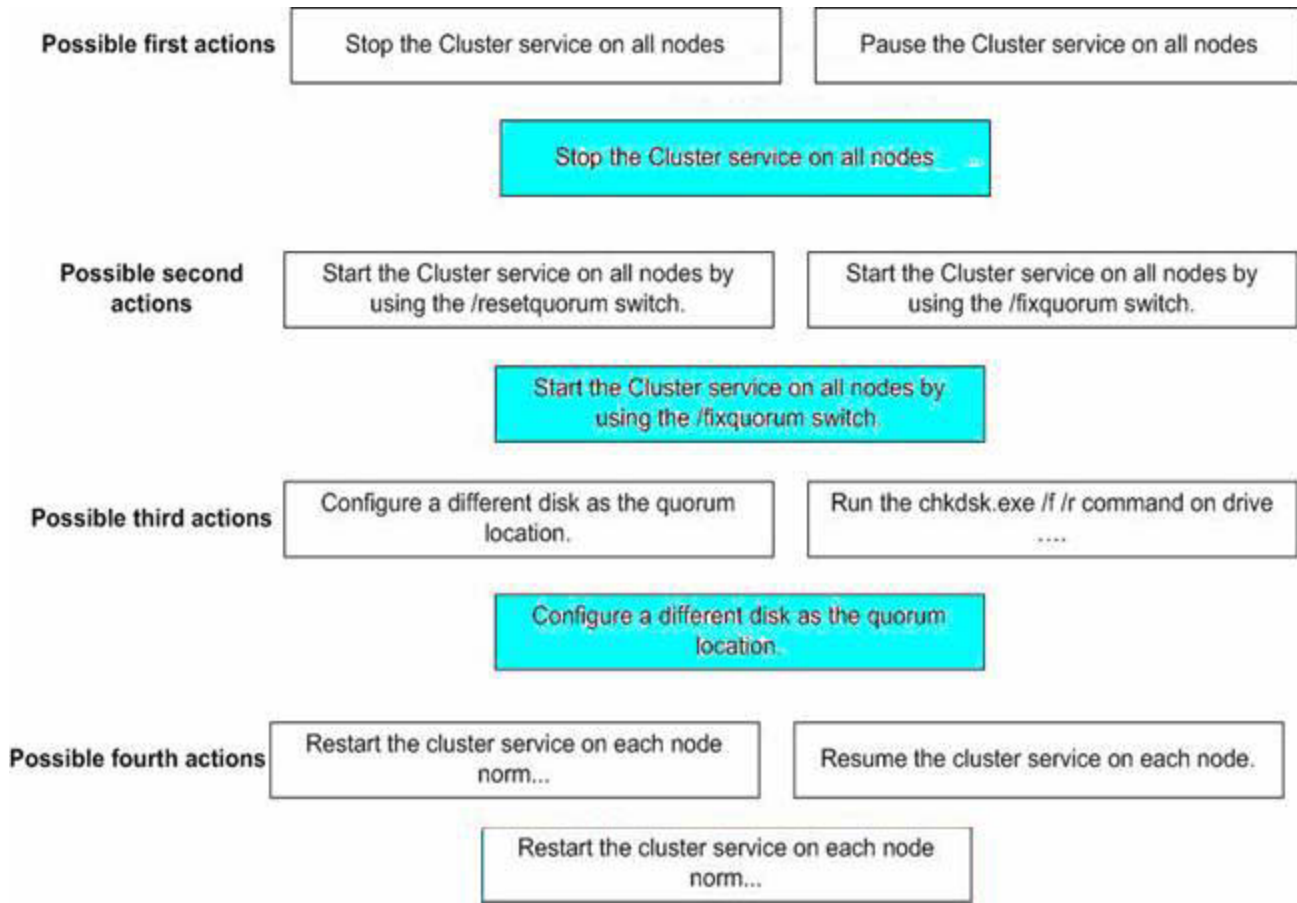
Possible fourth actions

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: 57

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: 58

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

Explanation: The permission **Allow – Issue and Manage Certificates** will enable the Cert Approvers group to issue the certificates.

QUESTION NO: 59

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:
-

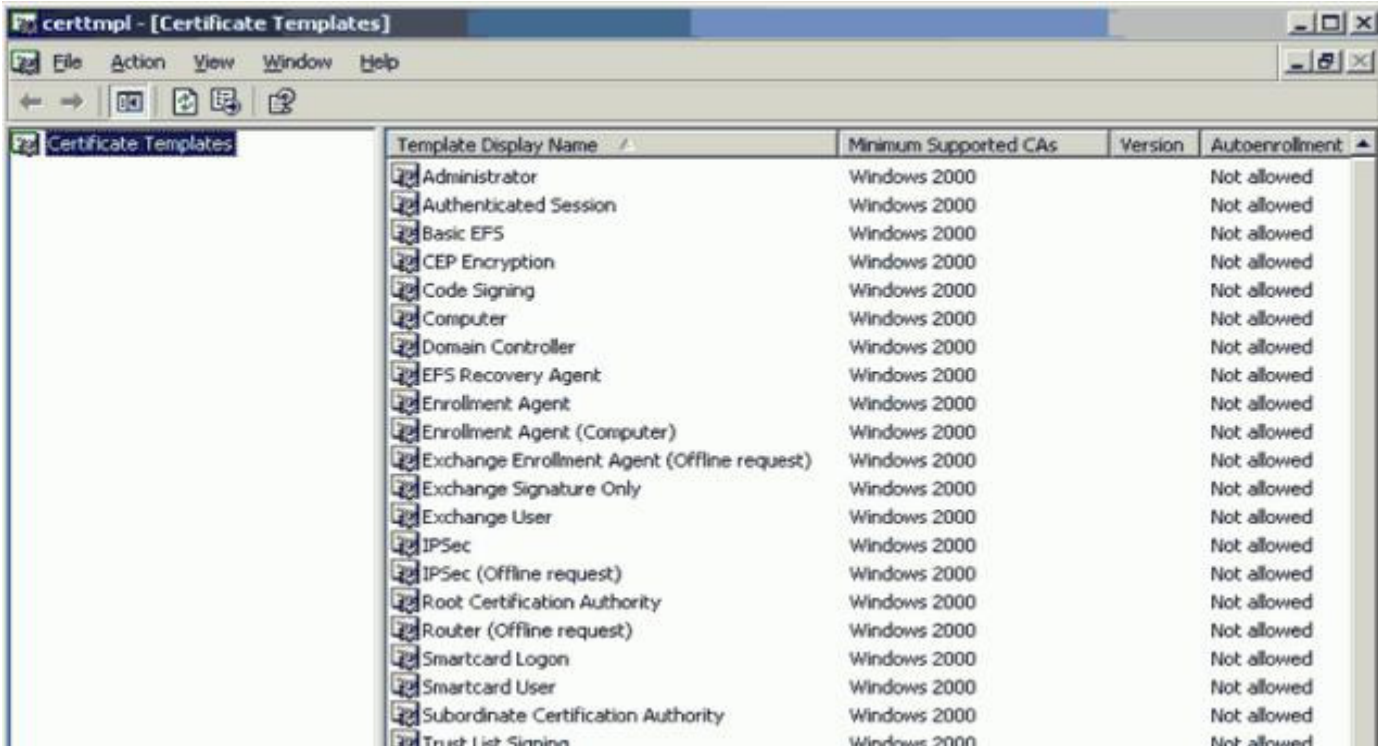
Setting	Affect on autoenrollment behavior
Enroll subject without requiring any user input	This setting will allow "silent" autoenrollment without requiring the user to take any action. This setting is preferred when clients require certificates but may not be aware that they are using them.
Prompt the 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	
<ul style="list-style-type: none"> 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: 60

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: 61

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.

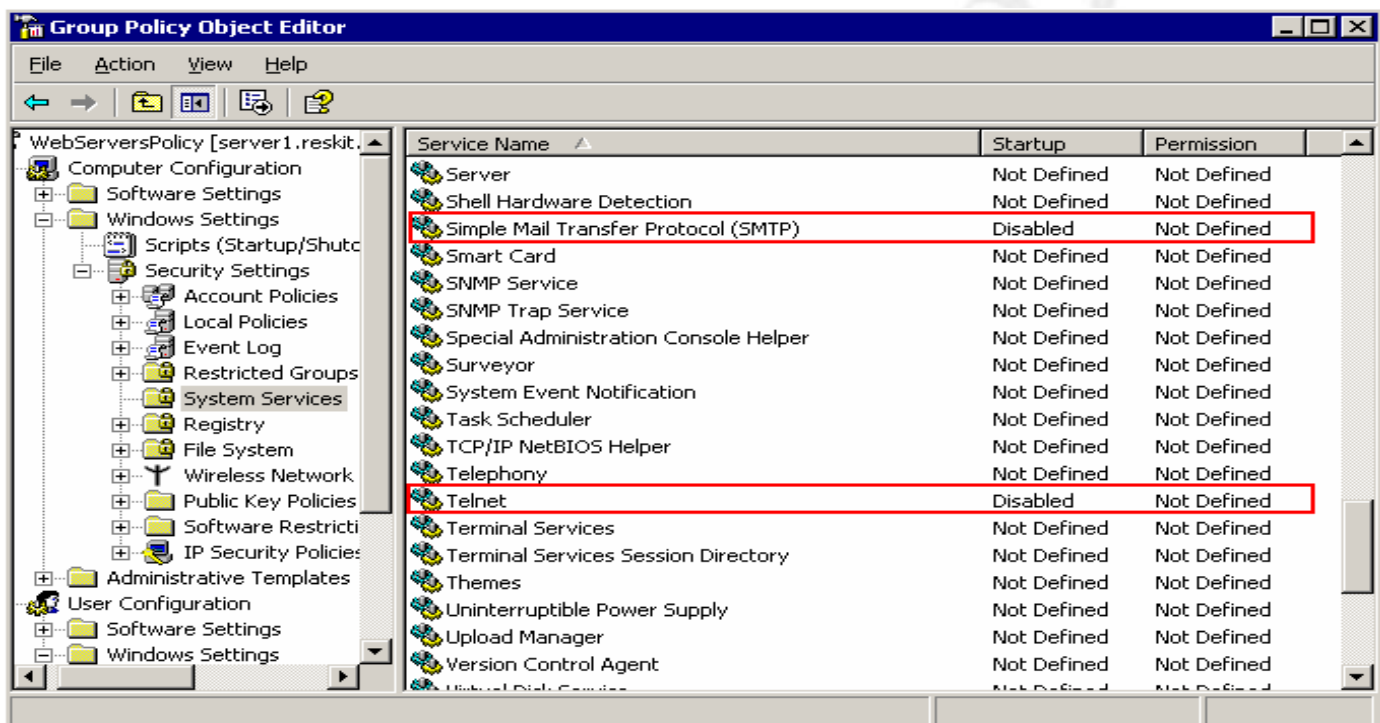
What should you do?

- 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: 62

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 be easier to link the GPO to a single parent OU.

QUESTION NO: 63

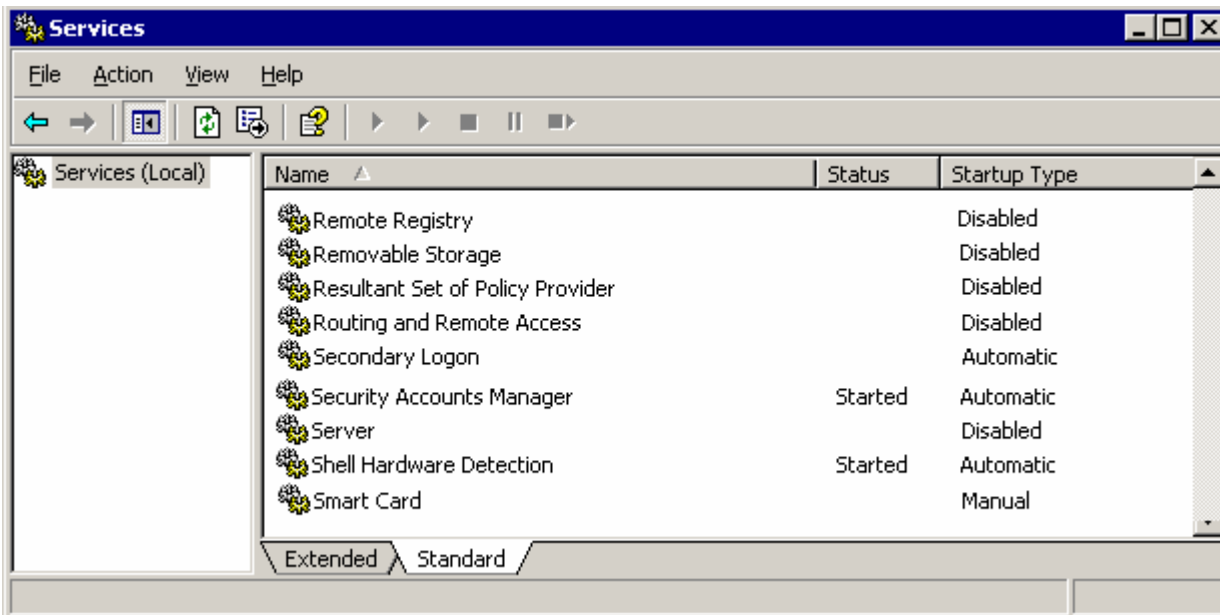
You are the network administrator for TestKing. The network consists of a single Active Directory domain named testking.com. The network contains a Windows Server 2003 member server named TestKingSrvA. The network also contains a Windows XP Professional computer named Client1. You use Client1 as an administrative 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

Reference MS White Paper Baseline Security Analyzer

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/mbsaqa.asp>

The following are the requirements for a computer to be scanned remotely by the tool:

- Windows NT 4.0 SP4 and above, Windows 2000, Windows XP (local scans only on Windows XP computers that use simple file sharing), or Windows Server 2003
- IE 5.01 or greater
- 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 desktop application vulnerability checks)
- **The following services must be installed/enabled: Server service, Remote Registry service, File & Print Sharing**

QUESTION NO: 64

You are the network administrator for TestKing. The network consists of a single Active Directory domain named testking.com. The network contains 10 application servers that run Windows Server 2003.

The application servers are accessed from the TestKing network and from the Internet. The network design requires that the application servers must have specifically configured security settings, including

Leading the way in IT testing and certification tools, www.testking.com

the password policy, audit policies, and security options settings. You create a security template named App.inf that contains the security settings required by the network design.

You are concerned that an unauthorized user will modify the configuration and gain access to the application servers. You want to capture any changes made to the security settings of the application servers.

You need to generate a report that compares the current settings of each application server with the required settings every 24 hours.

What should you do?

- A. Use a Group Policy startup script to run the **secedit** command in analysis mode with the App.inf template, and set the Group Policy refresh interval for computers to 24 hours.
- B. Import the App.inf template into Group Policy, and set the Group Policy refresh interval for computers to 24 hours.
- C. Use Task Scheduler to run the **gpresult** command in verbose mode every 24 hours.
- D. Use a custom script in Task Scheduler to run the secedit command in analysis mode with the App.inf template every 24 hours.

Answer: D

Explanation: The gpresult utility is a command line version of the RSoP utility. In verbose mode, it will list the effective policies on a computer. We can use the Task Scheduler to run the gpresult command every 24 hours. We can then examine the output to verify that the correct settings are applied.

Incorrect Answers:

- A:** A Group Policy startup script will only run when the computer starts up. It does not run every time the group policy is refreshed.
- B:** This will reapply the required settings every 24 hours, but the question states that you want to capture any changes by comparing the current settings to the required settings.
- C:** The gpresult utility is a command line version of the RSoP utility. In verbose mode, it will list the effective policies on a computer. However, it won't list the differences between the current settings and the required settings.

QUESTION NO: 65

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: 66

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: 67

Leading the way in IT testing and certification tools, www.testking.com

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: 68

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 adapter in each server to a separate network switch.
Connect the management port on the switch to a WAN port on the office router.
Enable IPSec on the router.
- C. Enable Routing and Remote Access on a server in each branch office, and configure it as an L2TP/IPSec VPN server.
Configure a remote access policy to allow only authorized administrative staff to make a VPN connection.
- D. On each server, enable the Telnet service with a startup parameter of **Automatic**.
Configure Telnet on each server to use only NTLM authentication.
Apply the Server (Request Security) IPSec policy to all servers.

- E. On each server, enable Emergency Management Services console redirection and the Emergency Management Services Special Administration Console (SAC).

Answer: A, C, E

Explanation:

Special Administration Console Helper

You can use the Special Administration Console Helper system service to perform remote management tasks if the Windows Server 2003 family operating system stops functioning due to a Stop error message.

The main functions of Special Administration Console (!SAC) are to:

- Redirect Stop error message explanatory text
- Restart the system
- Obtain computer identification information

The !SAC is an auxiliary Emergency Management Services command – line environment that is hosted by Windows Server 2003 family operating systems. It also accepts input, and sends output through the out – of – band port. SAC is a separate entity from both !SAC and Windows Server 2003 family command – line environments.

After a specific failure point is reached, Emergency Management Services components determine when the shift should be made from SAC to !SAC. !SAC becomes available automatically if SAC fails to load or is not functioning.

If the Special Administration Console Helper service is stopped, SAC services will no longer be available. If this service is disabled, any services that explicitly depend on this service will not start.

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

Terminal concentrators

A terminal concentrator is a hardware device that consolidates serial access to multiple servers into a single networked device. You can use this device to monitor a large number of servers simultaneously from one location.

Terminal concentrators include many serial ports serial ports

An interface on the computer that allows asynchronous transmission of data characters one bit at a time. Also called a *communication port* or *COM port*.

connected to multiple servers using null modem cables

null modem cables

Special cabling that eliminates the modem's need for asynchronous communications between two computers over short distances. A null modem cable emulates modem communication.

Typically, you access terminal concentrators over the network through the Telnet Telnet

A protocol that enables an Internet user to log on to and enter commands on a remote computer linked to the Internet, as if the user were using a text-based terminal directly attached to that computer. Telnet is part of the TCP/IP suite of protocols. The term *telnet* also refers to the software (client or server component) that implements this protocol.

protocol. Terminal concentrators provide an interface through which you can remotely view data on multiple servers that use serial ports as their out-of-band connection
out-of-band connection

A connection between two computers that relies on a nonstandard network connection, such as a serial port connection, and nonstandard remote administration tools, such as Special Administration Console (SAC). An out-of-band connection is usually used only when a remote computer cannot access a network or is not in a functional state because of hardware or software failure.

Terminal concentrators can improve your management of servers because they can establish in-band connections to the servers and then perform out-of-band management tasks. In addition, terminal concentrators make it easier to manage servers for the following reasons:

- You can use terminal concentrators to manage multiple servers without needing to be within a serial cable's distance to the computer.
- Several administrators can simultaneously view the output of different servers.
- Using an out-of-band connection, you can use terminal concentrators to monitor servers methodically. You can also manage multiple servers from one location.

Several companies manufacture terminal concentrators; their setup, features, and configuration details vary.

When assessing the appropriateness of a particular terminal concentrator, consider the following:

- The number of serial ports available.
- Built-in Telnet security features, such as passwords.
- Remote-access capabilities.
- The number of Ethernet

Ethernet

The IEEE 802.3 standard that uses Carrier Sense Multiple Access with Collision Detection (CSMA/CD) as the medium access control. Ethernet supports different mediums, such as coaxial cable, fiber-optic cable, and twisted-pair wiring, and different data rates, such as 10 megabits per second (Mbps).
ports available.

Telnet security features are not standard across terminal concentrators.

If your device does not include security features, consider using a secondary private management network accessible through a direct-dial remote access connection or a virtual private network (VPN)

Make sure that the terminal emulation software you use supports serial port and terminal definition settings that are compatible with Emergency Management Services, as well as with your service processor or system firmware. If possible, use terminal emulation software that supports the VT-UTF8 protocol because VT-UTF8 support for Unicode provides for multilingual versions of Windows. If English is the only language you need to support, the VT100+ terminal definition is sufficient. At minimum, you can use the VT100

definition, but this terminal definition requires that you manually enter escape sequences for function keys and so forth.

virtual private network (VPN)

The extension of a private network that encompasses encapsulated, encrypted, and authenticated links across shared or public networks. VPN connections can provide remote access and routed connections to private networks over the Internet.

connection. You can also use a router

router

Hardware that helps local area networks (LANs) and wide area networks (WANs) achieve interoperability and connectivity and that can link LANs that have different network topologies (such as Ethernet and Token Ring). Routers match packet headers to a LAN segment and choose the best path for the packet, optimizing network performance.

to secure network traffic going to the terminal concentrator.

References:

Server Help

QUESTION NO: 69

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 policies.

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.

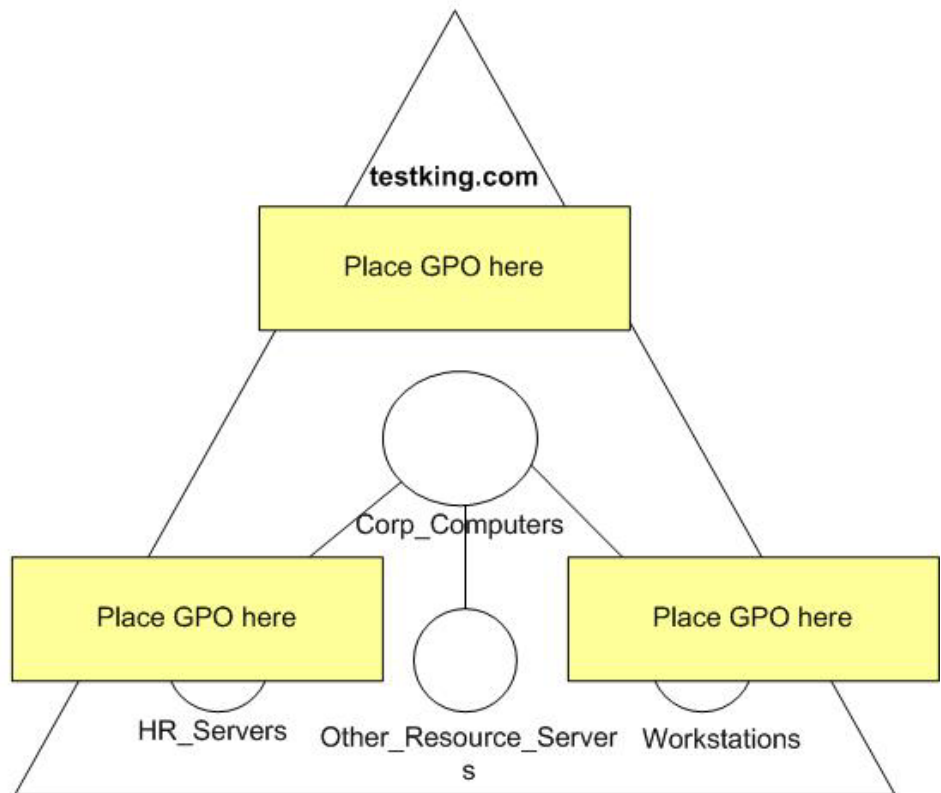
GPOs

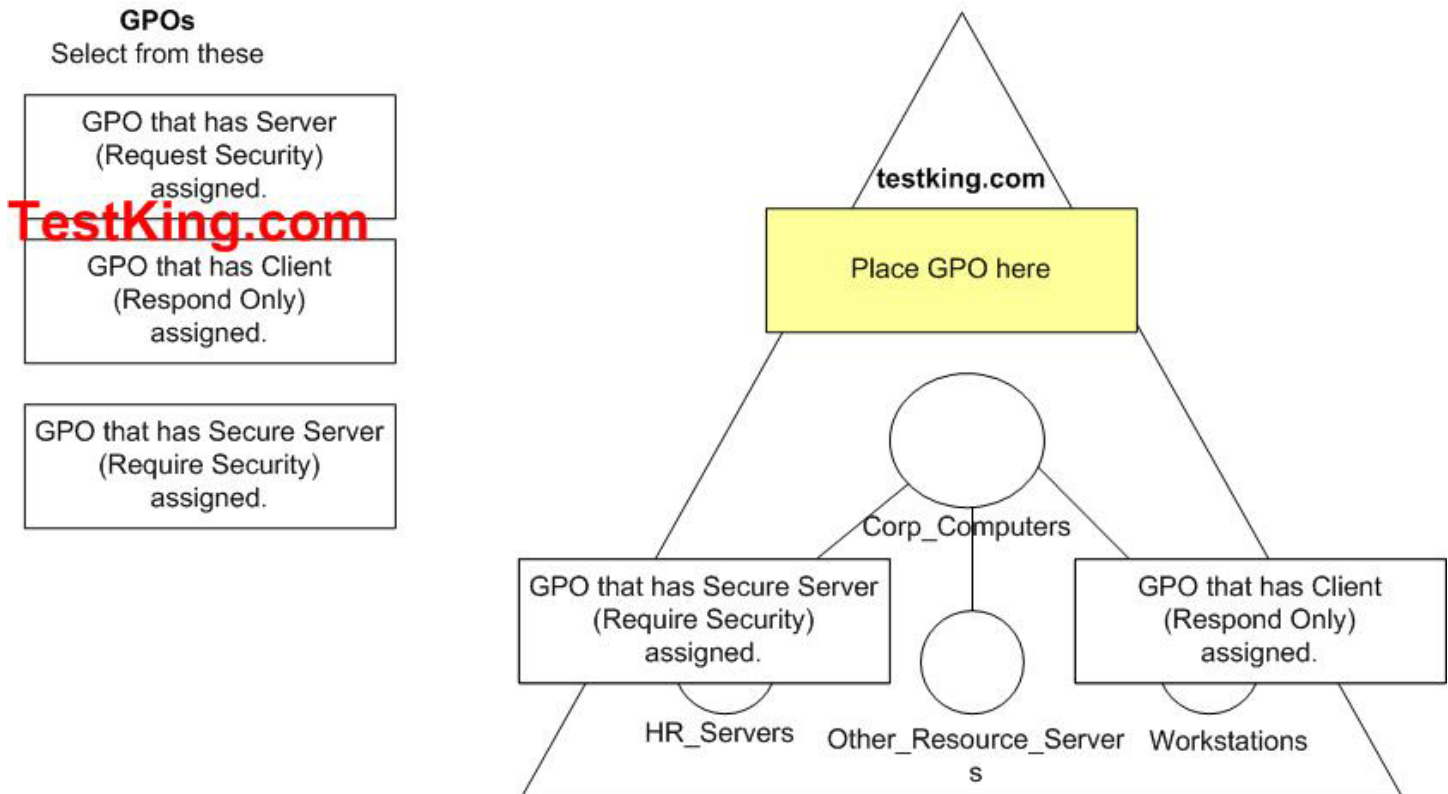
Select from these

GPO that has Server
(Request Security)
assigned.

GPO that has Client
(Respond Only)
assigned.

GPO that has Secure Server
(Require Security)
assigned.

**Answer:**



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

IPSEC for High security

Computers that contain highly sensitive data are at risk for data theft, accidental or malicious disruption of the system (especially in remote dial-up scenarios), or any public network communications.

Understanding Default IPSec Policies

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

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

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

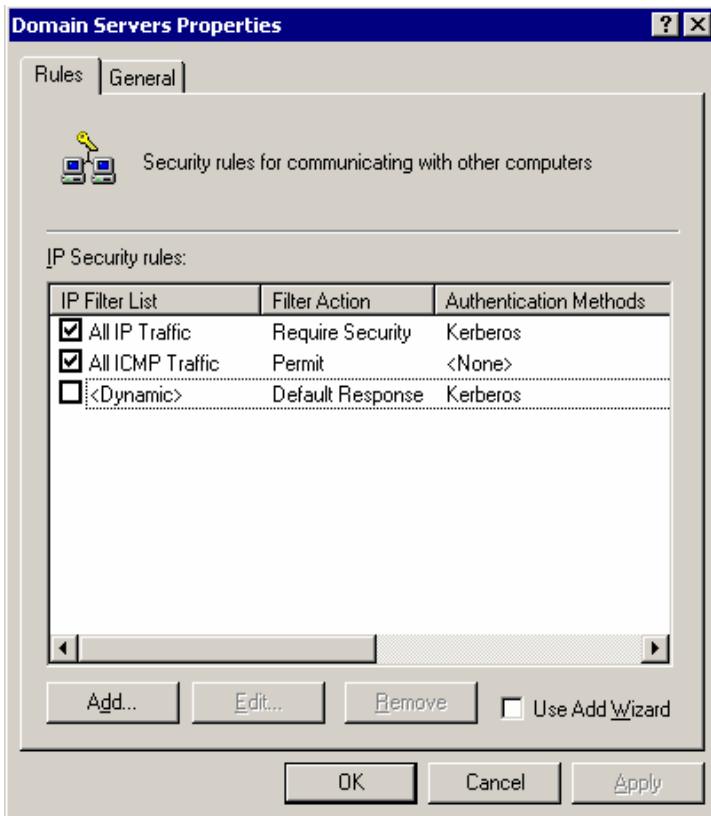
Reference

Server Help

QUESTION NO: 70

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.

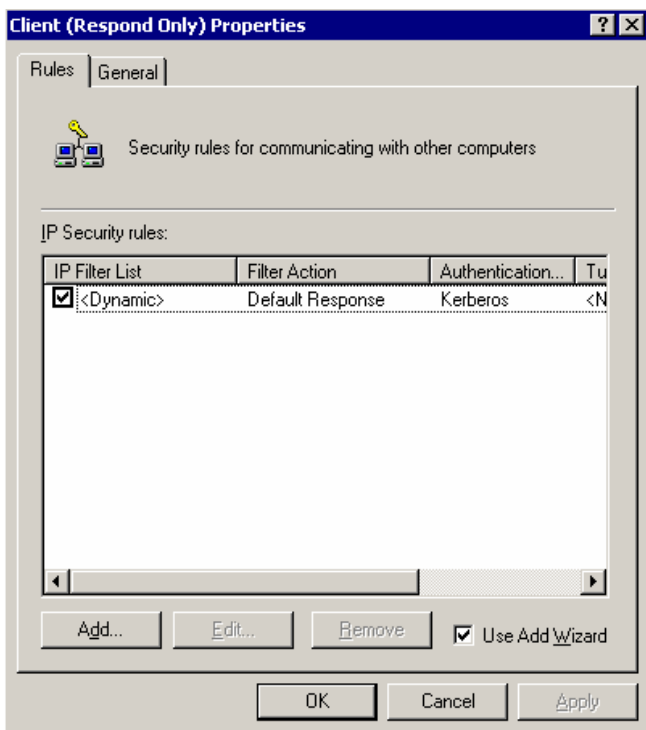
What should you do?

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

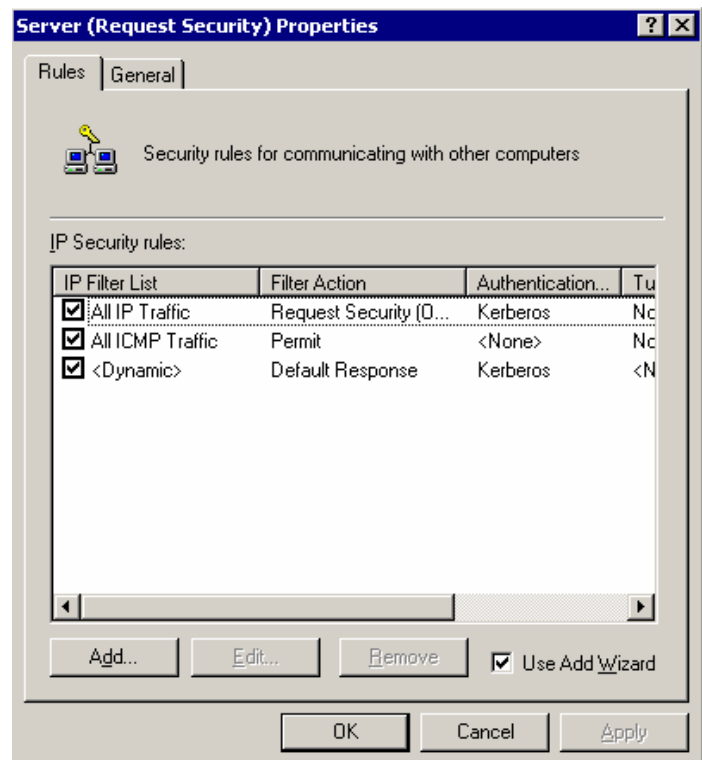
Answer: B

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.

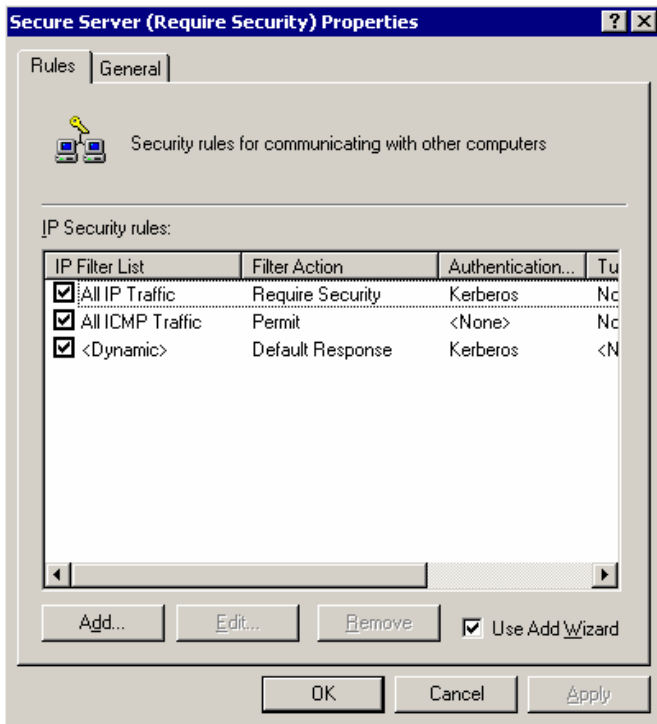
Client Only Default Response Picture



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.

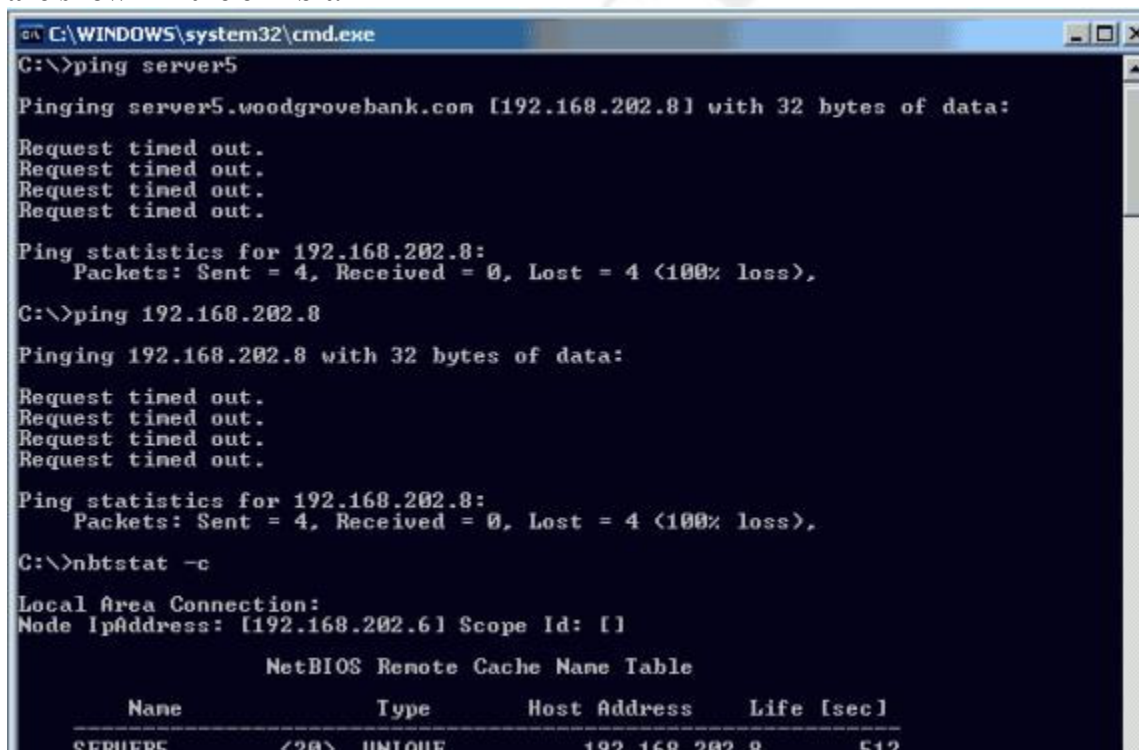
Reference Server Help

QUESTION NO: 71

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: In the exhibit, you pinged using the fully qualified domain name. The exhibit shows that DNS has resolved the hostname to 192.168.202.8. The NBTstat command also shows that the NetBIOS cache has cached the IP address of 192.168.202.8. However, pinging the IP address 192.168.202.8 failed. It is likely that the IP address of Server5 has changed but WINS and DNS still have the old address. We can fix this by reregistering Server5 with WINS and running the **ipconfig** command with the **/registerdns** option to update the DNS record.

QUESTION NO: 72

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 its 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 effect.

QUESTION NO: 73

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: C

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
 - $12 \times 220 = 2640$

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: 74

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.

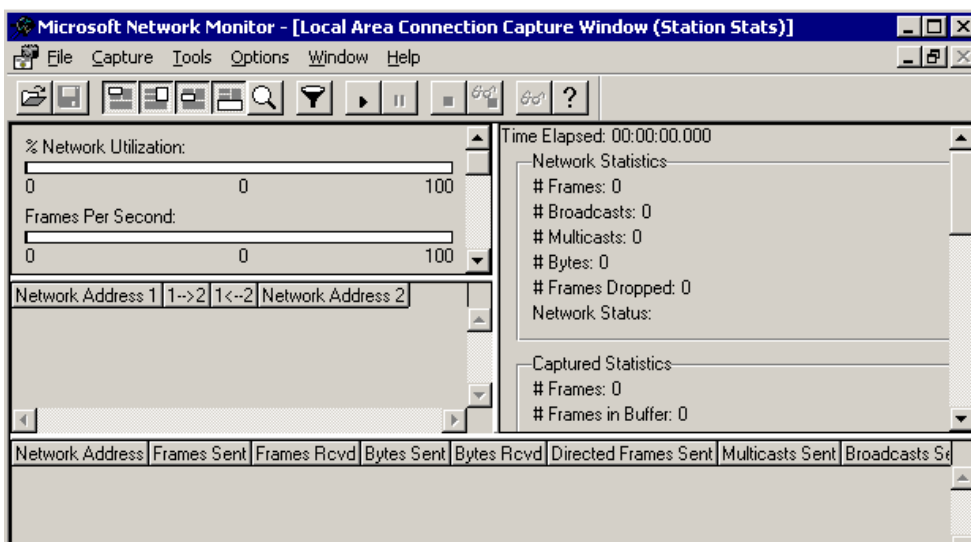
This command-line tool allows a system administrator to monitor packets on a LAN and write the information to a log file. NetCap uses the Network Monitor Driver to sniff packets on local network segments.

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.



www.testking.com

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: 75

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: 76

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: 77

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.

Connection Types:	All network connections	LAN	Remote access
	Place connection type here		
IP Filter Lists	All ICMP traffic	All IP Traffic	
	Place IP Filter here		
Filter Actions	Permit	Server (Request Security)	Secure Server (Require Security)
	Place Filter action here		
Authentication Methods	Kerberos	Certificate	Preshared key
	Place Authentication Method here		

Answer:

TestKing.com

Connection Types:	All network connections	LAN	Remote access
IP Filter Lists	All ICMP traffic	All IP Traffic	
Filter Actions	Permit	Server (Request Security)	Secure Server (Require Security)
Authentication Methods	Kerberos	Certificate	
		Preshared key	

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: 78

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 policies 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 policies 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:

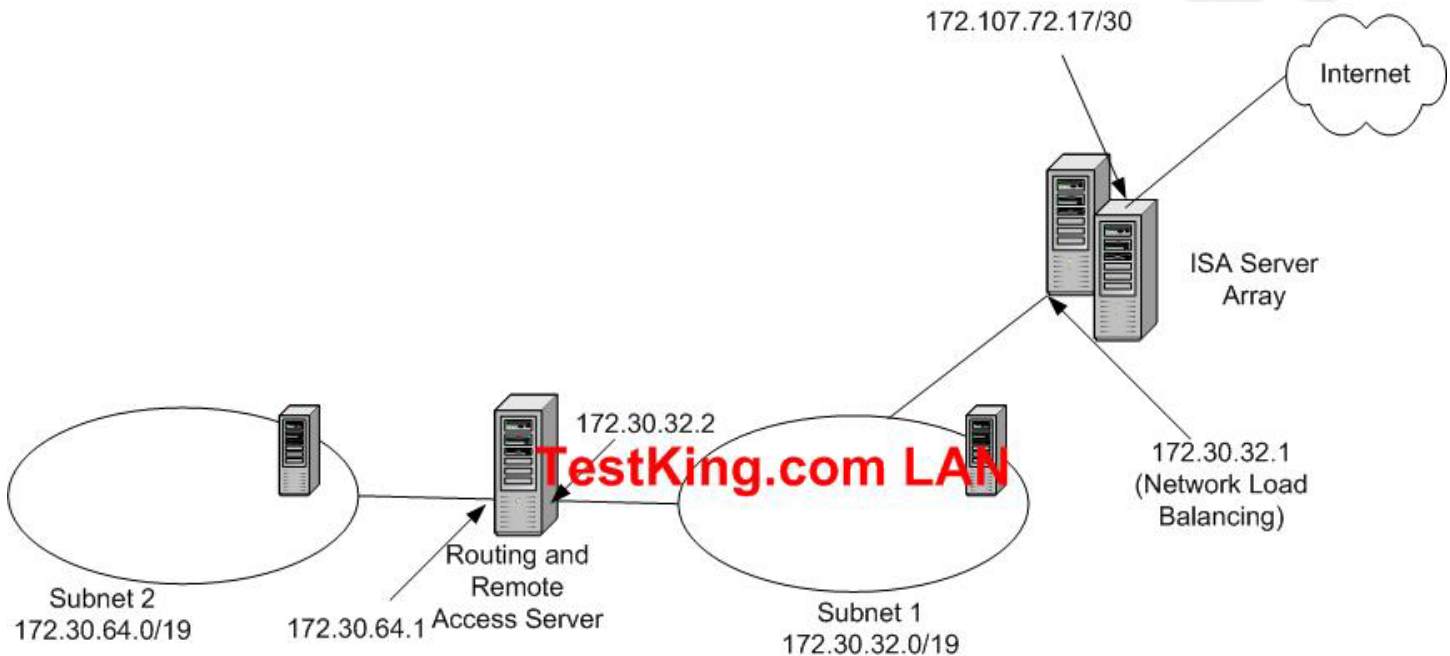
- A:** This policy isn't preventing the remote access. The Connections to Microsoft Routing and Remote Access server policy is preventing the access.
- B:** The global group is fine. Changing it won't help.
- C:** The Connections to Microsoft Routing and Remote Access server policy is preventing the 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: 79

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: 80

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 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.

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: 81

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 adapter 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: 82

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: 83

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: 84

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: 85

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 servers 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: 86

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: 87

You are the network administrator for TestKing. The network consists of a single Active Directory forest that contains three domains named testking.com, texas.testking.com, and dakota.testking.com. The functional level of the forest is Windows Server 2003.

Both texas.testking.com and dakota.testking.com contain employee user accounts, client computer accounts, and resource server computer accounts. The domain named testking.com contains only administrative user accounts and computer accounts for two domain controllers. Each resource server computer provides a single service of file server, print server, Web server, or database server.

TestKing plans to use Group Policy objects (GPOs) to centrally apply security settings to resource server computers. Some security settings need to apply to all resource servers and must not be overridden. Other security settings need to apply to specific server roles only.

You need to create an organizational unit (OU) structure to support the GPO requirements. You want to create as few GPOs and links as possible.

What should you do?

- A. Create a top-level OU for each server role under the testking.com domain.
Create a top-level OU named Servers under the texas.testking.com domain.
Create a top-level OU named Servers under the dakota.testking.com domain.
- B. Create a top-level OU named Servers under the texas.testking.com domain.
Create a child OU for each server role under the Servers OU.
Create a top-level OU named Servers under the Dakota.testking.com domain.
Create a child OU for each server role under the Servers OU.
- C. Create a top-level OU named Servers under the testking.com domain.
Create a child OU for each server role under the Servers OU.
- D. Create a top-level OU for each server role under the texas.testking.com domain.
Create a top-level OU for each server role under the dakota.testking.com domain.

Answer: B

Explanation: With a top-level OU named Servers, we can apply group policies to all the resource servers. With child OUs for each server role, we can apply group policies to individual server roles. Two domains have resource servers, dakota.testking.com and texas.testking.com. We need to create the OU structure in each of these two domains.

Incorrect Answers:

A: We need an OU for each server role in dakota.testking.com and texas.testking.com, because the resource servers are in those domains.

C: We need a top level OU for all the resource servers in dakota.testking.com and texas.testking.com, so we can apply group policies to all the servers.

D: We need a top level OU for all the resource servers in dakota.testking.com and texas.testking.com, so we can apply group policies to all the servers.

QUESTION NO: 88

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.

TestKing has one office in Hong Kong and another office in Beijing. Each office is configured as an Active Directory site. Each site contains two domain controllers.

The network is configured to display a legal notice on the computer screens of all users before they log on to their client computers. At the request of the legal department, you make changes to the wording of the notice by changing the settings in a Group Policy object (GPO). The GPO is linked to the domain.

The legal department reports that not all users are receiving the new notice. You discover that users in the Beijing office receive the new notice, but users in the Hong Kong office receive the old notice. The problem continues for several days.

You need to ensure that the new notice appears correctly on all computers in the network.

What should you do?

- A. Create a new security group that contains the computer accounts for all computers in the Hong Kong site.
Grant permissions to this security group to read and apply the GPO.
- B. Temporarily assign one of the domain controllers in the Hong Kong site to the Beijing site.
Wait 24 hours, and then reassign the domain controller to the Hong Kong site.
- C. Force replication of Active Directory between the two sites.
- D. Log on to one of the domain controllers in the Hong Kong site, and seize the infrastructure master role.

Answer: C

Explanation: It looks like the GPO settings haven't been replicated to the Hong Kong office – they are still receiving the old notice. We can manually force replication between the two sites to ensure that the Hong Kong office receives the new GPO settings.

Incorrect Answers:

- A:** The Hong Kong users still receive the old legal notice. Therefore, this is not a permissions problem on the group policy object.
- B:** This is unnecessary an impractical.
- D:** This has nothing to do with the replication of the GPO.

QUESTION NO: 89

You are the network administrator for TestKing. The network consists of a single Active Directory domain named testking.com. The domain contains an organizational unit (OU) named Sales. You create three Group Policy objects (GPOs) that have four configuration settings, as shown in the following table.

Location	GPO name	GPO configuration	Setting
Domain	ScreenSaver	Hide Screen Saver tab	Disabled
Sales OU	Display and Wallpaper	Hide Screen Saver tab	Enabled
Sales OU	Display and Wallpaper	Set Active Desktop Wallpaper to c:\WINNT\web\wallpaper\bliss.jpg	Enabled
Sales OU	Wallpaper	Set Active Desktop Wallpaper to c:\WINNT\web\wallpaper\autumn.jpg	Enabled

The ScreenSaver GPO has the No Override setting enabled. The Sales OU has the Block Policy inheritance setting enabled. The priority for GPOs linked to the Sales OU specifies first priority for the Display and Wallpaper GPO and second priority for the Wallpaper GPO.

For user accounts in the Sales OU, you want the Screen Saver tab to be hidden and the desktop wallpaper to be Autumn.jpg. You log on to a test computer by using a user account from the Sales OU, but you do not receive the settings you wanted.

You need to configure the settings to hide the Screen Saver tab and set the desktop wallpaper to Autumn.jpg for the user accounts in the Sales OU. You want to avoid affecting user accounts in other OUs.

What should you do?

- A. Enable the **No Override** setting for the Display and Wallpaper GPO.
- B. Disable the **No Override** setting on the ScreenSaver GPO.
Reorder the Wallpaper GPO to be first in the list.
- C. Create a GPO and link it to the Default-First-Site-Name.
Configure the GPO to set the Active Desktop Wallpaper to c:\WINNT\web\wallpaper\autumn.jpg.
- D. Disable the **Block Policy inheritance** setting on the Sales OU.
Change the Display and Wallpaper GPO to set the Active Desktop Wallpaper to c:\WINNT\web\wallpaper\autumn.jpg.

Answer: B

Explanation: The No Override setting on the Screensaver GPO is causing all computers in the domain to display the Screensaver tab. We want to hide the screensaver tab for the sales OU, so we'll have to remove the No Override settings from the Screensaver GPO. This will enable the Screensaver GPO settings to be overwritten by other GPOs.

By configuring the Wallpaper GPO to be first in the list, we are giving it a higher priority than the Display and Wallpaper GPO. This means that the Wallpaper GPO settings will overwrite the Display and Wallpaper GPO settings, thus setting the wallpaper to Autumn.jpg.

Group Policy Order of application

1. The unique local Group Policy object.
2. Site Group Policy objects, in administratively specified order.
3. Domain Group Policy objects, in administratively specified order.
4. Organizational unit Group Policy objects, from largest to smallest organizational unit (parent to child organizational unit) and in administratively specified order at the level of each organizational unit.

Enforcing policy from above

You can set policies that would otherwise be overwritten by policies in child organizational units to **No Override** at the Group Policy object level.

- Policies set to **No Override** cannot be blocked.
- The **No Override** and **Block** options should be used sparingly. Casual use of these advanced features complicates troubleshooting.

Reference: Server Help**QUESTION NO: 90**

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. Each client computer runs Windows NT Workstation 4.0, Windows 2000 Professional, or Windows XP Professional. The computer accounts for all client computers are located in an organizational unit (OU) named CompanyComputers. All user accounts are located in an OU named CompanyUsers.

TestKing has a written policy that requires a logon banner to be presented to all users when they log on to any client computer on the network. The banner must display a warning about unauthorized use of the computer.

You need to ensure that the logon banner appears when a user logs on to a client computer.

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

- A. Create a Group Policy object (GPO) that includes the appropriate settings in the interactive logon section.
Link the GPO to the domain.
- B. Create a script that presents the required warning.
Create a Group Policy object (GPO) that will cause the script to run during the startup process.
Link the GPO to TestKingUsers OU.
- C. Create a system policy file named Ntconfig.pol that includes the appropriate settings.
Place a copy of this file in the appropriate folder on the domain controller.
- D. Create a batch file named Autoexec.bat that presents the required warning.
Copy the file to root folder on ***MISSING***

Answer: A, C

Explanation: We need to configure a GPO to display the logon message that will apply to the Windows 2000 and Windows XP clients. We need to configure a system policy to display the logon message that will apply to the Windows NT clients.

This policy is created with System policies and the System Policy Editor, System policies are used by network administrators to configure and control individual users and their computers. Administrators use POLEDIT.EXE to set Windows NT profiles that are either network- or user-based. Using this application, you can create policies, which are either local or network-driven, that can affect Registry settings for both hardware and users. The file created to apply the policy is named NTConfig.pol.

Interactive logon: Message text for users attempting to log on

Description

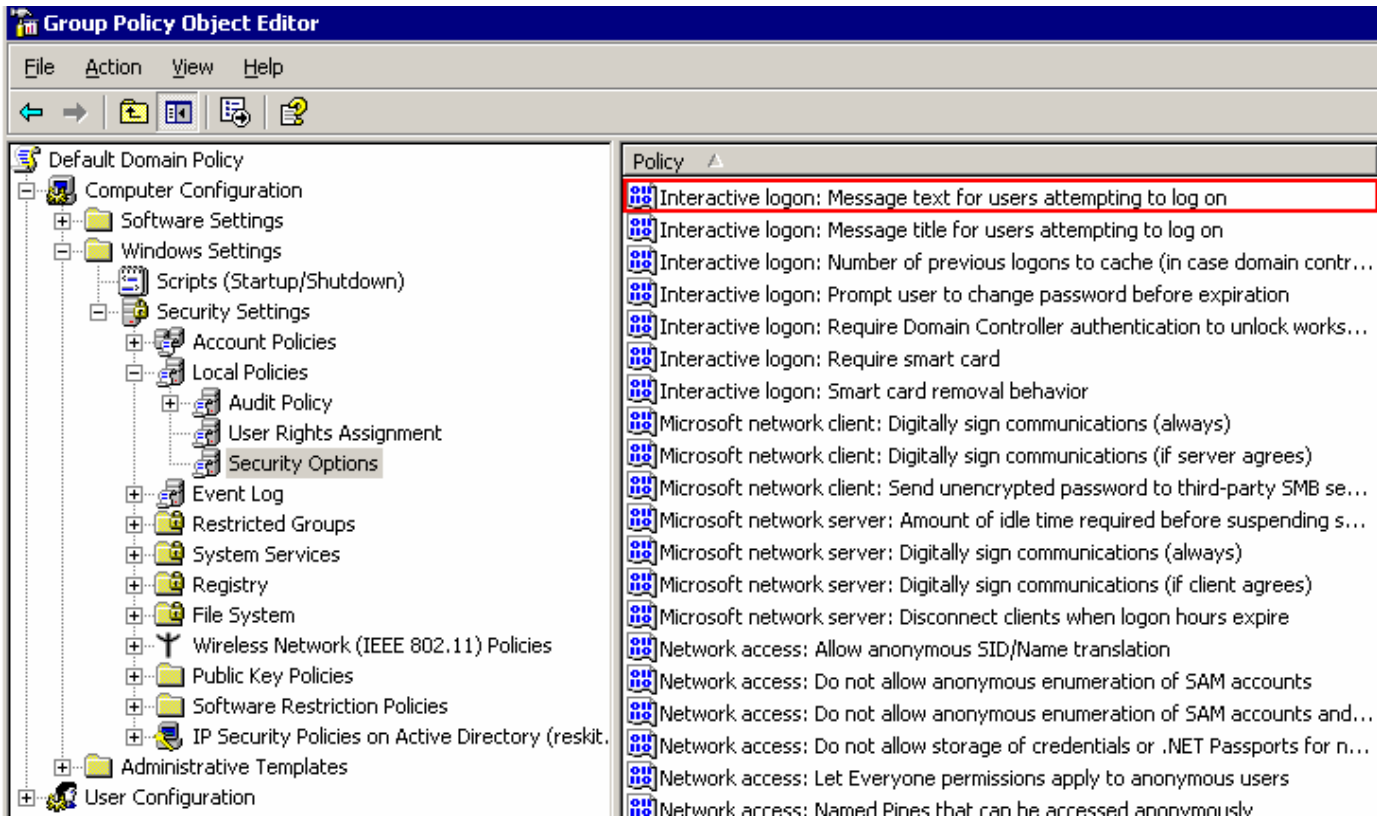
This security setting specifies a text message that is displayed to users when they log on.

This text is often used for legal reasons, for example, to warn users about the ramifications of misusing company information or to warn them that their actions may be audited.

Default: No message.

Configuring this security setting

You can configure this security setting by opening the appropriate policy and expanding the console tree as such: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\



Reference

Group Policy Help

QUESTION NO: 91

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. Except for IT staff, users are not local administrators on client computers.

TestKing obtains a new application for order processing. This application must be installed on each client computer. The application is contained in an .msi file. You copy the .msi file to a shared folder on a file server. You assign the Authenticated Users group the Allow – Read permissions for the shared folder.

To deploy the application, you instruct users to double-click the .msi file in the shared folder. When users attempt to install the application, they receive an error message, and setup fails.

You need to configure the network so that the application can be installed successfully.

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

- A. Modify the Default Domain Policy Group Policy object (GPO) and assign the new application to all client computers.
- B. Grant the users the permissions required to create temporary files in the shared folder that contains the .msi file.
- C. Modify the Default Domain Policy Group Policy object (GPO) and disable the **Prohibit User Installs** setting in the Windows Installer section of the computer settings.
- D. Modify the Default Domain Policy Group Policy object (GPO) and enable the **Always install with elevated privileges** setting in the Windows Installer section of the computer settings.

Answer: A, D

Explanation: The software installation fails because the users don't have the necessary permissions to install the software. We can solve this problem by either assigning the application to the users in a group policy, or by using a group policy to enable the **Always install with elevated privileges** setting in the Windows Installer section of the computer settings.

Software installation

You can use the Software Installation extension of Group Policy to centrally manage software distribution in your organization. You can assign and publish software for groups of users and computers using this extension.

Assigning Applications

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.

Publishing Applications

You can also publish applications to users, making the application available for users to install. To install a published application, users can use Add or Remove Programs in Control Panel, which includes a list of all published applications that are available for them to install. Alternatively, if the administrator has selected the

Auto-install this application by file extension activation feature, users can open a document file associated with a published application. For example, double clicking an .xls file will trigger the installation of Microsoft Excel, if it is not already installed. Publishing applications only applies to user policy; you cannot publish applications to computers.

To take advantage of all of the features of Group Policy Software Installation, it is best to use applications that include a Windows Installer (.msi) package. For example, published MSI packages support installation for users who do not have administrative credentials.

However, you can also publish legacy setup programs using a .zap file. These applications will be displayed in Add or Remove Programs like any other published application, but typically can only be installed by users with administrative credentials.

A .zap file is a simple text file that describes the path to the setup program, as well as any arguments to be passed on the command line.

A simple example illustrating the syntax of a .zap file is shown below:

[Application]

FriendlyName = Microsoft Works 4.5a

SetupCommand = """"\\DeploymentServer\Apps\Works 4.5a\Standard\Setup.exe""""

Note

When using quotes in zap files, the following rules apply:

- The path and name of the setup executable must always be quoted.
- If there are no command-line arguments, they must be quoted twice.

Non-Windows Installer Applications

It is possible to publish applications that do not install with the Windows Installer. They can only be published to users and they are installed using their existing Setup programs.

Impersonate a client after authentication

Assigning this privilege to a user allows programs running on behalf of that user to impersonate a client.

Requiring this user right for this kind of impersonation prevents an unauthorized user from convincing a client to connect (for example, by remote procedure call (RPC) or named pipes) to a service that they have created and then impersonating that client, which can elevate the unauthorized user's permissions to administrative or system levels.

Caution

Assigning this user right can be a security risk. Only assign this user right to trusted users.

Non Windows installer applications

Because these non-Windows Installer applications use their existing Setup programs, such applications cannot:

- **Use elevated privileges for installation.**
- Install on the first use of the software.
- Install a feature on the first use of the feature.
- Rollback an unsuccessful operation, such a install, modify, repair, or removal, or take advantage of other features of the Windows Installer.
- Detect a broken state and automatically repair it.

References:

Group policy help

Step-by-Step Guide to Software Installation and Maintenance

<http://www.microsoft.com/windows2000/techinfo/planning/management/swinstall.asp>

QUESTION NO: 92

You are a network administrator for TestKing. The network consists of a single Active Directory forest that contains two domains. All servers run Windows Server 2003. The domains and organizational units (OUs) are structured as shown in the work area.

Users in the research department have user accounts in the research.testking.com domain. All other user accounts and resources are in the testking.com domain. All domain controllers are in the Domain Controllers OU of their respective domain. No other computer or user accounts are in the Domain Controllers OUs.

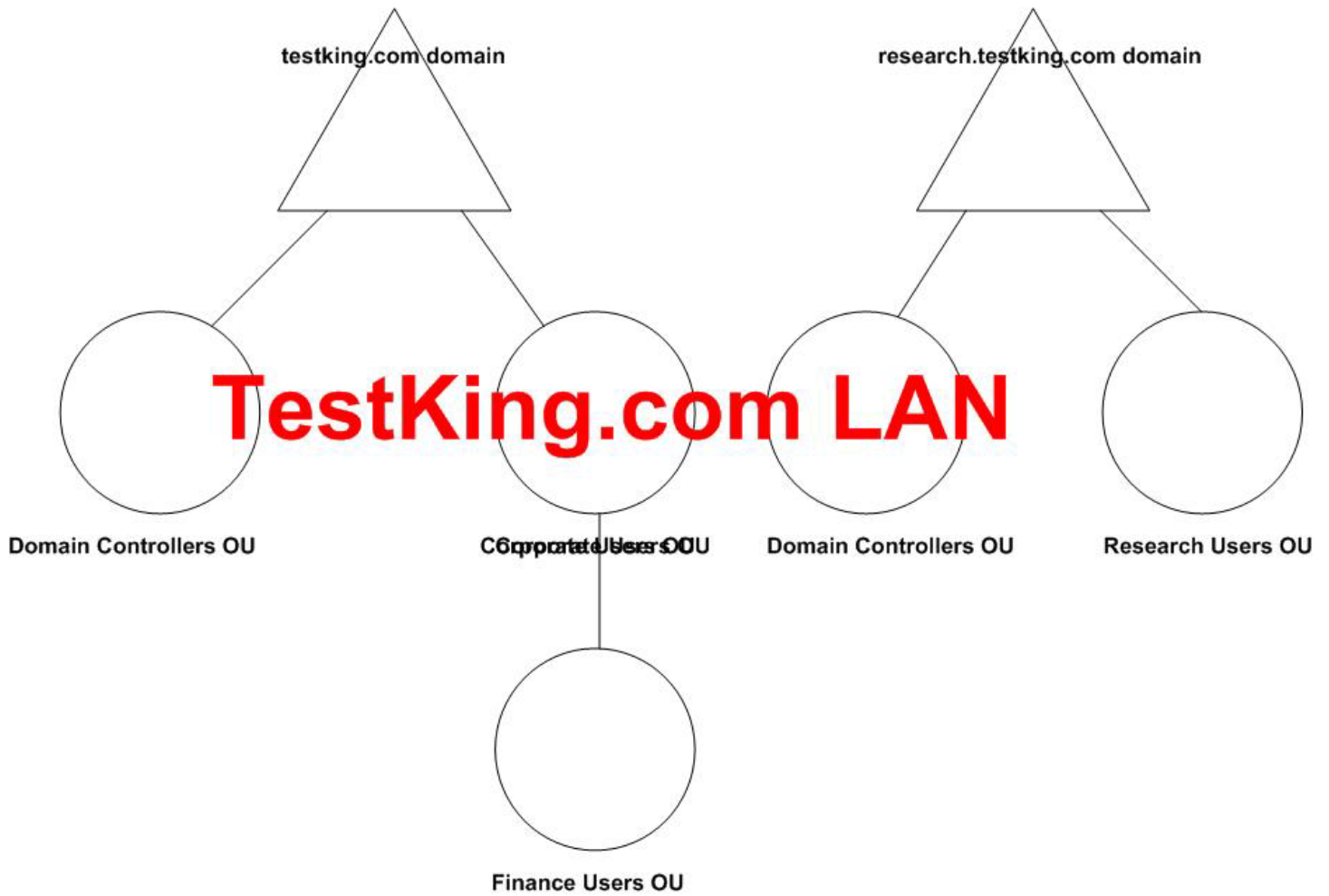
A written company policy requires that all users working in the research department must use complex passwords of at least nine characters in length. The written policy states that no other users are to have password restrictions. All affected users have user accounts in an OU named Research Users in the research.testking.com domain.

You create a Group Policy object (GPO) that contains the required settings.

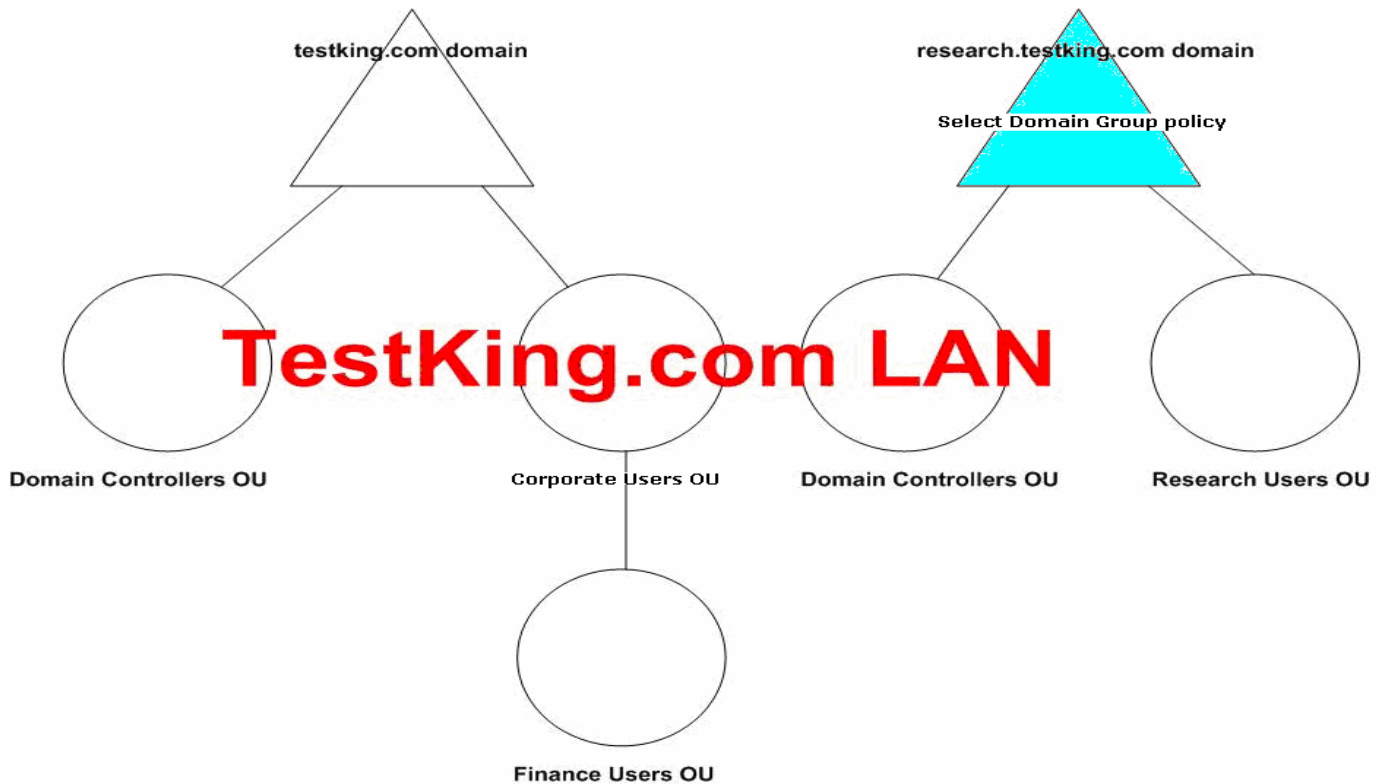
You need to ensure that these settings affect the users in the research department, and that the settings do not affect any other domain users or local accounts.

Where should you link the GPO?

To answer, select the appropriate location or locations in the work area.



Answer: Select the research.testking.com domain.

**Explanation:**

Password restrictions for domain user accounts must always be set at domain level. Password policies applied at OU level will only apply to local user accounts. In this scenario, **research.testking.com** contains only research users so applying the policy at the domain level will not affect any other others.

QUESTION NO: 93

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.

All servers that are not domain controllers have computer accounts in an organizational unit (OU) named **ApplicationServers**. Client computers have computer accounts in 15 OUs organized by department. All users have user accounts in an OU named **CompanyUsers**.

TestKing wants all users to have Microsoft Word available on their client computers. TestKing does not want to install Word on domain controller or other servers.

You need to configure the network to install the application as required, without affecting any existing policies or settings.

What should you do?

- A. Create a Group Policy object (GPO) configured with Microsoft Word listed in the software installation section of the computer settings.
Link this GPO to the domain.
Configure the Domain Controllers OU and the ApplicationServers OU to block policy inheritance.
- B. Create a Group Policy object (GPO) configured with Microsoft Word listed in the software installation section of the computer settings.
Link this GPO to the domain.
Configure permissions on the GPO so that all servers and domain controller accounts are denied the permissions to read and apply the GPO.
- C. Create a Group Policy object (GPO) configured with Microsoft Word listed in the software installation section of the user settings.
Link this GPO to the domain.
Configure the Domain Controllers OU and the ApplicationServers OU to block policy inheritance.
- D. Create a Group Policy object (GPO) configured with Microsoft Word listed in the software installation section of the user settings.
Link this GPO to the domain.
Configure permissions on the GPO so that all server and domain controller accounts are denied the permissions to read and apply the GPO.

Answer: B

Explanation: The software can be installed on all the client computers, but not the domain controllers or application servers. Because the client computers are in 15 OUs, it would be easier to link the GPO at the domain level. The OUs containing the client computers would then inherit the GPO settings.

To prevent the GPO applying to the domain controllers and servers, we can simply deny the permissions to read and apply the GPO for the domain controller and server computer accounts.

Software installation

You can use the Software Installation extension of Group Policy to centrally manage software distribution in your organization. You can assign and publish software for groups of users and computers using this extension.

Assigning Applications

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.

Publishing Applications

You can also publish applications to users, making the application available for users to install. To install a published application, users can use Add or Remove Programs in Control Panel, which includes a list of all published applications that are available for them to install. Alternatively, if the administrator has selected the Auto-install this application by file extension activation feature, users can open a document file associated with a published application. For example, double clicking an .xls file will trigger the installation of Microsoft Excel, if it is not already installed. Publishing applications only applies to user policy; you cannot publish applications to computers.

Filter user policy settings based on membership in security groups.

You can specify users or groups for which you do not want a policy setting to apply by clearing the Apply Group Policy and Read check boxes, which are located on the Security tab of the properties dialog box for the GPO.

When the Read permission is denied, the policy setting is not downloaded by the computer.

As a result, less bandwidth is consumed by downloading unnecessary policy settings, which enables the network to function more quickly. To deny the Read permission, select Deny for the Read check box, which is located on the Security tab of the properties dialog box for the GPO.

Incorrect Answers:

A: It is likely that some domain level policies should apply to the domain controllers and the servers. Therefore, blocking policy inheritance isn't recommended.

C: It is likely that some domain level policies should apply to the domain controllers and the servers. Therefore, blocking policy inheritance isn't recommended.

D: This won't stop the software being installed on the servers, because the software installation would be defined in the user section of the group policy.

QUESTION NO: 94

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 either

Windows XP Professional or Windows 2000 Professional. All client computer accounts are located in an organizational unit (OU) named Workstation.

A written company policy states that the Windows 2000 Professional computers must not use offline folders. You create a Group Policy object (GPO) to enforce this requirement. The settings in the GPO exist for both Windows 2000 Professional computers and Windows XP Professional computers.

You need to configure the GPO to apply only to Windows 2000 Professional computers.

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

- A. Create a WMI filter that will apply the GPO to computers that are running Windows 2000 Professional.
- B. Create a WMI filter that will apply the GPO to computers that are not running Windows XP Professional.
- C. Create two OUs under the Workstation OU.
Place the computer accounts for the Windows XP Professional computers in one OU, and place the computer accounts for the Windows 2000 Professional computers in the other OU.
Link the GPO to the Workstation OU.
- D. Create a group that includes the Windows XP Professional computers.
Assign the group the **Deny – General Resultant Set of Policy(Logging)** permission.
- E. Create a group that includes the Windows 2000 Professional computers. Assign the group the **Deny – Apply Group Policy** permission.

Answer: A, B

Explanation: This is a tricky question because WMI filters are ignored by Windows 2000 clients. However, that doesn't matter. The Windows XP clients can evaluate the filters and that is good enough. For answer A, the XP clients will evaluate the filter and see that the GPO should not apply to them. The Windows 2000 clients will just apply the GPO without evaluating the WMI filter. For answer B, the same thing will happen. The XP clients will evaluate the filter and see that the GPO should not apply to them. The Windows 2000 clients will just apply the GPO without evaluating the WMI filter.

WMI filtering

WMI filters are only available in domains that have the Windows Server 2003 configuration. Although none of the domain controllers need to be running Windows Server 2003, you must have run ADPrep /DomainPrep in this domain. Also note that WMI filters are only evaluated by clients running Windows XP, Windows Server 2003, or later. WMI filters associated with a Group Policy object will be ignored by Windows 2000 clients and the GPO will always be applied on Windows 2000.

Incorrect Answers:

C: This looks like a good idea. However, applying the GPO to the Workstation OU will (by inheritance) apply the GPO to the two child OUs.

D: This won't prevent the application of the GPO.

E: This answer is close, but incorrect. This will prevent the GPO applying to the Windows 2000 clients. If the group contained the Windows XP clients, then it would work.

QUESTION NO: 95

You are the network administrator for TestKing. The network consists of a Single Active Directory domain with three sites. There is a domain controller at each site. All servers run Windows Server 2003. Each client computer runs either Windows 2000 Professional or Windows XP Professional.

The IT staff is organized into four groups. The IT staff work at the three different sites. The computers for the IT staff must be configured by using scripts. The script or scripts must run differently based on which site the IT staff user is logging on to and which of the four groups the IT staff user is a member of.

You need to ensure that the correct logon script is applied to the IT staff users based on group membership and site location.

What should you do?

- A. Create four Group Policy objects (GPOs).
Create a script in each GPO that corresponds to one of the four groups.
Link the four new GPOs to all three sites.
Grant each group permissions to apply only the GPO that was created for the group.
- B. Create a single script that performs the appropriate configuration based on the user's group membership.
Place the script in the Netlogon shared folders on the domain controllers.
- C. Configure a Group Policy object (GPO) with a startup script that configures computers based on IT staff group.
Link the GPO to the three sites.
- D. Create a script that configures the computers based on IT staff group membership and site.
Create and link a GPO to the Domain Controllers OU to run the script.

Answer: A

Explanation: The easiest way to filter which users or computers a GPO should apply to is to set permissions on the GPOs. A user or computer needs the Allow – Read and Apply Group Policy permissions in order to apply the GPO. In this question, we have four groups, each with different requirements. By creating four different GPOs and linking them to each of the three sites, we can manage who receives the GPO by configuring the permissions on the GPOs.

Incorrect Answers:

B: The script needs to be linked to an Active Directory container.

C: It's easier to use GPO permissions to determine which users or computers should receive a GPO.

D: It's easier to use GPO permissions to determine which users or computers should receive a GPO. Furthermore, the GPO is linked to the wrong container in this answer.

QUESTION NO: 96

You are the network administrator for TestKing, a company that has a single office. The network consists of a single Active Directory domain and a single site. All servers run Windows Server 2003.

All file and print servers and application servers are located in an organizational unit (OU) named Servers. A server support team handles daily support issues for the file and print servers and application servers. All of the server support team's user accounts are located in the OU named SST.

You are responsible for managing security for TestKing's servers. You create a group named ServerSupport that includes all the user accounts of the server support team.

You need to ensure that members of the server support team can log on locally to only the file and print servers and the application servers.

What should you do?

- A. Create a Group Policy object (GPO) to grant the ServerSupport group the **Allow log on locally** user right.
Link the GPO to the SST OU.
- B. Create a Group Policy object (GPO) to grant the ServerSupport group the **Allow log on locally** user right.
Link the GPO to the Servers OU.
- C. Assign the ServerSupport group the **Allow – Full Control** permission for the Servers OU.
- D. Assign the ServerSupport group the **Allow – Full Control** permission for the Computers container.

Answer: B

Explanation: All file and print servers and application servers are located in an organizational unit (OU) named Servers. Therefore, we can simply a Group Policy object (GPO) to grant the ServerSupport group the **Allow log on locally** user right and link the GPO to the Servers OU.

Incorrect Answers:

A: The GPO needs to be linked to the OU containing the computer accounts for the servers.

C: This would allow the ServerSupport group to create objects in the OU, and to modify the permission on existing objects. This is more 'permission' than necessary.

D: This would allow the ServerSupport group to create objects in the computers container, and to modify the permission on existing objects. This would have no effect on the servers because they are in a separate OU.

QUESTION NO: 97

You are the network administrator for TestKing. The network consists of a single Active Directory forest. The forest consists of 19 Active Directory domains. Fifteen of the domains contain Windows Server 2003 domain controllers. The functional level of all the domains is Windows 2000 native. The network consists of a single Microsoft Exchange 2000 Server organization.

You need to create groups that can be used only to send e-mail messages to user accounts throughout TestKing. You want to achieve this goal by using the minimum amount of replication traffic and minimizing the size of the Active Directory database.

You need to create a plan for creating e-mail groups for TestKing.

What should you do?

- A. Create global distribution groups in each domain.
Make the appropriate users from each domain members of the global distribution group in the same domain.
Create universal distribution groups.
Make the global distribution groups in each domain members of the universal distribution groups.
- B. Create global security groups in each domain.
Make the appropriate users from each domain members of the security group in the same domain.
Create universal security groups.
Make the global security groups in each domain members of the universal security groups.
- C. Create universal distribution groups.
Make the appropriate users from each domain members of a universal distribution group.
- D. Create universal security groups.
Make the appropriate users from each domain members of a universal security group.

Answer: A

Explanation: We need to minimize replication traffic. We can do this by placing the users into Global groups, then place the Global groups into Universal groups. In Active Directory, a Universal group lists all its members. If the Universal group contained user accounts, and a user account was added or removed, then the Universal group information would be replicated throughout the forest. This is why placing user accounts directly into Universal groups isn't recommended. We need to use Distribution groups for email groups. Answers B and D are wrong because they suggest using security groups. Answer C is wrong because it suggests placing the user accounts directly into Universal groups.

Domain functional levels	Domain controllers supported	Group scopes supported
Windows 2000 mixed (default)	Windows NT Server 4.0, Windows 2000, Windows Server 2003	Global, domain local
Windows 2000 native	Windows 2000, Windows Server 2003	Global, domain local, universal
Windows Server 2003	Windows Server 2003	Global, domain local, universal

When to use global groups

Because global groups have a forest-wide visibility, do not create them for domain-specific resource access.

Use a global group to organize users who share the same job tasks and need similar network access requirements.

A different group type is more appropriate for controlling access to resources within a domain.

When to use universal groups

Use universal groups to nest global groups so that you can assign permissions to related resources in multiple domains.

A Windows Server 2003 domain must be in Windows 2000 native mode or higher to use universal groups.

When to use domain local groups

Use a domain local group to assign permissions to resources that are located in the same domain as the domain local group.

You can place all global groups that need to share the same resources into the appropriate domain local group.

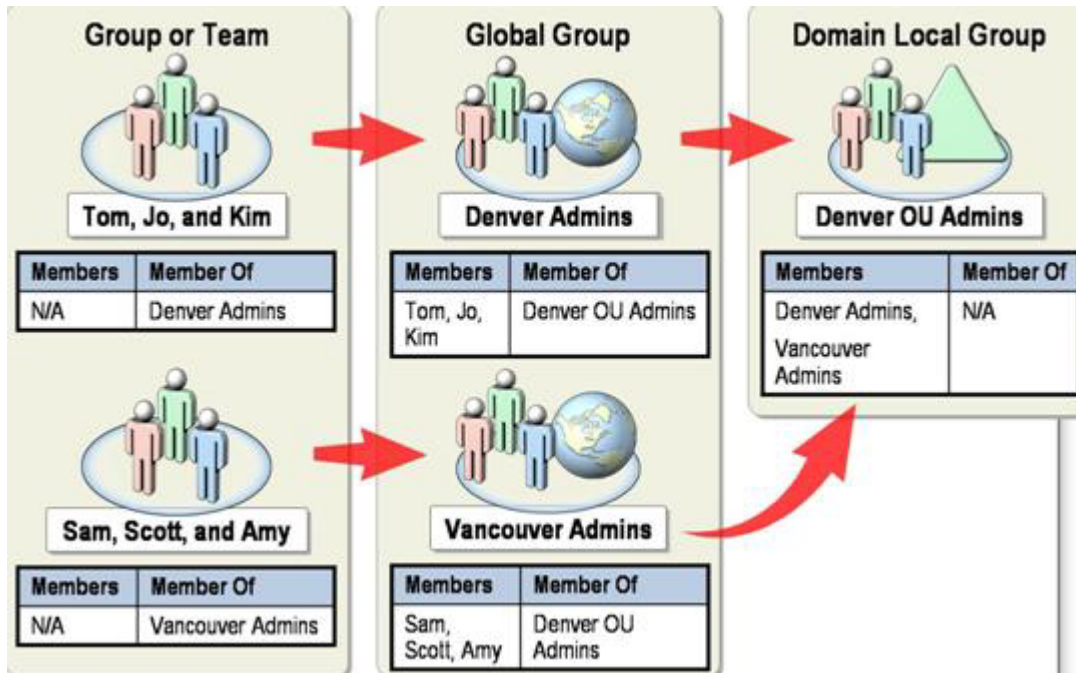
MS THUMB RULES

Grant permissions to groups instead of users.

- A G P
- A DL P
- A G DL P
- A G U DL P
- A G L P

A (Account)
G (Global Group)
U (Universal Group)
DL (Domain Local Group)

P (Permissions)



Group scope

Groups, whether a [security group](#) or a [distribution group](#), are characterized by a scope that identifies the extent to which the group is applied in the domain tree or forest. There are three group scopes: universal, global, and domain local.

- Members of universal groups can include other groups and accounts from any domain in the domain tree or forest and can be assigned permissions in any domain in the domain tree or forest.
- Members of global groups can include other groups and accounts only from the domain in which the group is defined and can be assigned permissions in any domain in the forest.
- Members of domain local groups can include other groups and accounts from Windows Server 2003, Windows 2000, or Windows NT domains and can be assigned permissions only within a domain.

The following table summarizes the behaviors of the different group scopes.

Universal scope	Global scope	Domain local scope
When the domain functional level is set to Windows 2000 native or Windows Server 2003, members of universal groups can include accounts, global groups, and universal groups from any domain.	When the domain functional level is set to Windows 2000 native or Windows Server 2003, members of global groups can include accounts and global groups from the same domain.	When the domain functional level is set to Windows 2000 native or Windows Server 2003, members of domain local scope can include accounts, global groups, and universal groups from any domain, as well as domain local groups from the same domain.
When the domain functional level is set to Windows 2000 mixed, security groups with universal scope cannot be created.	When the domain functional level is set to Windows 2000 mixed, members of global groups can include accounts from the same domain.	When the domain functional level is set to Windows 2000 native or Windows Server 2003, members of domain local groups can include accounts and global groups from any domain.
When the domain functional level is set to Windows 2000 native or Windows Server 2003, groups can be added to other groups and assigned permissions in any domain.	Groups can be added to other groups and assigned permissions in any domain.	Groups can be added to other domain local groups and assigned permissions only in the same domain.
Groups can be converted to domain local scope. Groups can be converted to global scope, as long as no other universal groups exists as members.	Groups can be converted to universal scope, as long as the group is not a member of any other group with global scope.	Groups can be converted to universal scope, as long as the group does not have as its member another group with domain local scope.

Reference

Server Help

Schema classes and attributes, MS workshop 2209

QUESTION NO: 98

You are the network administrator for Acme Inc. Your network consists of a single Active Directory forest that contains one domain named acme.com. The functional level of the forest is Windows Server 2003.

Acme, Inc., acquires a company named TestKing. The TestKing network consists of a single Active Directory forest that contains a root domain named testking.com and a child domain named

asia.testking.com. The functional level of the forest is Windows 2000. The functional level of the asia.testking.com domain is Windows 2000 native.

A business decision by TestKing requires that asia.testking.com domain to be removed.

You need to move all user accounts from the asia.testking.com domain to the acme.com domain by using the Active Directory Migration Tool. You need to accomplish this task without changing the logon rights and permissions for all other users. You need to ensure that users in asia.testking.com can log on to acme.com by using their current user names and passwords.

What should you do?

- A. Create a two-way Windows Server 2003 external trust relationship between the acme.com domain and the testking.com domain.
- B. Create a one-way Windows Server 2003 external trust relationship in which the acme.com domain trusts the testking.com domain.
- C. Create a temporary two-way external trust relationship between the acme.com domain and the asia.testking.com domain.
- D. Create a temporary one-way external trust relationship in which the asia.testking.com domain trusts the acme.com domain.

Answer: C

Explanation: To use ADMT, we need a two way trust between the acme.com domain and the asia.testking.com domain.

Incorrect Answers:

- A:** This would enable users in testking.com to log in to acme.com and users in acme.com to log in to testking.com.
- B:** This would enable users in testking.com to log in to acme.com.
- D:** The trust must be a two-way trust.

QUESTION NO: 99

You are the network administrator for TestKing. Your network consists of a single Active Directory forest that contains three domains. The forest root domain is named testking.com. The domain contains two child domains named asia.testking.com and africa.testking.com. The functional level of the forest is Windows Server 2003.

Each domain contains two Windows Server 2003 domain controllers named DC1 and DC2. DC1 in the testking.com domain performs the following two operations master roles: schema master and domain

naming master. DC1 in each child domain performs the following three operations master roles: PDC emulator master, relative ID (RID) master, and infrastructure master. DC1 in each domain is also a global catalog server.

The user account for Tess King in the africa.testking.com domain is a member of the Medicine Students security group. Because of a name change, the domain administrator of africa.testking.com changes the Last name field of Tess's user account from King to Edwards.

The domain administrator of asia.testking.com discovers that the user account for Tess is still listed as Tess King.

You need to ensure that the user account for Tess Edwards is correctly listed in the Medicine Students group.

What should you do?

- A. Transfer the PDC emulator master role from DC1 to DC2 in each domain.
- B. Transfer the infrastructure master role from DC1 to DC2 in each domain.
- C. Transfer the RID master role from DC1 to DC2 on each domain.
- D. Transfer the schema master role from DC1 to DC2 in the testking.com domain.

Answer: B

Explanation: Problems like this can occur when the infrastructure master role is on the same domain controller as the Global Catalog. There is no reason to transfer any other master roles.

Infrastructure master

A domain controller that holds the infrastructure operations master role in Active Directory. The infrastructure master updates the group-to-user reference whenever group memberships change and replicates these changes across the domain. At any time, the infrastructure master role can be assigned to only one domain controller in each domain.

The infrastructure master is responsible for updating references from objects in its domain to objects in other domains. The infrastructure master compares its data with that of a global catalog. Global catalogs receive regular updates for objects in all domains through replication, so the global catalog data will always be up to date. If the infrastructure master finds data that is out of date, it requests the updated data from a global catalog. The infrastructure master then replicates that updated data to the other domain controllers in the domain.

Important

Unless there is only one domain controller in the domain, the **infrastructure master role should not be assigned to the domain controller that is hosting the global catalog**. If the infrastructure master and global

catalog are on the same domain controller, the infrastructure master will not function. The infrastructure master will never find data that is out of date, so it will never replicate any changes to the other domain controllers in the domain.

In the case where all of the domain controllers in a domain are also hosting the global catalog, all of the domain controllers will have the current data and it does not matter which domain controller holds the infrastructure master role.

The infrastructure master is also responsible for updating the group-to-user references whenever the members of groups are renamed or changed. When you rename or move a member of a group (and that member resides in a different domain from the group), the group may temporarily appear not to contain that member. The infrastructure master of the group's domain is responsible for updating the group so it knows the new name or location of the member. This prevents the loss of group memberships associated with a user account when the user account is renamed or moved. The infrastructure master distributes the update via multimaster replication.

There is no compromise to security during the time between the member rename and the group update. Only an administrator looking at that particular group membership would notice the temporary inconsistency.

QUESTION NO: 100

You are the network administrator for TestKing. The network consists of a single Active Directory domain with two sites. Each site contains two domain controllers. One domain controller in each site is a global catalog server.

You add a domain controller to each site. Each new domain controller has a faster processor than the existing domain controllers.

TestKing requires Active Directory replication to flow through the servers that have the most powerful CPUs in each site.

You need to configure the intersite replication to comply with TestKing's requirement for Active Directory replication.

What should you do?

- A. Configure the new domain controllers as global catalog servers.
- B. Configure the new domain controller in each site as a preferred bridgehead server for the IP transport.
- C. Configure the new domain controller in each site as a preferred bridgehead server for the SMTP transport.
- D. Configure an additional IP site link between the two sites.
Assign a lower site link cost to this site link than the site link cost for the original site link.

Answer: B

Explanation:

Replication.

Directory information is replicated both within and among sites. Active Directory replicates information within a site more frequently than across sites. This balances the need for up-to-date directory information with the limitations imposed by available network bandwidth.

You customize how Active Directory replicates information using site links to specify how your sites are connected. Active Directory uses the information about how sites are connected to generate Connection objects that provide efficient replication and fault tolerance.

You provide information about the cost of a site link, times when the link is available for use and how often the link should be used. Active Directory uses this information to determine which site link will be used to replicate information. Customizing replication schedules so replication occurs during specific times, such as when network traffic is low, will make replication more efficient.

Ordinarily, all domain controllers are used to exchange information between sites, but you can further control replication behavior by specifying a bridgehead server for inter-site replicated information. **Establish a bridgehead server when you have a specific server you want to dedicate for inter-site replication, rather than using any server available.** You can also establish a bridgehead server when your deployment uses proxy servers, such as for sending and receiving information through a firewall.

Site link

Site links are logical paths that the KCC uses to establish a connection for Active Directory replication. Site links are stored in Active Directory as site link objects. A site link object represents a set of sites that can communicate at uniform cost through a specified intersite transport.

All sites contained within the site link are considered to be connected by means of the same network type. Sites must be manually linked to other sites by using site links so that domain controllers in one site can replicate directory changes from domain controllers in another site. Because site links do not correspond to the actual path taken by network packets on the physical network during replication, you do not need to create redundant site links to improve Active Directory replication efficiency.

When two sites are connected by a site link, the replication system automatically creates connections between specific domain controllers in each site called *bridgehead servers*. In Microsoft® Windows® 2000, intersite replication of the directory partitions (e.g. domain, configuration, and schema) between domain controllers in different sites is performed by the domain controllers (one per directory partition) in those sites designated by the KCC as the bridgehead server. In Windows Server 2003, the KCC may designate more than one domain controller per site hosting the same directory partition as a candidate bridgehead server. The replication connections created by the KCC are randomly distributed between all candidate bridgehead servers in a site to share the replication workload. By default, the randomized selection process takes place only when new connection objects are added to the site.

However, you can run Adlb.exe, a new Windows Resource Kit tool called Active Directory Load Balancing (ADLB) to rebalance the load each time a change occurs in the site topology or in the number of domain controllers the site. In addition, ADLB can stagger schedules so that the outbound replication load for each domain controller is spread out evenly across time. Consider using ADLB to balance replication traffic between the Windows Server 2003–based domain controllers when they are replicating to more than 20 other sites hosting the same domain

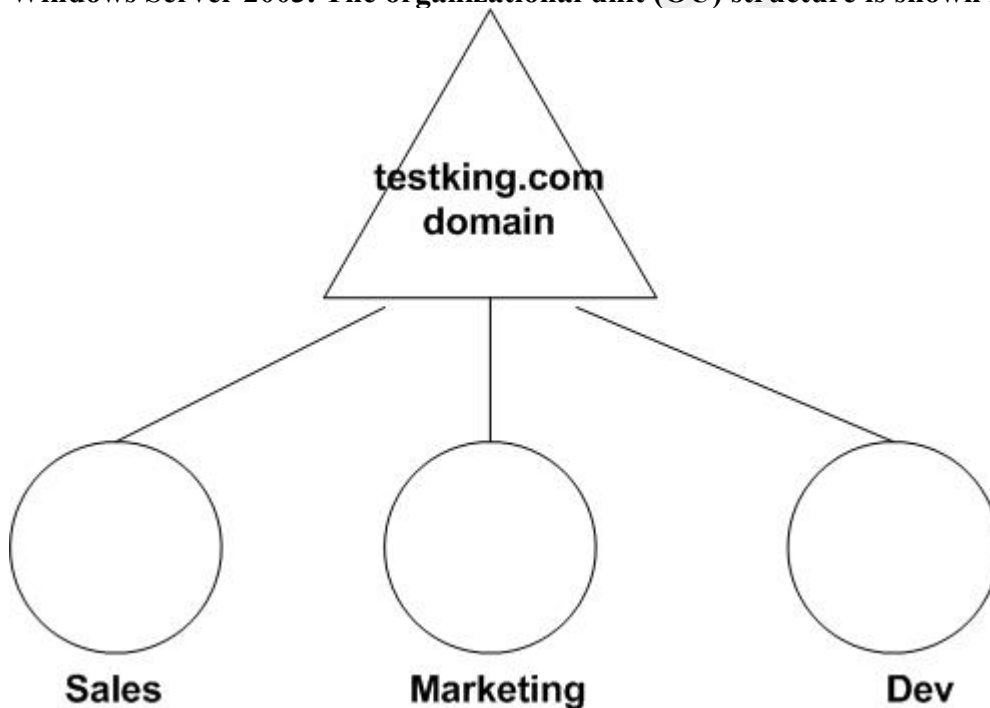
Reference

MS Windows Server 2003 Deployment Kit

Designing and Deploying Directory and Security Services
Active Directory Replication Concepts

QUESTION NO: 101

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. The functional level of the domain is Windows Server 2003. The organizational unit (OU) structure is shown in the exhibit.



TestKing uses an X.500 directory service enabled product to support a sales and marketing application. The application is used only by users in the sales department and the marketing department. The

application uses InetOrgPerson objects as user accounts. InetOrgPerson objects have been created in Active Directory for all Sales and Marketing users. These users are instructed to log on by using their InetOrgPerson object as their user account.

Microsoft Identity Integration Server is configured to copy changes to InetOrgPerson objects from Active Directory to the X.500 directory service enabled product. All InetOrgPerson objects for marketing employees are located in the Marketing OU. All InetOrgPerson objects for sales employees are located in the Sales OU.

King is another administrator in TestKing. King is responsible for managing the objects for users who require access to the X.500 directory service enabled product.

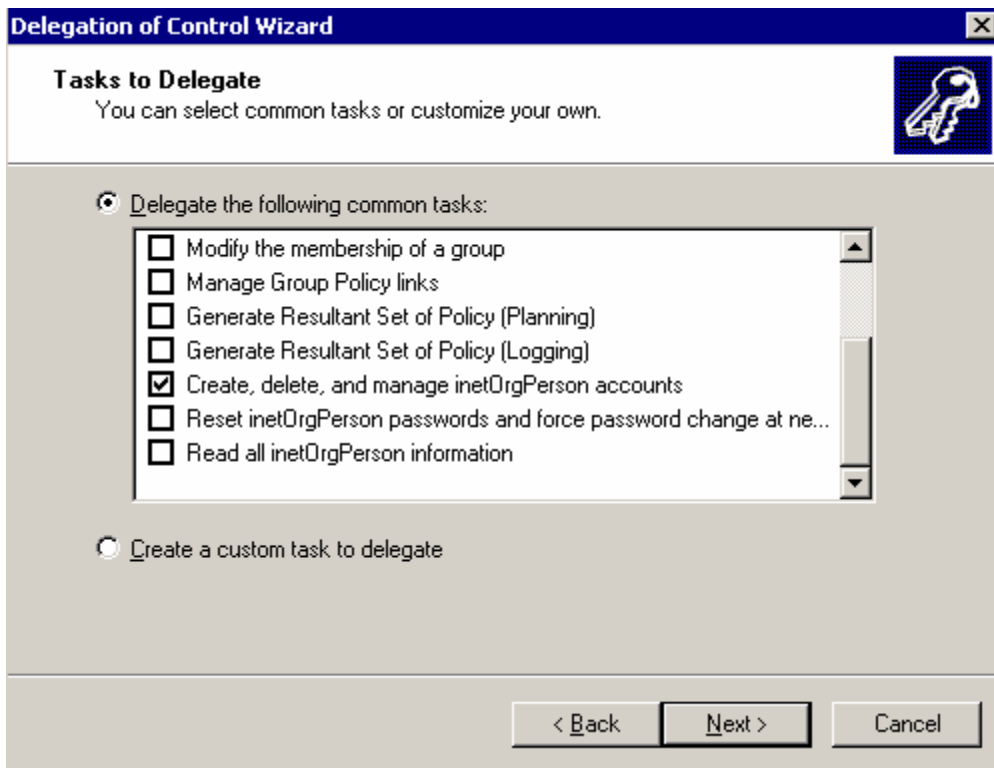
You need to configure Active Directory to allow King to perform his responsibilities.

Which action or actions should you take? (Choose all that apply)

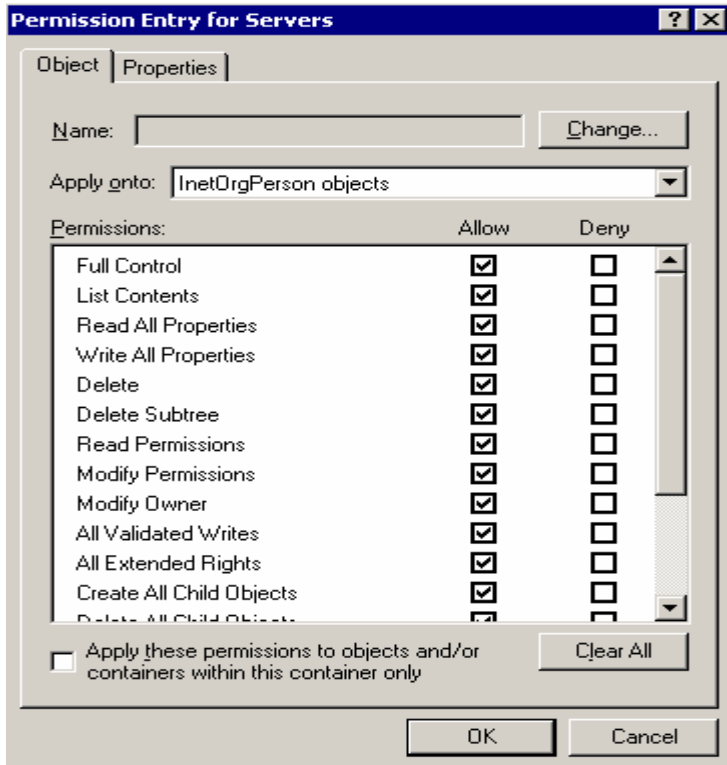
- A. On the domain, grant King the permission to manage user objects.
- B. On the domain, grant King the permission to manage InetorgPerson objects.
- C. On the Sales OU, block the inheritance of permissions.
- D. On the Marketing OU, block the inheritance of permissions.
- E. On the Dev OU, block the inheritance of permissions.

Answer: B, E

Explanation: The administrator named King needs to manage the InetorgPerson objects. We could delegate this task as shown in the exhibit below, but this isn't given as an option.



Instead we can set permissions at the domain level. The permissions shouldn't apply to the Dev OU, so we'll have to block the inheritance of the permissions for the Dev OU.

**QUESTION NO: 102**

You are the network administrator for TestKing. The network consists of a single Active Directory forest that contains five domains. The functional level of the forest is Windows 2000. You have not configured any universal groups in the forest.

One domain is a child domain named usa.testking.com that contains two domain controllers and 50 client computers. The functional level of the domain is Windows Server 2003.

The network includes an Active Directory site named Site1 that contains two domain controllers. Site1 represents a remote clinic, and the location changes every few months. All of the computers in usa.testking.com are located in the remote clinic. The single WAN connection that connects the remote clinic to the main network is often saturated or unavailable. Site1 does not include any global catalog servers.

You create several new user accounts on the domain controllers located in Site1. You need to ensure that users in the remote clinic can always quickly and successfully log on to the domain.

What should you do?

- A. Enable universal group membership caching in Site1.
- B. Add the **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\IgnoreGCFailures** key to the registry on both domain controllers in Site1.
- C. Add the **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\IgnoreGCFailures** key to the registry on all global catalog servers in the forest.
- D. Raise the functional level of the forest to Windows Server 2003.

Answer: B

Explanation:

Native Mode Domain

A native mode domain, where all domain controllers are Windows 2000 domain controllers and the domain has been irrevocably switched to native mode, allows the usage of universal groups. When processing a logon request for a user in a native-mode domain, a domain controller sends a query to a global catalog server to determine the user's universal group memberships. Since you can explicitly deny a group access to a resource, complete knowledge of a user's group memberships is necessary to enforce access control correctly. If a domain controller of a native-mode domain cannot contact a global catalog server to determine universal group membership when a user wants to log on, the domain controller refuses the logon request.

The following registry key can be set so that the domain controller ignores the global catalog server failure when expanding universal groups:

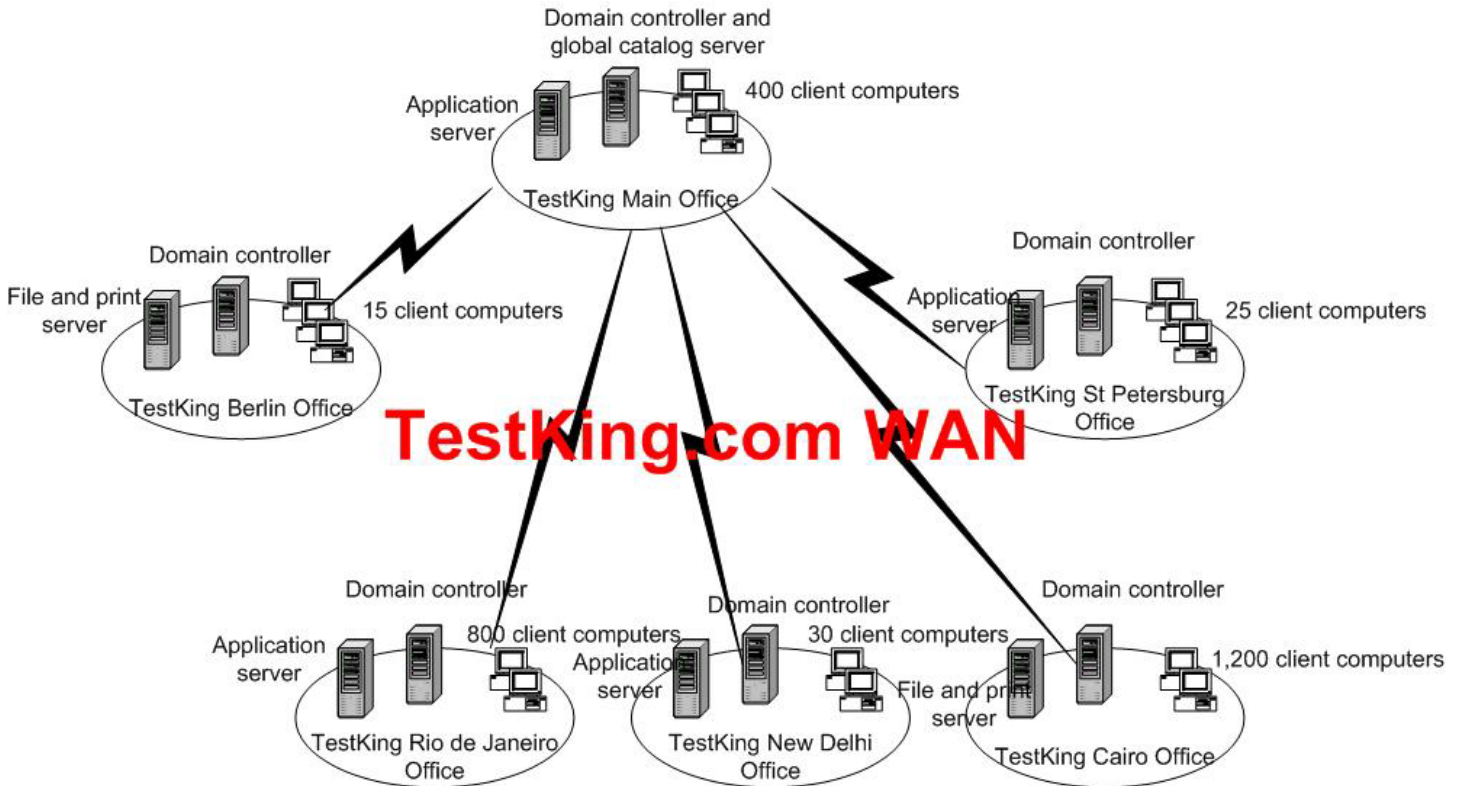
HKEY_LOCAL_MACHINE \System \CurrentControlSet \Control \Lsa \IgnoreGCFailures

The domain controller still tries to connect to the global catalog server, however, and the timeout for that query must expire. For more information on using this registry key, refer to article Q241789 in the Microsoft Knowledge Base.

QUESTION NO: 103

You are a network administrator for TestKing that has a main office and five branch offices. The network consists of six Active Directory domains. All servers run Windows Server 2003. Each office is configured as a single domain. Each office is also configured as an Active Directory site.

TestKing uses an application server that queries user information from the global catalog. You install application servers in the main office and in three branch offices. The network is configured as shown in the exhibit.



You monitor the WAN connections between the main office and each branch office and discover that the utilization increased from 70 percent to 90 percent. Users report slow response times when accessing information on the application server.

You need to place global catalog servers in offices where they will improve the response times for the application servers. You need to achieve this goal with a minimum amount of increase in WAN traffic.

In which office or offices should you place a new global catalog server or servers? (Choose all that apply)

- A. Berlin
- B. Rio de Janeiro
- C. New Delhi
- D. St Petersburg
- E. Cairo

Answer: B, C, D

Explanation:

Because the application server queries Global catalog attributes, we need to put one Global Catalog server in each site hosting an application server; in this case Rio de Janeiro, New Delhi and St Petersburg.

QUESTION NO: 104

You are the network administrator for TestKing, a company with six offices. The network consists of a single Active Directory domain named testking.com.

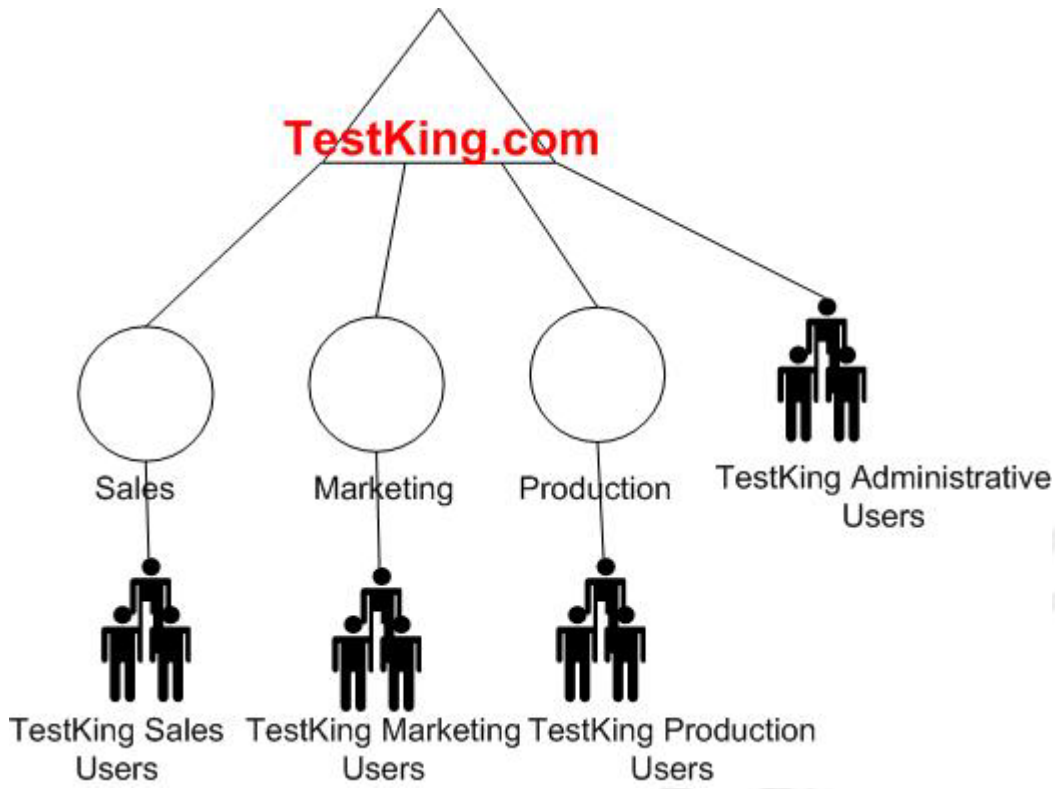
Each office has users who work in the sales, marketing, and production departments. All Active Directory administration is performed by the IT group. The IT group provides a help desk, a level-two support group, and an MIS group. Each office has one employee who works for the help desk group. Administrative responsibilities are listed in the following table.

Group	Role
Help desk	User account maintenance for all employees who are not management
Level-two support	User account maintenance for all employees, the help desk users, and all management users
MIS group	Service account maintenance, maintenance of domain administrator accounts, and built-in accounts in Active Directory

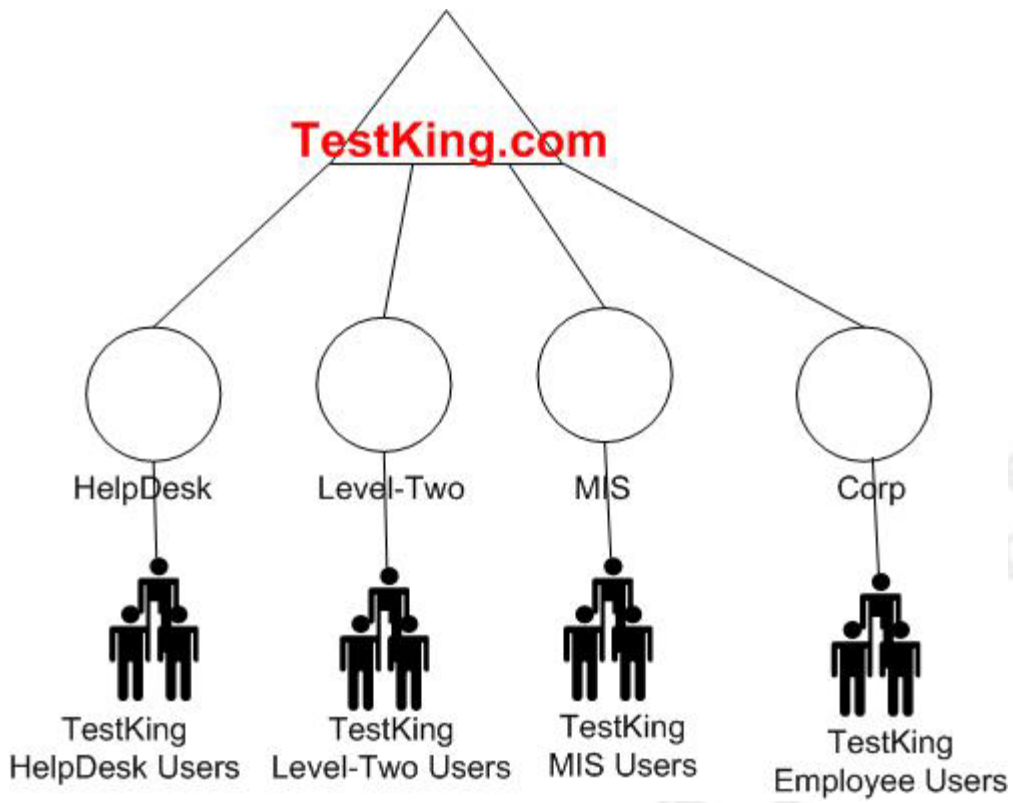
You need to plan an organizational unit (OU) structure that allows delegation of administration. Your plan must ensure that permissions can be maintained by using the minimum amount of administrative effort.

Which OU structure should you use?

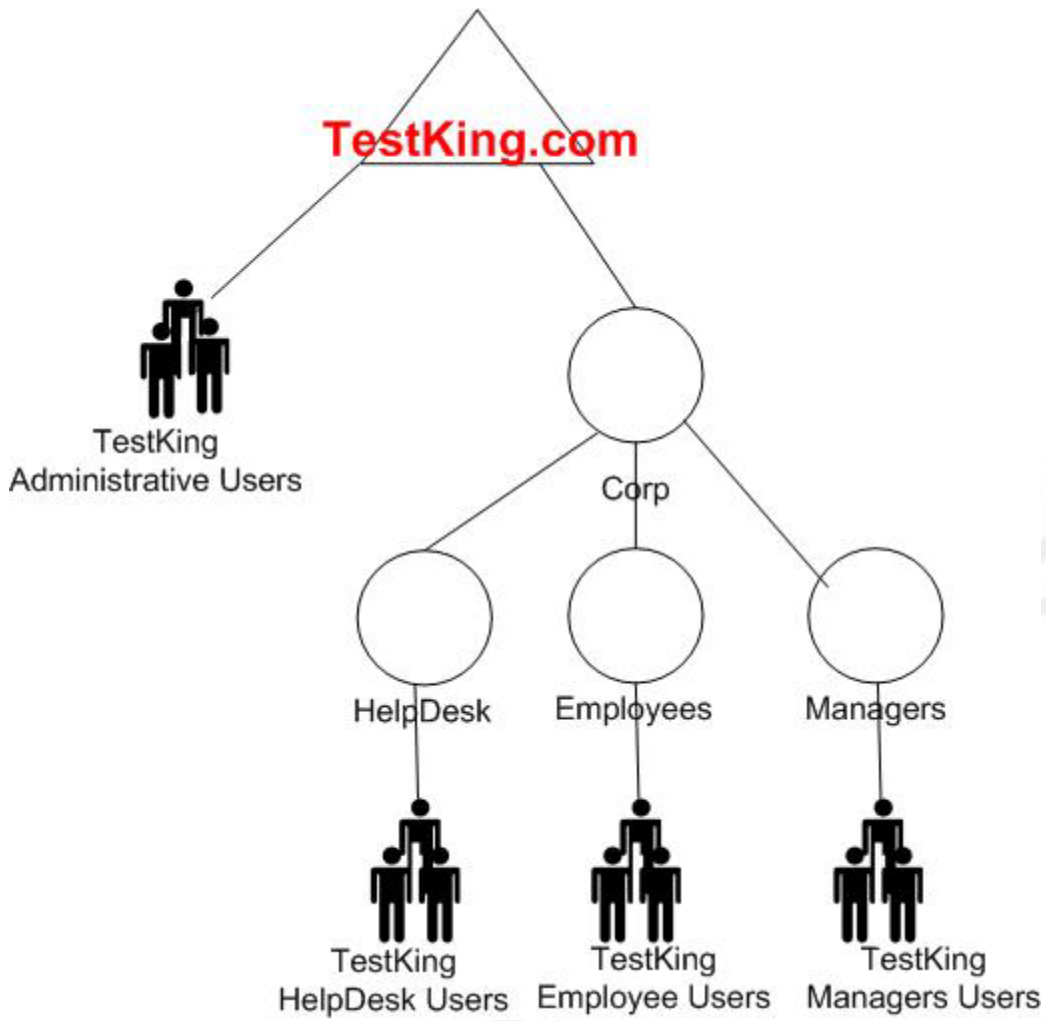
A.



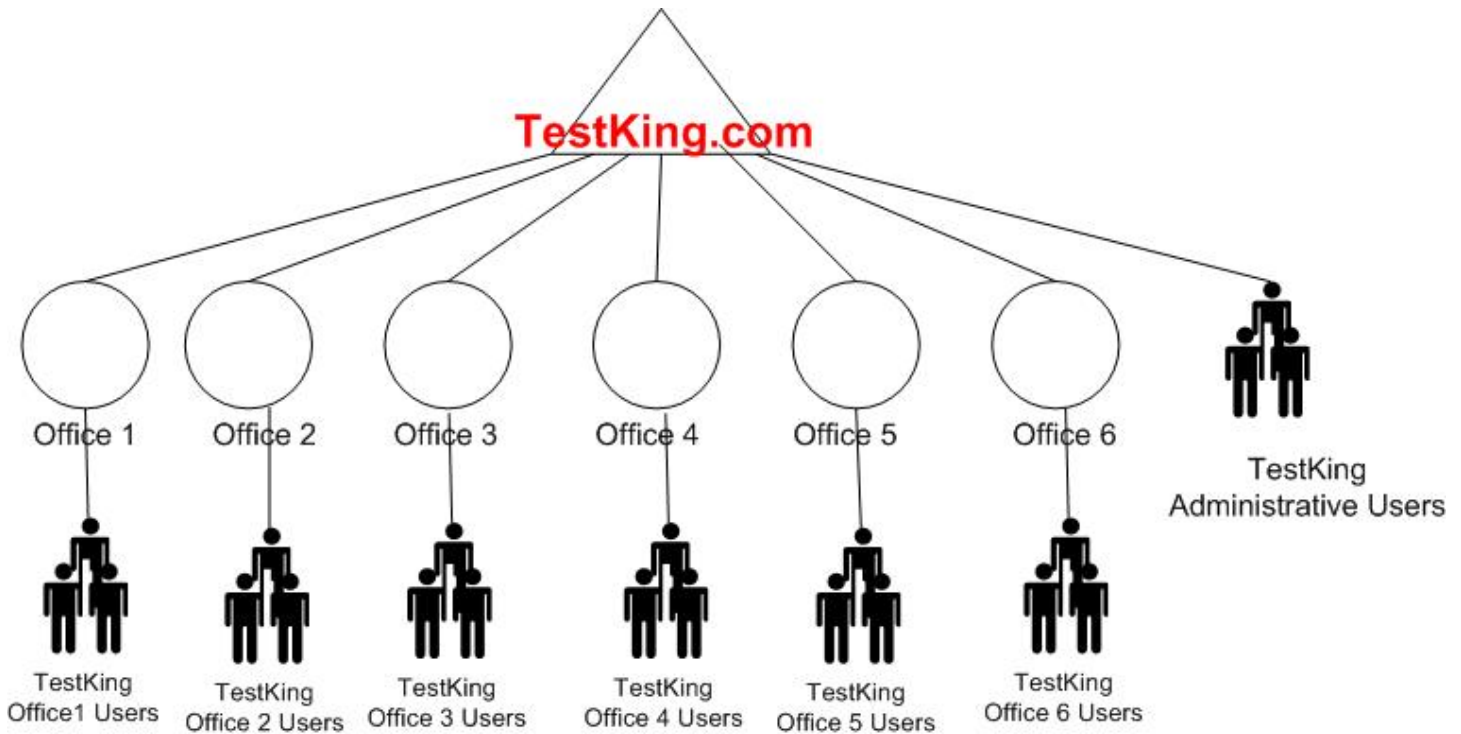
B.



C.



D.



Answer: C

Explanation: We need to delegate the management of different groups of users. We have the non-management employees, who should be managed by the Help Desk staff. We have the employees (including management and help desk staff), who should be managed by the level 2 staff. The MIS group need to manage every other account.

To solution to this question is to delegate the management of user accounts at domain level for the MIS group.

Delegate the management of user accounts to the Employees OU to the help desk staff.

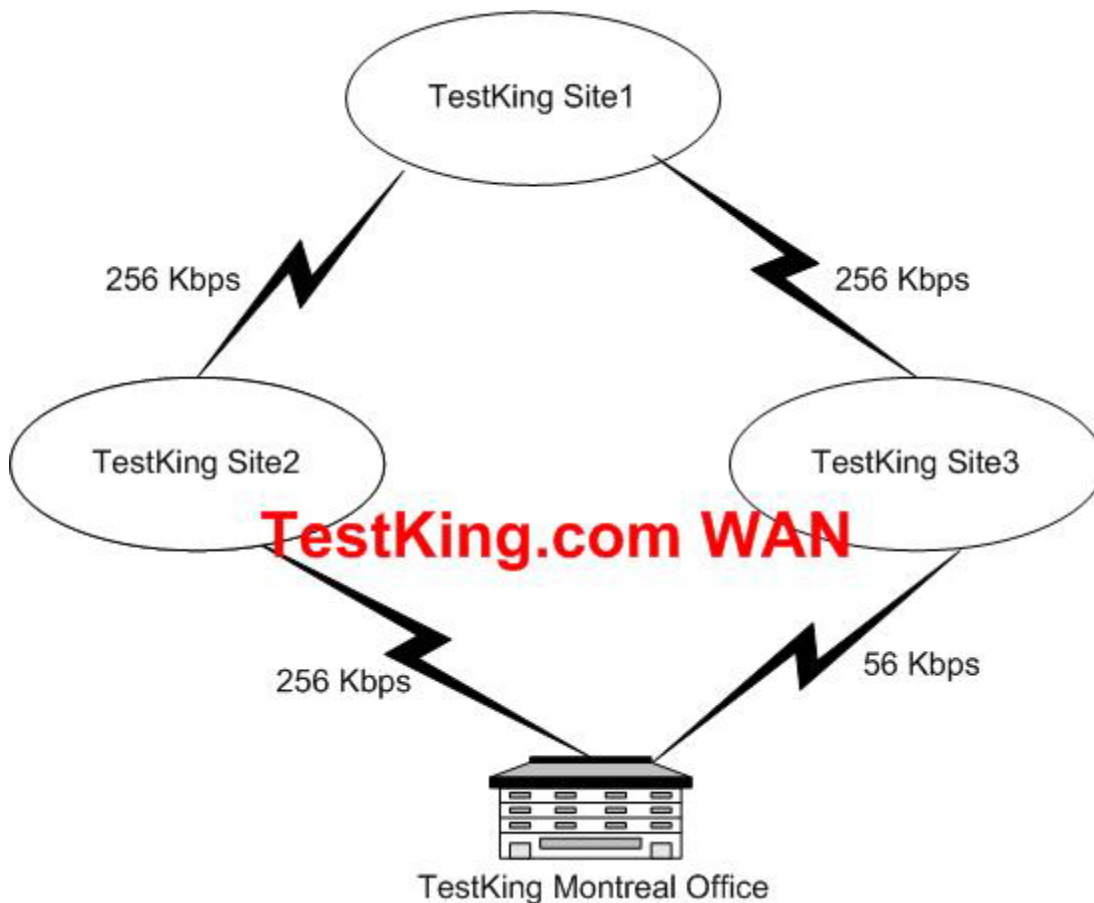
Delegate the management of user accounts to the Corp OU to the second-level support staff.

QUESTION NO: 105

You are the network administrator for TestKing. TestKing has three offices. The network consists of a single Active Directory domain with three sites. Each office is configured as a separate site.

TestKing opens a new branch office in Montreal that has 10 users. This office does not contain a domain controller.

The Montreal Office has WAN connections to two of the existing offices. A router is installed at each of the four offices to route network traffic across the WAN connections. The network after the addition of the Montreal Office is shown in the exhibit.



You need to ensure that when the users in the Montreal office log on the domain during normal operations, they will be authenticated by a domain controller in TestKing Site2.

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

- A. Create a new IP subnet object that includes the subnet used in the Montreal Office. Link the new subnet object to the TestKing Site2 site object.
- B. Create a new IP subnet object that includes the subnet used in the Montreal Office. Link the new subnet object to the TestKing Site3 site object.
- C. Create an additional site for the Montreal Office. Configure a site link to TestKing Site3 with a cost of 300. Configure a site link to TestKing Site2 with a cost of 200.
- D. Create an additional site for the Montreal Office. Configure a site link to TestKing Site2 with a cost of 300. Configure a site link to TestKing Site3 with a cost of 200.
- E. Assign IP addresses to the client computers in the Montreal Office that are on the same IP subnet as the network at Site2.

Answer: A, C

Explanation:

If we create a new subnet for Montreal site and include in this site the DC for that site, all the computers that are in that subnet will logon in the DC of Montreal subnet.

If we create a new site, and configure a site link to TestKing Site3 with a cost of 300 and a site link to TestKing Site2 with a cost of 200, user logons will go over the site link with the lowest cost.

Setting Site Link Properties

Intersite replication occurs according to the properties of the connection objects. When the KCC creates connection objects it derives the replication schedule from properties of the site link objects. Each site link object represents the WAN connection between two or more sites.

Setting site link object properties includes the following steps:

Determining the cost that is associated with that replication path.

- The KCC uses cost to determine the least expensive route for replication between two sites that replicate the same directory partition.
- Determining the schedule that defines the times during which intersite replication can occur.
- Determining the replication interval that defines how frequently replication should occur during the times when replication is allowed as defined in the schedule.

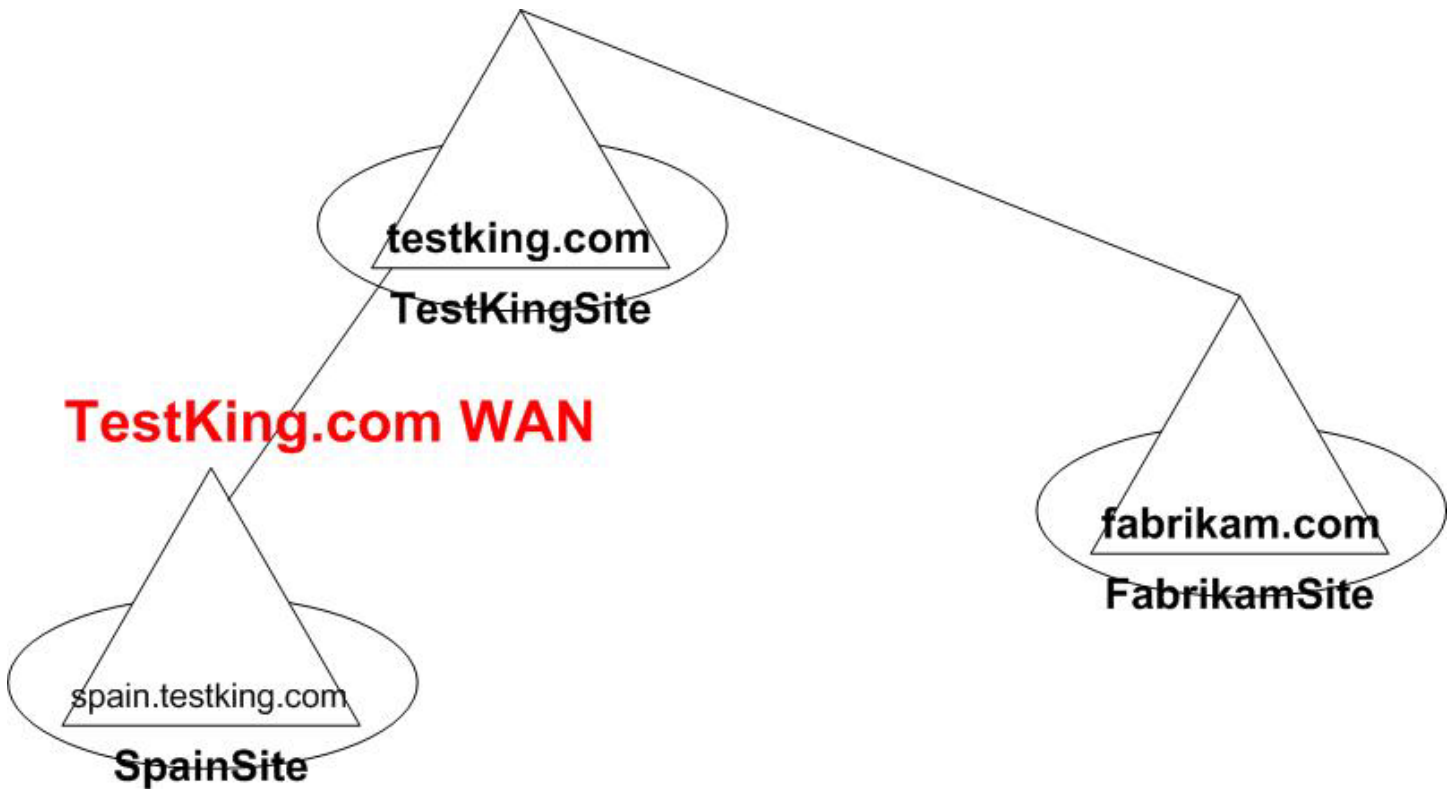
Reference:

MS Windows server 2003 Deployment Kit

Designing and Deploying Directory and Security Services
Setting Site Link Properties

QUESTION NO: 106

You are the network administrator for Acme. Acme consists of two subsidiaries named TestKing and Fabrikam, Inc. The network consists of a single Active Directory forest that contains three domains. The domain and site configuration is shown in the exhibit.



A computer named DC1.spain.testking.com is a domain controller in the spain.testking.com domain. DC1.spain.testking.com is also a global catalog server and the preferred bridgehead server for SpainSite.

The Active Directory database on DC1.spain.testking.com contains 1 GB of data. The Spain departments in TestKing are implementing an Active Directory-enabled application. You expect size of the database on DC1.spain.testking.com to increase by 200 MB.

Active Directory stops responding on DC1.spain.testking.com. You discover that the hard disk has less than 5 MB of space remaining.

You need to configure DC1.spain.testking.com so that Active Directory can restart. You also need to configure the server so that additional space is available on the hard disk for the additional data that will be added to the Active Directory database.

What should you do?

- A. Delete all log files that are located in the NTDS folder.
- B. Install another hard disk in DC1.spain.testking.com.
Use the Ntdsutil utility to move the database to the new hard disk.
- C. Install another hard disk in DC1.spain.testking.com.
Use the Ntdsutil utility to move the transaction logs to the new hard disk.

- D. Configure another server in the site to operate as a preferred bridgehead server.
Configure DC1.spain.testking.com so that it no longer operates as a preferred bridgehead server.

Answer: B

Explanation:

You will need to use the NTDSUTIL command with the 'files' switch. To perform this operation you will need to restart the DC in Directory services restore mode. This operation can not be performed in normal mode, because the database and log are in use.

Ntdsutil

Ntdsutil.exe is a command-line tool that provides management facilities for Active Directory. Use Ntdsutil.exe to perform database maintenance of Active Directory, manage and control single master operations, and remove metadata left behind by domain controllers that were removed from the network without being properly uninstalled. This tool is intended for use by experienced administrators.

Files

Provides commands for managing the directory service data and log files. The data file is called Ntds.dit. At the **files:** prompt, type any of the parameters listed under **Syntax**.

Syntax

{**compact to %s|header | info | integrity|move DB to %s|move logs to %s|recover|set path backup %s|set path db %s|set path logs %s|set path working dir %s**

Parameters

compact to %s (where %s identifies an *empty target directory*)

Invokes Esentutl.exe to compact the existing data file and writes the compacted file to the specified directory. The directory can be remote, that is, mapped by means of the **net use** command or similar means. After compaction is complete, archive the old data file, and move the newly compacted file back to the original location of the data file. ESENT supports online compaction, but this compaction only rearranges pages within the data file and does not release space back to the file system. (The directory service invokes online compaction regularly.)

header

Writes the header of the Ntds.dit data file to the screen. This command can help support personnel analyze database problems.

info

Analyzes and reports the free space for the disks that are installed in the system, reads the registry, and then reports the sizes of the data and log files. (The directory service maintains the registry, which identifies the location of the data files, log files, and directory service working directory.)

integrity

Invokes Esentutl.exe to perform an integrity check on the data file, which can detect any kind of low-level database corruption. It reads every byte of your data file; thus it can take a long time to process large databases. Note that you should always run Recover before performing an integrity check.

move DB to %s(where %s identifies a target directory)

Moves the Ntds.dit data file to the new directory specified by %s and updates the registry so that, upon system restart, the directory service uses the new location.

move logs to %s(where %s identifies a target directory)

Moves the directory service log files to the new directory specified by %s and updates the registry so that, upon system restart, the directory service uses the new location.

recover

Invokes Esentutl.exe to perform a soft recovery of the database. Soft recovery scans the log files and ensures all committed transactions therein are also reflected in the data file. The Windows 2000 Backup program truncates the log files appropriately. Logs are used to ensure committed transactions are not lost if your system fails or if you have unexpected power loss. In essence, transaction data is written first to a log file and then to the data file. When you restart after failure, you can rerun the log to reproduce the transactions that were committed but hadn't made it to the data file.

set path backup %s (where %s identifies a target directory)

Sets the disk-to-disk backup target to the directory specified by %s. The directory service can be configured to perform an online disk-to-disk backup at scheduled intervals.

set path db %s (where %s identifies a target directory)

Updates the part of the registry that identifies the location and file name of the data file. Use this command only to rebuild a domain controller that has lost its data file and that is not being restored by means of normal restoration procedures.

set path logs %s (where %s identifies a target directory)

Updates the part of the registry that identifies the location of the log files. Use this command only if you are rebuilding a domain controller that has lost its log files and is not being restored by means of normal restoration procedures.

set path working dir %s (where %s identifies a target directory)

Sets the part of the registry that identifies the directory service's working directory to the directory specified by %s.

%s

An alphanumeric variable, such as a domain or domain controller name.

quit

Takes you back to the previous menu or exits the utility.

? or help

Displays help at the command prompt.

Reference

SERVER HELP

QUESTION NO: 107

You are the network administrator for TestKing. Your network consists of a single Active Directory domain testking.com. The functional level of the domain is Windows Server 2003.

You add eight servers for a new application. You create an organizational unit (OU) named Application to hold the servers and other resources for the application.

Users and groups in the domain will need varied permissions on the application servers. The members of a global group named Server Access Team need to be able to grant access to the servers. The Server Access Team group does not need to be able to perform any other tasks on the servers.

You need to allow the Server Access Team group to grant permissions for the application servers without granting the Server Access Team group unnecessary permissions.

What should you do?

- A. Create a Group Policy object (GPO) for restricted groups.
Configure the GPO to make the Server Access Team group a member of the Power Users group on each application server.
Link the GPO to the Application OU.
- B. Grant the Server Access Team group permissions to modify computer objects in the Application OU.
- C. Move the Server Access Team group object into the Application OU.
- D. Create domain local groups that grant access to the application servers.
Grant the Server Access Team group permissions to modify the membership of the domain local groups.

Answer: D

Explanation: The simplest way to do this is to create domain local groups with various permissions to the application servers. For example, one group has read access, another group has read and write access and so on. We can then use the Delegation of Control Wizard to grant the right to add or remove members of the groups.

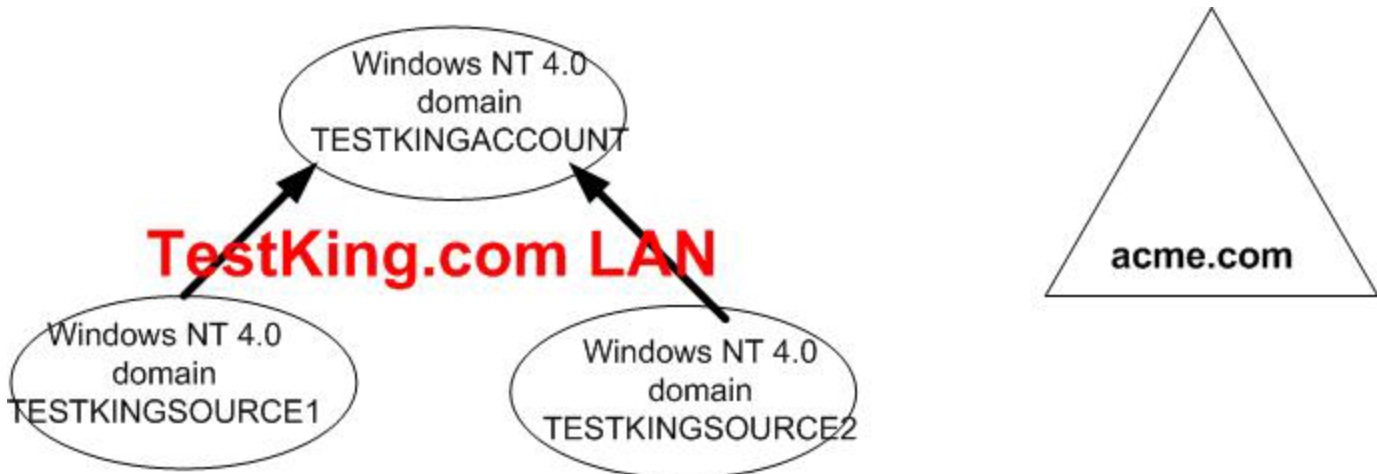
Incorrect Answers:

- A:** The Power Users group can perform many administrative tasks on the servers. This is more permission than necessary.
- B:** They don't need to modify the computer objects. This is more permission than necessary.
- C:** This won't give them the required permissions.

QUESTION NO: 108

You are the network administrator at Acme Inc. The network consists of a single Active Directory forest that contains a single domain named acme.com. The functional level of the forest is Windows Server 2003.

Acme purchase a company named TestKing. The TestKing network consists of one Windows NT 4.0 account domain and two Windows NT 4.0 resource domains, as shown in the exhibit.



All file resources are stored on file servers in the acme.com domain and in the TESTKINGSOURCE1 domain.

You need to accomplish the following goals:

- You need to minimize the number of trust relationships that must be maintained in the network environment.
- Users in each company must be able to access the file resources on the file servers in the other company's domain.

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

- Create a one-way external trust relationship in which the TESTKINGSOURCE1 domain trusts the acme.com domain.
- Create a one-way external trust relationship in which the acme.com domain trusts the TESTKINGSOURCE1 domain.
- Create a one-way external trust relationship in which the acme.com domain trusts the TESTKINGACCOUNT domain.
- Create a one-way external trust relationship in which the TESTKINGACCOUNT domain trusts the acme.com domain.

Answer: C, D

Explanation:

In NT 4.0 the relations between domains are not transitive by default as in Windows 2000 and Windows Server 2003; you need to create it. In the picture we show that the domains TestKingSource1 and TestKingSource2 already trust the TestKingAccount domain. This mean that we can treat this as an entire organization. The

question statement tells us that **Users in each company must be able to access the file resources on the file servers in the other company's domain.**

In this case we need to create one Trust between the root domain, acme.com and the domain where the NT 4.0 accounts reside (TestKingAccount). This way, any user can access the resources in each domain.

QUESTION NO: 109

You are a network administrator for Acme. Acme consists of two subsidiaries named Litware Inc., and TestKing GmbH. The network consists of a single Active Directory forest. The functional level of the forest is Windows Server 2003. The forest contains a forest root domain named litwareinc.com and an additional domain tree named testking.com, which contains two child domains. All domain controllers run Windows Server 2003.

The Directory Services object is configured with the default property settings. The forest contains 250,000 objects that are changed frequently.

You need to be able to restore objects in one of the child domains in the testking.com domain tree from a three-month-old backup. You need to make a change to a Directory Services property on a domain controller in one of the domains in order to achieve this goal.

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

- A. Run the **netdom** command on a domain controller in testking.com.
- B. Use the Ntdsutil utility on a domain controller in litwareinc.com.
- C. Use the ADSIEdit utility on a domain controller in testking.com.
- D. Run the **ldp** command on a domain controller in litwareinc.com.

Answer: C, D

Explanation: We need to edit a property of Active Directory. We can need to use a low level editor to do this.

AdsiEdit. A Microsoft Management Console (MMC) snap-in that acts as a low-level editor for the Active Directory® service. Through the Active Directory Services Interfaces (ADSI), it provides a means to add, delete, and move objects within the Directory Services. The attributes of each object can be viewed, changed, and deleted.

Ldp. A graphical tool that allows users to perform Lightweight Directory Access Protocol (LDAP) operations, such as connect, bind, search, modify, add, and delete, against any LDAP-compatible directory, such as Active Directory. LDAP is an Internet-standard wire protocol used by Active Directory.

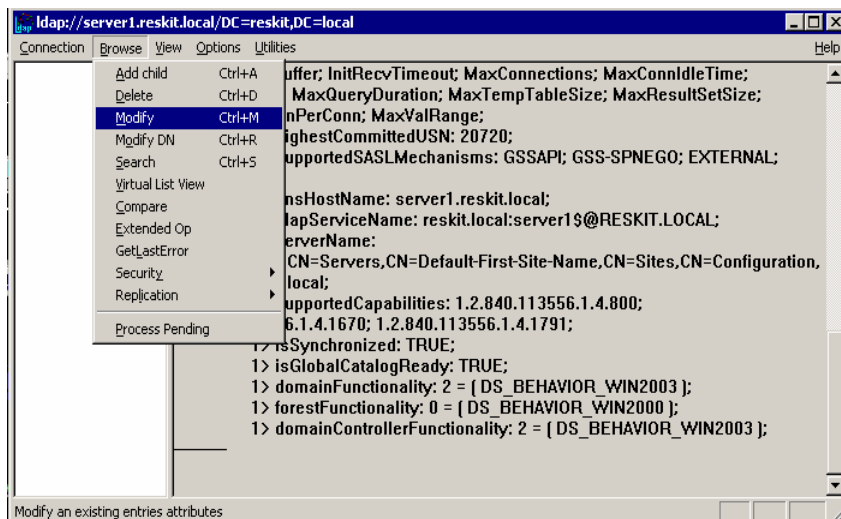
Reference:

<http://support.microsoft.com/default.aspx?scid=http://support.microsoft.com:80/support/kb/articles/Q216/9/93.ASP&NoWebContent=1>

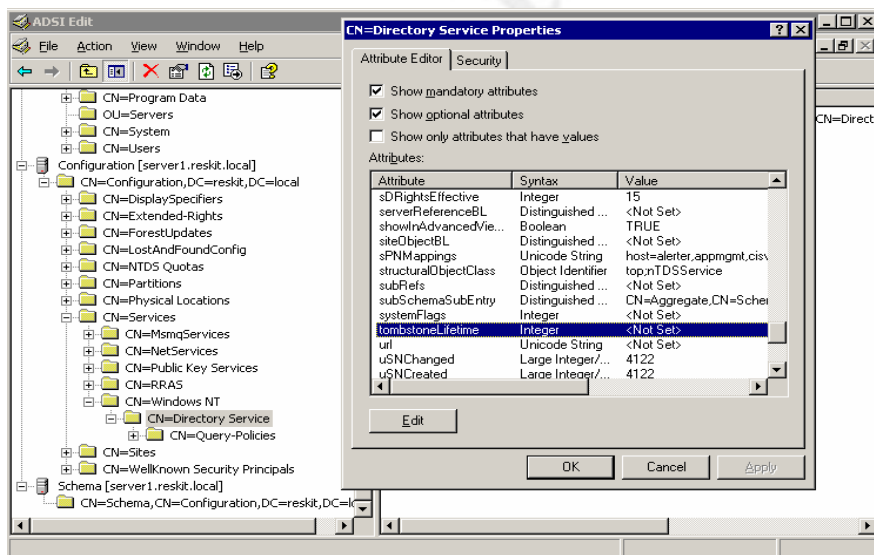
Backup of the Active Directory Has 60-Day Useful Life MS KB article 216993

Use the Active Directory editing tool of your choice so that the "tombstoneLifetime" attribute is set to be older than the backup used to restore the Active Directory. Supported tools include Adsiedit.msc, Ldp.exe, and ADSI Scripts.

LDP provides an interface to perform LDAP operations against Active Directory.



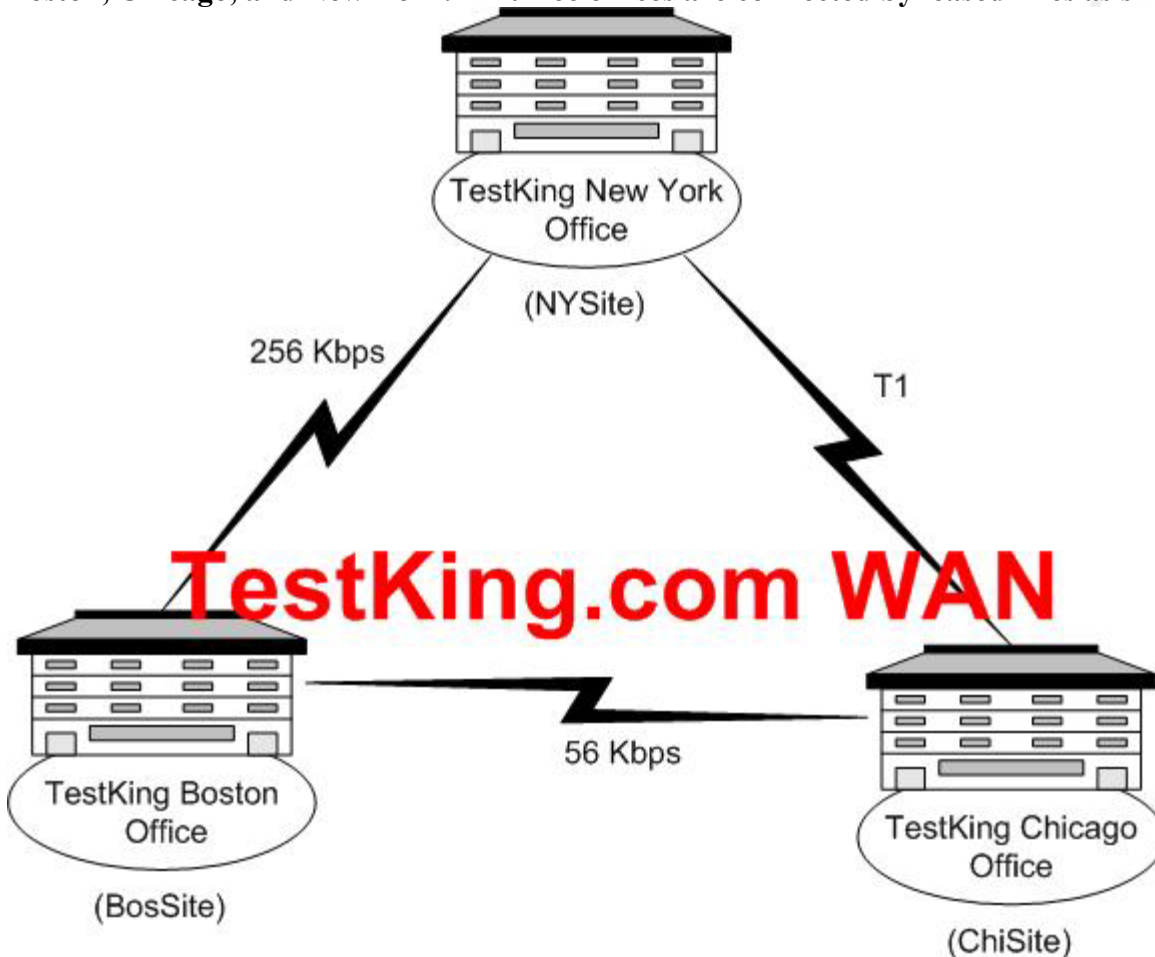
ADSI Edit you can use to edit objects in the Active Directory database.



Leading the way in IT testing and certification tools, www.testking.com

QUESTION NO: 110

You are the network administrator for TestKing, a company that has three offices. The offices are in Boston, Chicago, and New York. All three offices are connected by leased lines as shown in the exhibit.



TestKing is deploying a Windows Server 2003 forest. You create a single Active Directory domain named testking.com. You configure each office as a single site. You configure three domain controllers in NYSite. You create a domain controller in each of the other sites. You create site links based on the network topology. Each leased line is represented by a site link. Each site link connects only two sites. The cost and the schedule for all site links is the same. The sites and site links are named as shown in the following table.

Site link name	Linked site	Linked site
NYBoston	NYSite	BosSite
NYChi	NYSite	ChiSite
ChiBoston	ChiSite	BosSite

Users report that network requests between BosSite and ChiSite are taking much longer than they used to take. You discover that replication traffic is using an unacceptably large percentage of the bandwidth between BosSite and ChiSite

You need to reduce replication traffic over the ChiBoston site link.

What should you do?

- A. Create an SMTP-based connection object from a domain controller in NYSite to a domain controller in BosSite.
- B. Increase the cost of the ChiBoston site link.
- C. Create a site link bridge that includes the NYBoston and NYChi site links.
- D. Increase the replication interval for the NYBoston site link.

Answer: B

Explanation: If we increase the cost of the ChiBoston site link to a value greater than the cost of the other two links added together, then no replication will go over the ChiBoston site link – it will all travel over the NYBoston and the NYChi site links.

Setting Site Link Properties

Intersite replication occurs according to the properties of the connection objects. When the KCC creates connection objects it derives the replication schedule from properties of the site link objects. Each site link object represents the WAN connection between two or more sites.

Setting site link object properties includes the following steps:

Determining the cost that is associated with that replication path.

- The KCC uses cost to determine the least expensive route for replication between two sites that replicate the same directory partition.
- Determining the schedule that defines the times during which intersite replication can occur.
- Determining the replication interval that defines how frequently replication should occur during the times when replication is allowed as defined in the schedule.

Reference:

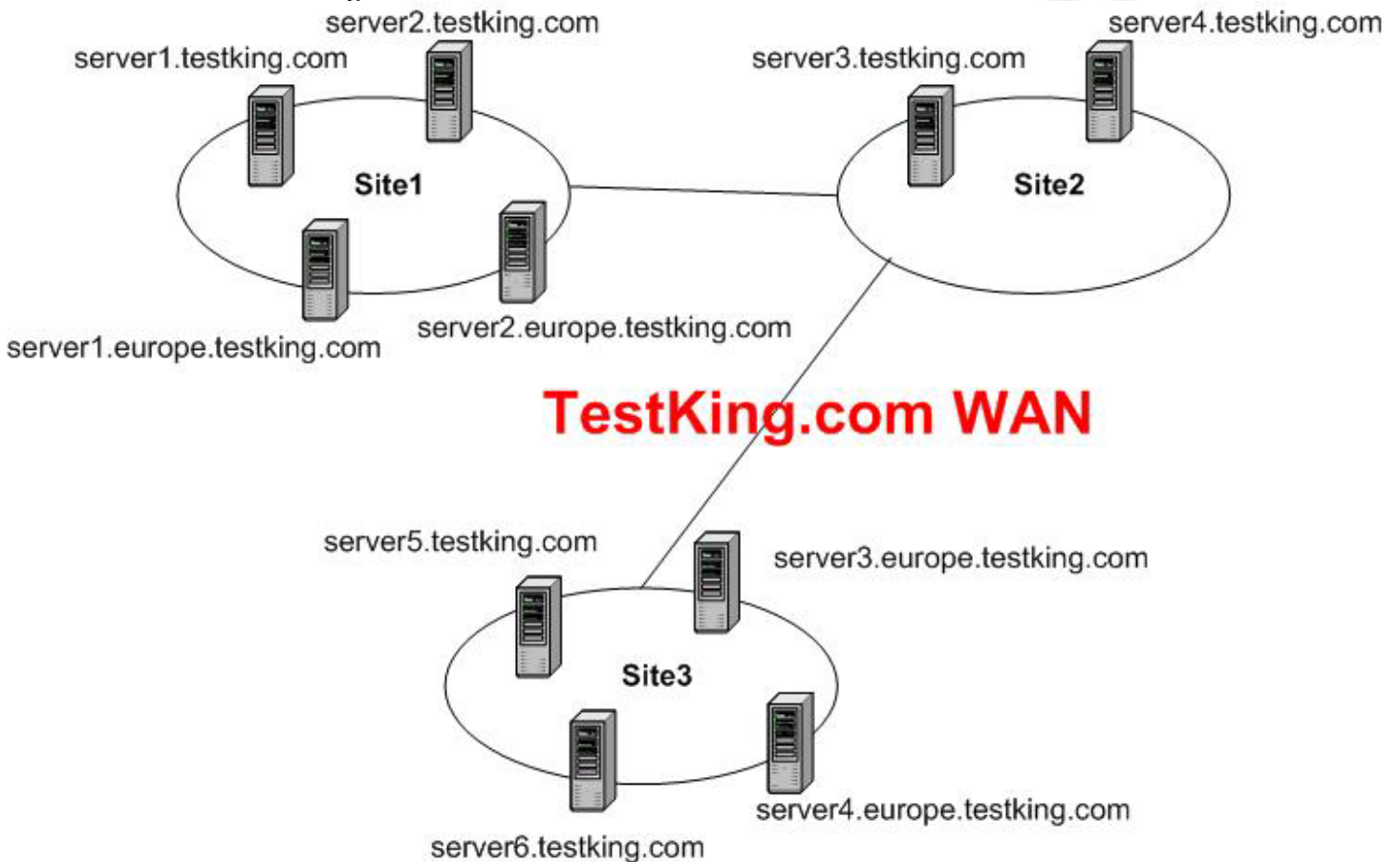
Leading the way in IT testing and certification tools, www.testking.com

MS Windows server 2003 Deployment Kit

Designing and Deploying Directory and Security Services
Setting Site Link Properties

QUESTION NO: 111

You are the network administrator for TestKing. The network consists of a single Active Directory forest that contains one root domain and one child domain. The forest also contains three separate sites, as shown in the Network Diagram exhibit.



The network is not fully routed and there is no direct physical connection between Site1 and Site3. Site links are not bridged.

You discover that the domain controllers for europe.testking.com located in Site1 have additional accounts that are not on the domain controllers for europe.testking.com located in Site3. You examine the directory service log in Event Viewer on a domain controller for europe.testking.com-

Leading the way in IT testing and certification tools, www.testking.com

You discover the error message shown in the Error Message exhibit.

```
Event ID: 1311
Source: NTDS KCC
Category: Knowledge Consistency Checker
Event Type: Error
User: NT AUTHORITY\ANONYMOUS LOGON
COMPUTER: Server1
```

Description: The Directory Service consistency checker has determined that there is not enough physical connectivity published via the Active Directory Sites and Services Manager to create a spanning tree connecting all the sites connecting the Naming Context DC=Europe, DC=testking, DC=com

You need to resolve the condition that is causing this error.

What should you do?

- A. Add a domain controller for the europe.testking.com domain to Site2.
- B. Configure a site link bridge between the site links for Site1 and Site3.
- C. Configure at least one domain controller in each site to be a global catalog server.
- D. Create a site link between Site1 and Site3.

Answer: B

Explanation: We don't have a site link between site1 and site3. We have a site link between Site1 and Site2 and between Site2 and Site3. We have no physical connectivity between site1 and site3, so we should therefore create a site link bridge between the site links for Site1 and Site3. Any replication between site1 and site3 will then travel over the two existing site links.

One computer in any given site owns the role of creating inbound replication connection objects between bridgehead servers from other sites. This domain controller is known as the Inter-Site Topology Generator. While analyzing the Site Link and Site Link Bridge structure to determine the most cost-effective route to synchronize a naming context between two points, it may determine that a site does not have membership in any Site Link and therefore has no means to create a replication object to a bridgehead server in that site.

The first site in the Active Directory (named "Default-First-Site-Name"), is created automatically for the administrator. This site is a member of the default Site Link ("DEFAULTIPSITELINK"), which is also created automatically for the administrator, and is used for RPC communication over TCP/IP. If the administrator were to create two additional sites ("Site1" and "Site2" for example), the administrator must define a Site Link that the site will be a member of before they can be written to the Active Directory.

However, the administrator can open the properties of a Site Link and modify which sites reside in the Site

Link. If the administrator were to remove a site from all Site Links, the KCC displays the error message listed above to indicate that a correction needs to be made to the configuration.

References:

Troubleshooting Event ID 1311: Knowledge Consistency Checker KB article 214745

Incorrect Answers:

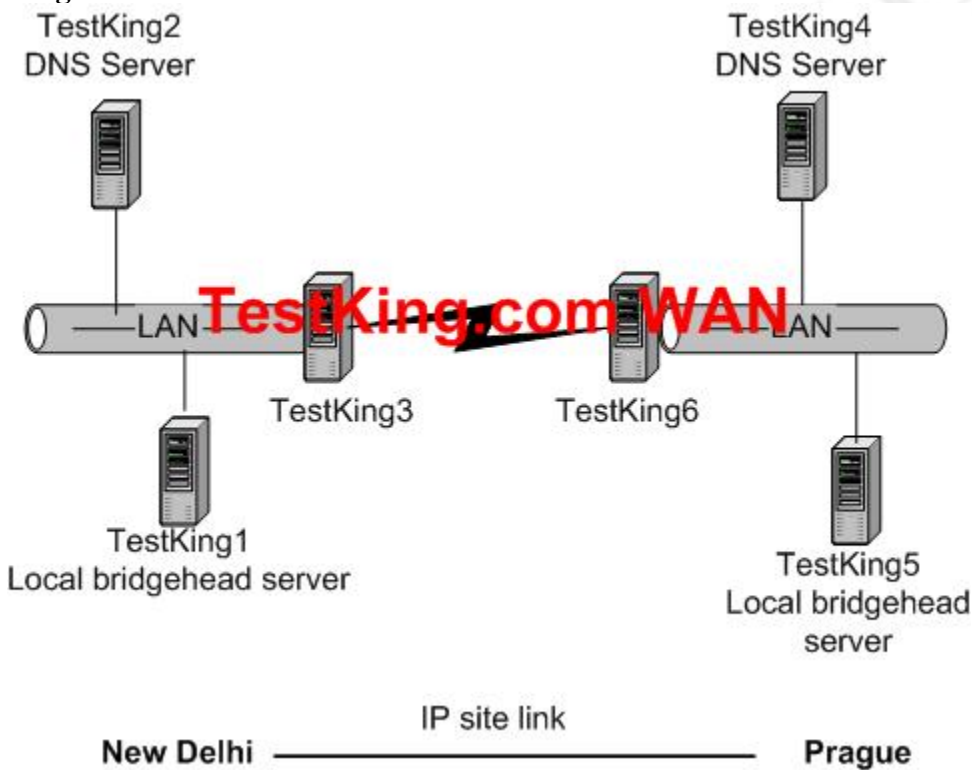
A: This will cause excessive replication traffic between site2 and site3. This defeats the object of using sites to control replication traffic.

C: Global Catalog placement is not the cause of the error in this question.

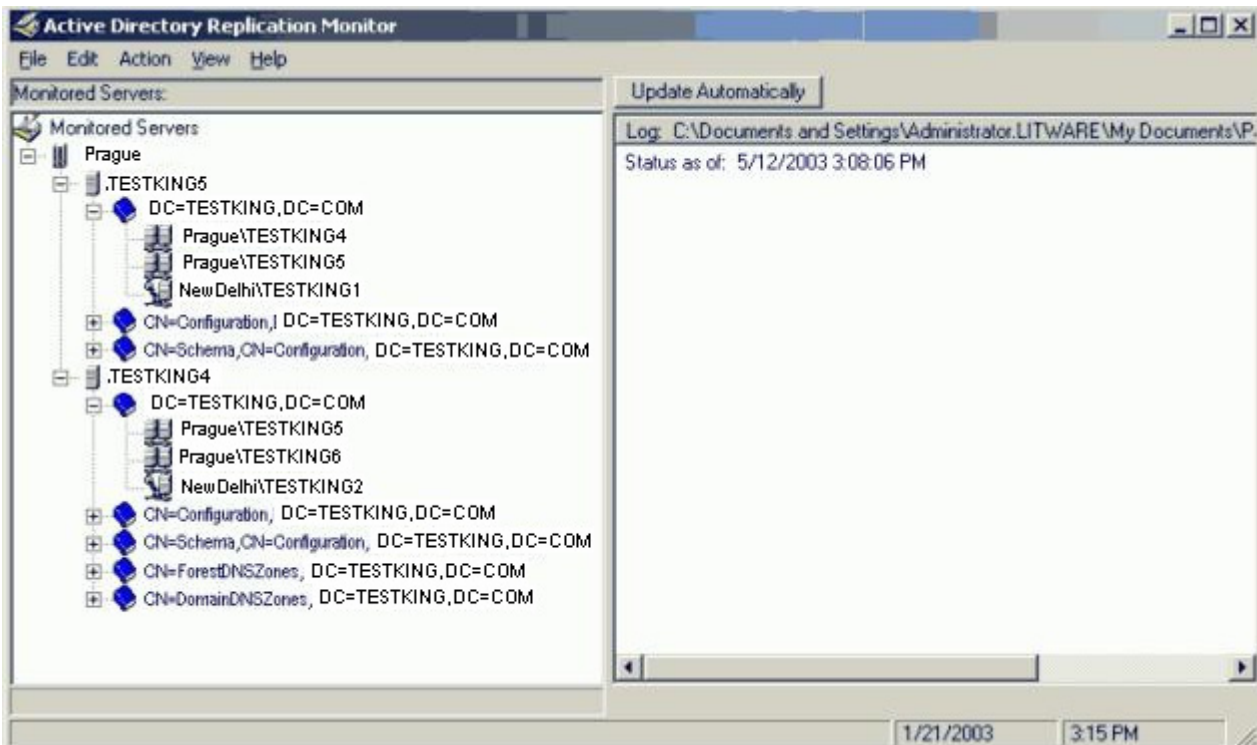
D: We have no physical connectivity between site1 and site3.

QUESTION NO: 112

You are a network administrator for TestKing. The network consists of a single Active Directory domain with two sites. All servers run Windows Server 2003. The network is configured as shown in the Network Diagram exhibit.



You use Replication Monitor to monitor Active Directory replication. You discover that replication connections are being established as shown in the Replication Monitor exhibit.



You need to ensure that replication takes place only between defined preferred bridgehead servers. You need to accomplish this task without incurring any additional replication traffic.

What should you do?

- A. Configure TestKing1 and TestKing5 as additional DNS servers.
- B. Configure TestKing3 and TestKing6 as additional DNS servers.
- C. Configure only TestKing2 and TestKing4 as preferred bridgehead servers.
- D. Configure only TestKing3 and TestKing4 as preferred bridgehead servers.

Answer: C

Explanation:

When two sites are connected by a site link, the replication system automatically creates connections between specific domain controllers in each site called *bridgehead servers*. In Microsoft® Windows® 2000, intersite replication of the directory partitions (e.g. domain, configuration, and schema) between domain controllers in different sites is performed by the domain controllers (one per directory partition) in those sites designated by the KCC as the bridgehead server. In Windows Server 2003, the KCC may designate more than one domain controller per site hosting the same directory partition as a candidate bridgehead server. The replication connections created by the KCC are randomly distributed between all candidate bridgehead servers in a site to

share the replication workload. By default, the randomized selection process takes place only when new connection objects are added to the site.

However, you can run Adlb.exe, a new Windows Resource Kit tool called Active Directory Load Balancing (ADLB) to rebalance the load each time a change occurs in the site topology or in the number of domain controllers the site. In addition, ADLB can stagger schedules so that the outbound replication load for each domain controller is spread out evenly across time. Consider using ADLB to balance replication traffic between the Windows Server 2003–based domain controllers when they are replicating to more than 20 other sites hosting the same domain

QUESTION NO: 113

You are a network administrator for TestKing. The network consists of a single Active Directory domain with two sites. The Active Directory database is backed up every evening.

A network administrator in Site1 deletes an empty organizational unit (OU) named Projects. At about the same time, a network administrator in Site2 moves 20 existing user accounts into the Projects OU. Later, the administrator in Site2 discovers that the Projects OU was deleted from Active Directory. He cannot see the user accounts that he moved into the OU.

You need to provide an OU named Projects and add the 20 user accounts to the Projects OU. The users' access to network resources must not be affected by this process.

What should you do?

- A. Perform an authoritative restore operation of the Projects OU and the user accounts on a domain controller in Site2.
- B. Perform a nonauthoritative restore operation of the Projects OU and the user accounts on a domain controller in Site2.
- C. Create a new OU named Projects.
Create 20 new user accounts that have the same user principal name (UPN) prefix.
Move the user accounts into the new Projects OU.
- D. Create a new OU named Projects.
Move the 20 user accounts from the LostAndFound container to the new Projects OU.

Answer: D

Explanation: You moved the users to an OU that had just been deleted. When you move objects to an object that is no longer there, the objects get moved to the LostAndFound container. This means that we haven't lost the user accounts, so we can just re-create the Projects OU and move the users from the LostAndFound container to the new OU.

Incorrect Answers:

A: The user accounts haven't been deleted, so we don't need to restore them.

B: The user accounts haven't been deleted, so we don't need to restore them.

C: The user accounts haven't been deleted, so we don't need to recreate them. Furthermore, recreating the user accounts in this way will not work to restore the original accounts. The new accounts will be different accounts with different SIDs (Security Identifiers).

QUESTION NO: 114

You are the network administrator for TestKing. The network consists of a single Active Directory forest that contains three domains named testking.com, usa.testking.com, and europe.testking.com. The functional level of the forest is Windows Server 2003.

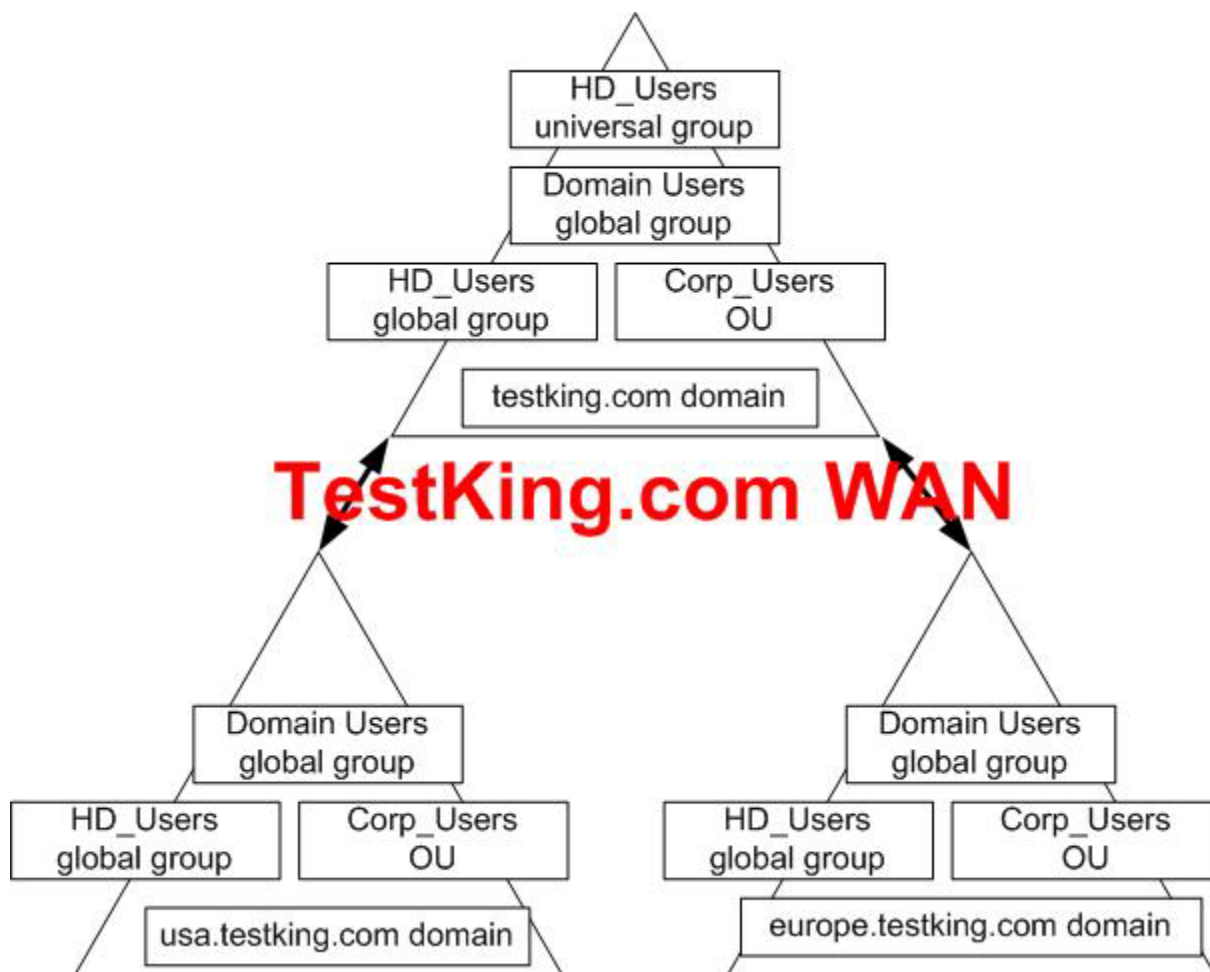
The help desk department is responsible for resetting passwords for all user accounts in the forest except for accounts that have administrative privileges. There is an organizational unit (OU) named Corp_Users in each domain that contains the user accounts in that domain. All of the user accounts that have administrative privileges are in the default Users container in each domain.

There is a universal group named HD_Users in the testking.com domain. All user accounts for the help desk department users are members of the HD_Users group.

You need to delegate the required authority for resetting passwords to the users in the help desk department.

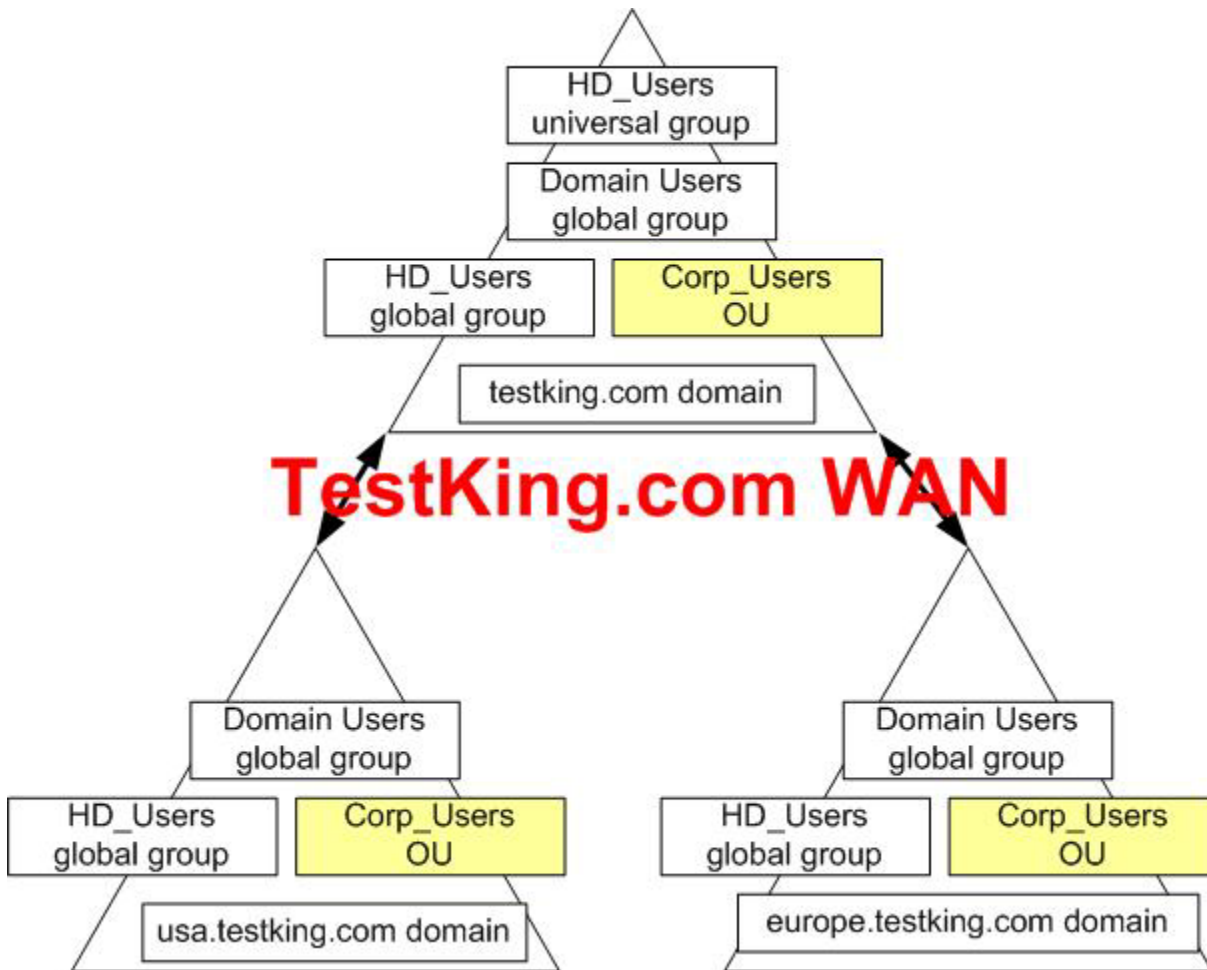
For which Active Directory component or components should you delegate control?

To answer, select the appropriate component or components in the work area.



Answer:

Select the Corp_Users OU in each domain.



Explanation: We need to delegate the required authority for resetting passwords for the Corp_Users OU to the HD_Users universal group. The Corp_Users OU in each domain contains the users that the help desk staff need to reset passwords for. The HD_Users universal group contains the help desk staff and is visible to all domains in the forest.

QUESTION NO: 115

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.

TestKing's written security policy requires the following account polices:

- User accounts must be automatically locked out in the event of three consecutive failed logon attempts within a 30-minutes period.
- Manual administrative action must be required to unlock a user account.

You need to configure the account policies for the domain to comply with the security requirements.

What should you do?

To answer, drag the appropriate account policy setting or settings to the correct location or locations in the work area.

Account Policy Settings
Select from these

30 0 99
999 3 2

Place here

setting Account lockout duration
setting Account lockout threshold
setting Reset account lockout counter after

Answer:

Account Policy Settings
Select from these

99
999 2

Place here

0 Account lockout duration
3 Account lockout threshold
30 Reset account lockout counter after

Account lockout duration

This security setting determines the number of minutes a locked-out account remains locked out before automatically becoming unlocked. **The available range is from 0 minutes through 99,999 minutes.** If you set the account lockout duration to 0, the account will be locked out until an administrator explicitly unlocks it. If an account lockout threshold is defined, the account lockout duration must be greater than or equal to the reset time.

Default: None, because this policy setting only has meaning when an Account lockout threshold is specified.

Account lockout threshold

This security setting determines the number of failed logon attempts that causes a user account to be locked out. A locked-out account cannot be used until it is reset by an administrator or until the lockout duration for the account has expired. You can set a **value between 0 and 999 failed logon attempts.** If you set the value to 0, the account will never be locked out.

Reset account lockout counter after

This security setting determines the number of minutes that must elapse after a failed logon attempt before the failed logon attempt counter is reset to 0 bad logon attempts.

The available range is 1 minute to 99,999 minutes.

Failed password attempts against workstations or member servers that have been locked using either CTRL+ALT+DELETE or password-protected screen savers count as failed logon attempts.

QUESTION NO: 116

You are the network administrator for TestKing. TestKing consists of a single Active Directory domain named testking.com. TestKing has a main office and a branch office. The domain contains four domain controllers. Two domain controllers are located in the main office, and two domain controllers are located in the branch office.

You create a Group Policy object (GPO) named WPSoft and link it to the domain. You configure WPSoft to assign a word processing application to the User Configuration section of the GPO. Users in the branch office report that the application is not available to use. Users in the main office report that they can use the application.

You need to ensure that the users at the branch office receive the word processing application.

What should you do?

- A. Synchronize the Netlogon shared folder on both domain controllers in the branch office.
- B. Force replication between the domain controllers in the main office and the branch office.
- C. Run the **gpresult** command on the client computers in the branch office.
- D. Run the **gpoutil** command on a client computer in the branch office.

Answer: B

Explanation: We have created a GPO and linked it to the domain. The domain controllers will receive the new group policy at the next replication interval. Alternatively, we can force replication between the domain controllers in the main office and the branch office by running the `gpupdate /force` command.

Incorrect Answers:

A: We need to initiate AD replication between the main office and the branch office.

C: This will have no effect as the domain controllers in the branch office haven't received the new GPO yet.

D: This will have no effect as the domain controllers in the branch office haven't received the new GPO yet.

QUESTION NO: 117

You are the network administrator for TestKing. The network consists of a single Active Directory domain named testking.com that contains two domain controllers. Both domain controllers run Windows Server 2003. All client computers run Windows XP Professional. The only account in the Domain Admins security group is the Administrator account in the domain. Each night, a full backup is made of the hard disks in each domain controller.

You disable the local Administrator account in the Default Domain Policy Group Policy object (GPO).

You discover that you are no longer able to log on to either domain controller as the Administrator from the domain.

You need to ensure that you can log on to both domain controllers as the Administrator from the domain.

What should you do?

- A. Restart one domain controller in Safe Mode.
Log on as Administrator.
Create an account for a second administrator.
Restart the domain controller and use the new account to remove the restrictions on the local Administrator accounts.
- B. Restore the entire hard disk on one domain controller by using the last nightly backup before the change was made.
Restart the domain controller.
Allow time for Active Directory replication to complete.
- C. Restart one domain controller and use a Windows Server 2003 CD to run the Recovery Console.
Stop the GPC service.
Restart the domain controller.
- D. Restart one domain controller in Directory Services Restore Mode.
Perform an authoritative restore operation of the Domain Controllers OU in Active Directory from the last nightly backup before the change was made.
Restart the domain controller.

Answer: A

Explanation: The default domain group policy object is disabling the Administrator accounts. When you restart a domain controller in safe mode, the group policy doesn't apply, so the administrator account isn't disabled. You need to start the computer in Safe Mode with Networking. This will enable you to access Active Directory Users and Computers. You can't modify existing objects, but you can create a new administrative account. Then you can reboot in normal mode and log in using the new administrative account and the new account to remove the restrictions on the local Administrator accounts.

Incorrect Answers:

B: It is not necessary to restore the entire hard disk. Furthermore, this won't work, because the GPO would replicate to the restored server and you'd be back to square one.

C:

D: The default domain group policy would still apply to the restored domain controller objects, so the administrator account will be disabled.

QUESTION NO: 118

You are the network administrator for TestKing. Your network consists of a single Active Directory domain testking.com. All servers run Windows Server 2003. You use Group Policy objects (GPOs) to distribute software.

TestKing uses two different applications to view graphics. Users are allowed to choose which program they will use based on the features and formats they require. Only the users are allowed to decide which of these two applications will be installed.

You need to configure the GPOs to install either graphics application based on the user's choice.

What should you do?

- A. Publish both applications with file extension activation.
- B. Publish both applications without file extension activation.
- C. Assign both applications to install on demand.
- D. Assign both applications to complete a full installation.

Answer: B

Explanation: You can publish applications to users, making the application available for users to install. To install a published application, users can use Add or Remove Programs in Control Panel, which includes a list of all published applications that are available for them to install.

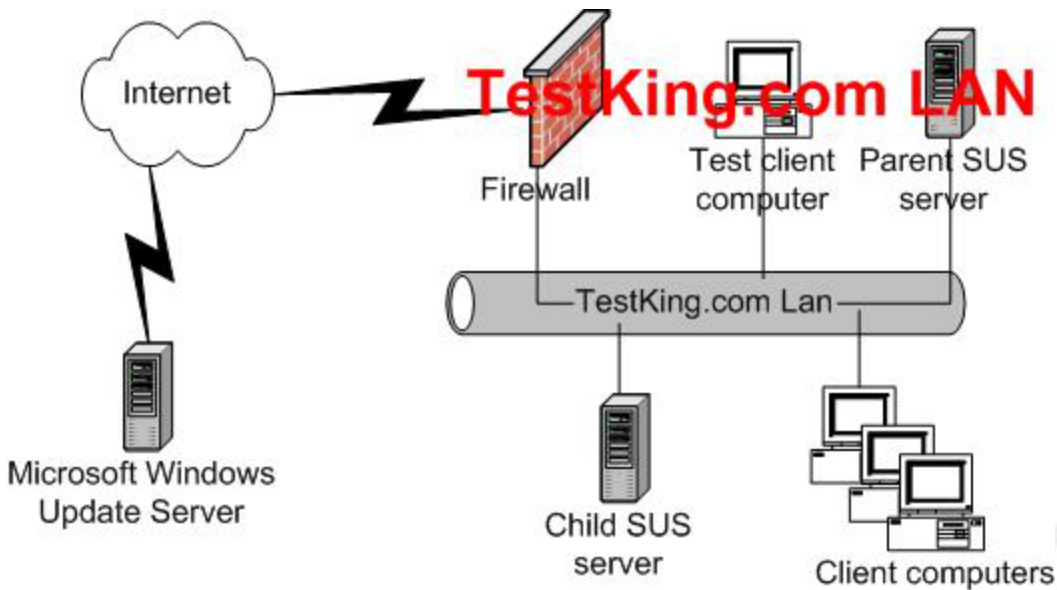
Incorrect Answers:

- A:** Only one application will install when a file is opened. The users won't have the choice.
- C:** The applications should be published, not assigned.
- D:** This doesn't make sense.

QUESTION NO: 119

You are the network administrator for TestKing. TestKing consists of a single Active Directory domain named testking.com. All servers run Windows Server 2003. All client computers run Windows XP Professional. All computer accounts for the client computers are located in an organizational unit (OU) named Computer Accounts. All user accounts are located in an OU named User Accounts.

Software Update Services (SUS) is installed on your network. The SUS infrastructure is shown in the exhibit.



Updates that are deployed must not cause any conflicts or errors on the client computers.

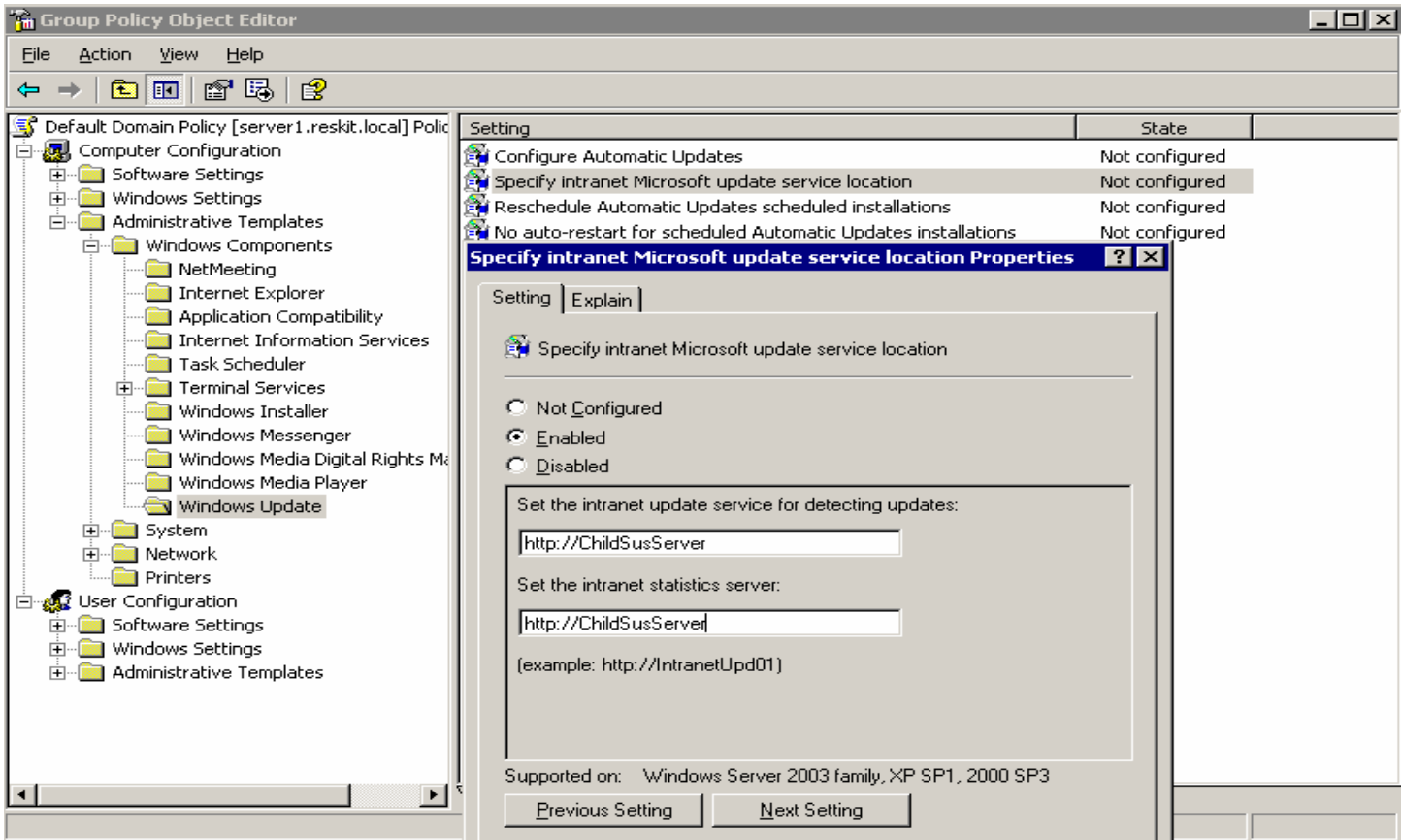
You need to configure the client computers to download approved updates from the correct server.

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

- A. Create a Group Policy object (GPO) to set the default package location to be the internal interface of the firewall.
- B. Create a Group Policy object (GPO) to set the default package location to be the child SUS server.
- C. Create a Group Policy object (GPO) to set the update service location to be the child SUS server.
- D. Create a Group Policy object (GPO) to set the update service location to be the Microsoft Windows Update server.
- E. Link the Group Policy object (GPO) to the User Accounts OU.
- F. Link the Group Policy object (GPO) to the Computer Accounts OU.

Answer: C, F

Explanation: You will need to specify the child SUS server and to link the policy to the computer accounts OU. Only approved updates can be downloaded and installed from the child SUS server.

**QUESTION NO: 120**

You are the systems engineer for TestKing, Ltd. The company is in the process of migrating from a Windows NT 4.0 domain-based network to a Windows Server 2003 Active Directory domain-based network.

The company currently has the DNS domain name testking.com registered for use for the company Web site and e-mail addresses. The testking.com domain namespace is currently hosted on DNS servers that are owned by the company's ISP. A firewall separates the publicly accessible network from the internal company network.

Company IT policy for the new directory services infrastructure includes the following requirements:

- All Active Directory data must be isolated from external users.
- The internal DNS namespace must be isolated from external users.

You install a Windows 2003 Server computer on the internal network, and you install the DNS Server service on the server.

You need to plan the new namespace design for TestKing. Your plan must comply with the company IT policy.

What should you do?

- A. Create a primary zone named ad.Testking.com on the internal DNS server.
- B. Create a secondary zone named Testking.com on the internal DNS server.
- C. Create a stub zone named ad.Testking.com on the internal DNS server.
- D. Create a delegation record on the ISP's DNS server for the internal DNS server.
- E. Configure zone transfers between the ISP's DNS server and the internal DNS server.

Answer: A

Explanation: We need a primary zone on the internal DNS server for the Active Directory. The only answer listed that gives a primary zone as an option is answer A.

Incorrect Answers:

B: This would enable use to resolve host addresses in the testking.com domain quicker than going through the internet DNS hierarchy, but it's not necessary and doesn't address the requirements set out in the question.

C: We need a primary zone on the internal DNS server for the Active Directory, not a stub zone.

D: This isn't necessary. No external DNS server needs to know about the internal zone.

E: This would enable use to resolve host addresses in the testking.com domain quicker than going through the internet DNS hierarchy, but it's not necessary and doesn't address the requirements set out in the question.

QUESTION NO: 121

You are the network administrator for TestKing. All Web servers on the network run Windows 2000 Server. The Web servers run several applications, including a collaborative Web-based application that uses ASP.NET and Web Distributed Authoring and Versioning (WebDAV).

You plan to migrate the Web servers to Windows Server 2003. You use the Configure Your Server Wizard to configure a Windows Server 2003 computer as an application server, and you enable ASP.NET in the process.

You install the Web-based application on the server.

Users now report that when they attempt to access the collaborative Web-based application, they receive the error message shown in the exhibit.



You need to enable the collaborative Web-based application to function on Windows Server 2003 while maintaining Web server security.

What should you do?

- A. Use IIS Manager to disable anonymous access.
- B. Use IIS Manager to allow the WebDAV Web service extension and to allow Httpext.dll.
- C. Use IIS Manager to grant the users of the Web-based application permissions for the default Web site.
- D. Use IIS Manager to allow the Active Server Pages Web service extension and to allow Asp.dll.

Answer: D

Explanation: By default, when Internet Information Services (IIS) is installed on any version of the Microsoft Windows Server 2003 family, IIS only serves static content (HTML). When you request dynamic content, such as Active Server Pages (ASP) or ASP.NET pages, you receive one of the following error messages:

HTTP Error 404 - File Not Found

-or-

HTTP Error 404- File or Directory not found

To permit IIS to serve other types of content, the administrator must unlock this content in the Web service extensions node in the IIS management console. To do this, either enable a pre-existing Web service extension or add a new Web service extension.

Incorrect Answers:

A: This is not a permissions problem. You can run ASP content with anonymous access enabled if you want to.

- B:** Webdav is used to access files over http. It is not required to run ASP content.
C: This is not a permissions problem. A permissions problem would return a different error message.

QUESTION NO: 122

You are the network administrator for TestKing. All servers run Windows Server 2003. All client computers run Windows XP Professional. All computers are connected to the network by using a wireless access point.

You configure a certification authority (CA). You require certificate-based IEEE 802.1x authentication on the wireless access point.

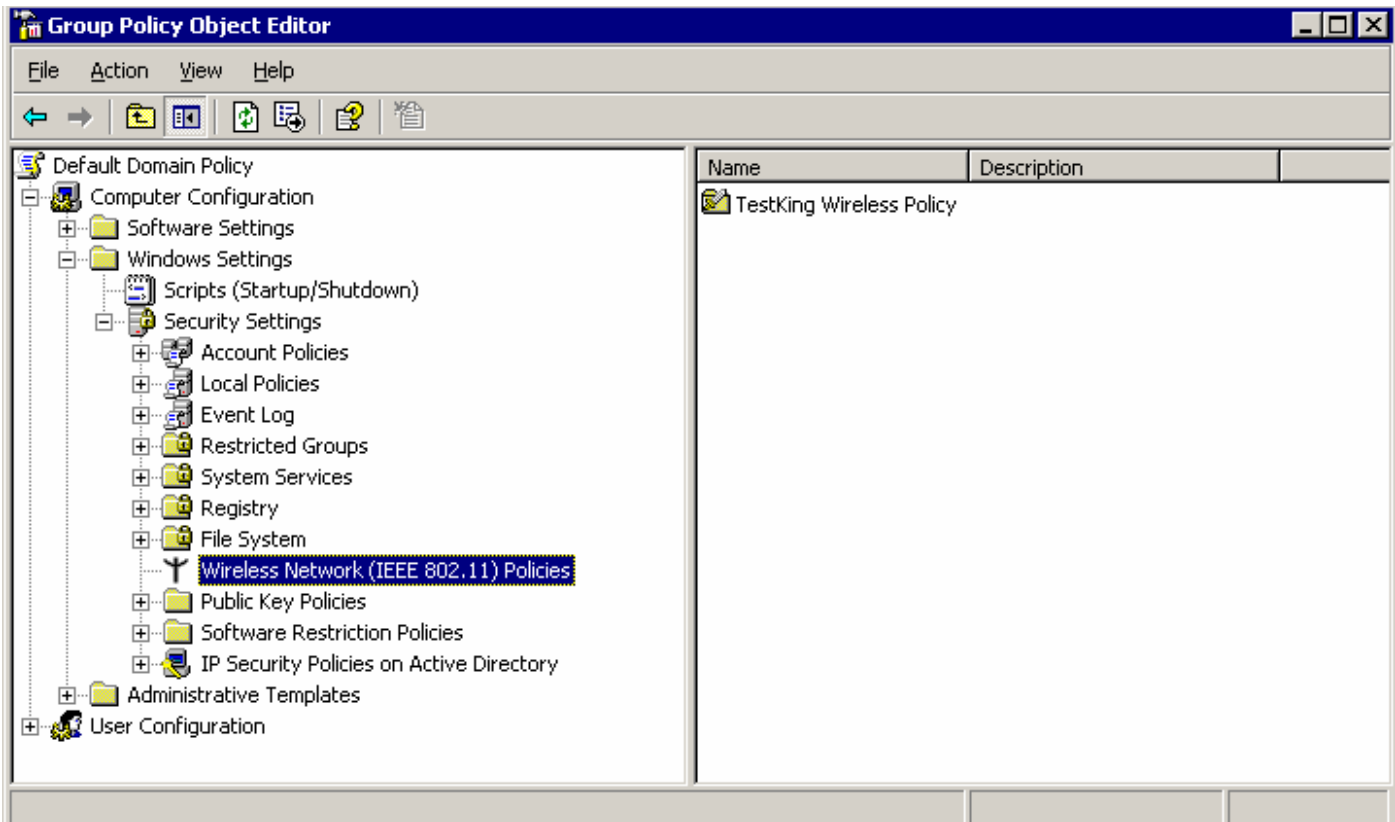
You need to enable all computers to communicate on the wireless network.

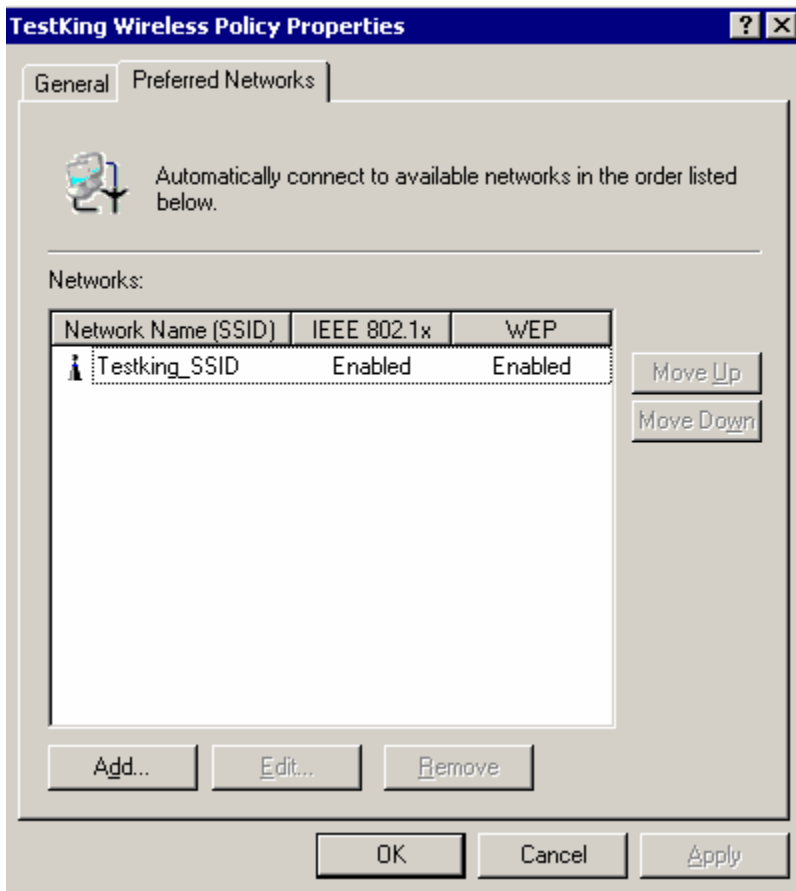
What are two possible ways to achieve this goal? (Each correct answer presents a complete solution. Choose two)

- A. Enter a 128-bit Wired Equivalent Privacy (WEP) key on the wireless access point and on the computers.
- B. In 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 disk.

Answer: A, B

Server Setup part:





Edit Testking_SSID Properties ? X

Network Properties | IEEE 802.1x

Network name (SSID):
Testking_SSID

Description:
Policy to access WIFI area in TestKing Domain

Wireless network key (WEP)
This network requires a key for the following:

- ☒ Data encryption (WEP enabled)
- ☐ Network authentication (Shared mode)
- ☒ The key is provided automatically

☐ This is a computer-to-computer (ad hoc) network; wireless access points are not used.

OK Cancel

Edit Testking_SSID Properties ? X

Network Properties IEEE 802.1x

☒ Enable network access control using IEEE 802.1x

EAPOL-Start message: Transmit

Parameters (seconds)

Max start: 3 Start period: 60

Held period: 60 Authentication period: 30

EAP type: Smart Card or other certificate

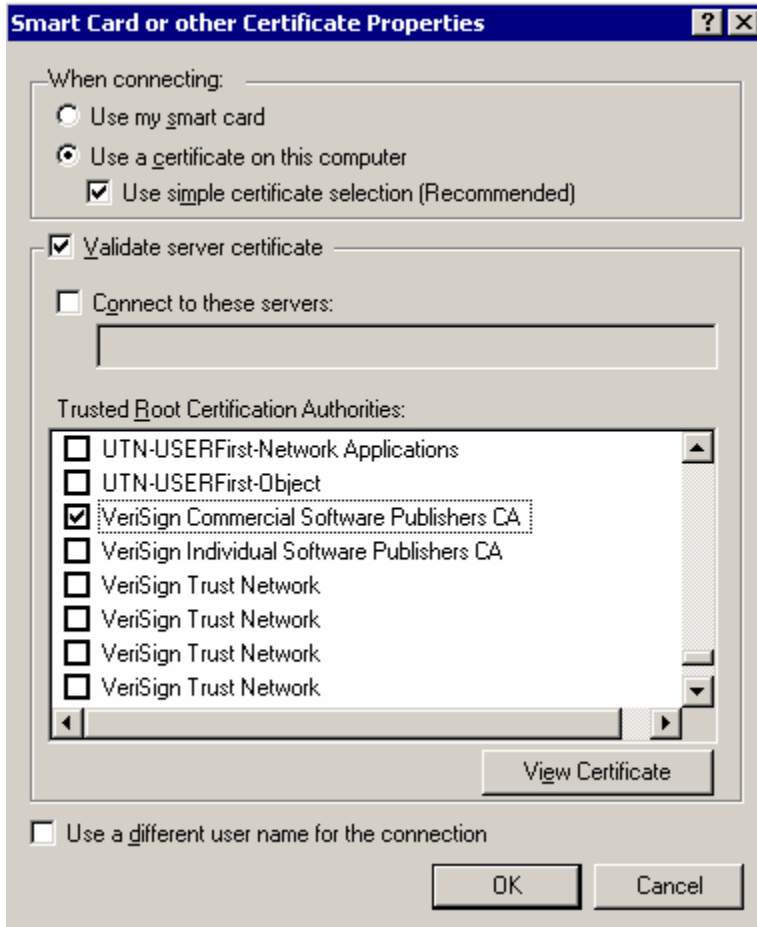
Settings...

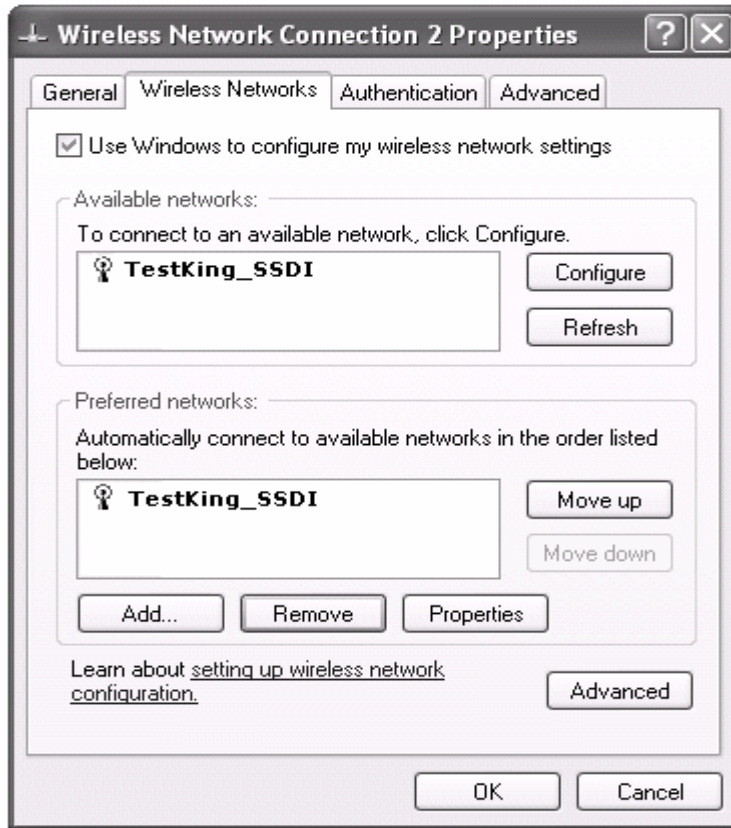
☐ Authenticate as guest when user or computer information is unavailable

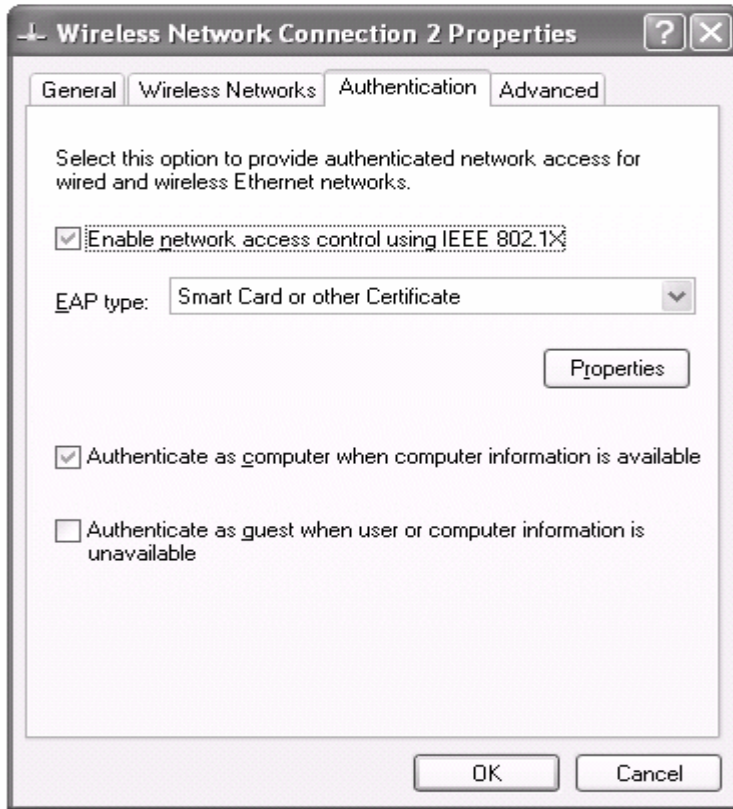
☒ Authenticate as computer when computer information is available

Computer authentication: With user re-authentication

OK Cancel



Client Part**Enabling Wireless Zero Configuration in Windows XP, Picture**



802.1x enabled for your wireless client. Picture

Setting Up Your Computer for Wireless Networking

Wireless networking is integrated into Windows XP and can be set up quickly with the Windows XP automatic networking Setup. All you need is a 802.11b wireless adapter installed on the mobile device, and an operating 802.11b standard wireless network

Connecting to the Network

Windows XP automatically polls the area for available wireless access points. If one is present, Windows XP attempts to connect to it. Sometimes, you will find that even though there is a wireless network in the area, Windows XP cannot recognize it

Installing Computer and User Certificates on Wireless Client Computers

For user authentication with EAP-TLS, configure either user certificates or smart card authentication. Certificates can reside either in the certificate store on your computer or on a smart card.

A smart card is a credit-card-sized device that is inserted into a smart card reader. The smart card reader is installed internally in your computer or connected externally to your computer.

Leading the way in IT testing and certification tools, www.testking.com

- For smart card authentication, use the Smart Card Enrollment station to permit you, the administrator, to act on behalf of a user, and to request and to install a Smart Card Logon certificate or Smart Card User certificate on the user's smart card. Then, issue smart cards to the users.
- **For user certificate-based authentication, the computer must request a user certificate from a Windows Server 2003 CA on the internal network.**

If you configured the domain to automatically allocate certificates to computers that are connected to the domain, you can connect the client computer to the domain by using a wired connection and a computer certificate is automatically issued.

Reference

HOW TO: Enable Windows XP Automatic Wireless Network Configuration KB article 314897

HOW TO: Support Wireless Connections That Use EAP-TLS Authentication in Windows Server 2003 KB article 816589

QUESTION NO: 123

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

Client computers in the human resources department run Windows XP Professional. Employees in the human resources department use the human resources client computers to transmit confidential data to the file servers.

The network also contains kiosk computers. The kiosk computers are used by temporary employees to transmit data to file servers. The kiosk computers run Windows XP Professional. TestKing's written security policy requires that all data transmissions from the kiosk computers must be able to be monitored by using a protocol analyzer.

You need to ensure that the confidential data transmissions to and from the human resources client computers remain confidential. You also need to ensure that you can detect any alterations in the data transmissions made by any computer. You need to comply with the written security policy.

What should you do?

- Use IPSec encryption on both the human resources client computers and the kiosk computers.
- Use IPSec encryption on the human resources client computers and IPSec integrity on the kiosk computers.
- Use IPSec integrity on the human resources client computers and IPSec encryption on the kiosk computers.

D. Use IPSec integrity on both the human resources client computers and the kiosk computers.

Answer: B

Explanation: We want to monitor IPSEC traffic. We can not use ESP because it encrypts the IP header. **If you need to diagnose ESP software-encrypted communication, you must disable ESP encryption and use ESP-null encryption by changing the IPSec policy on both computers**

We need to use AH so that we can monitor network traffic and preserve the integrity of messages,

Using both AH and ESP is the only way to both protect the IP header and encrypt the data. However, this level of protection is rarely used because of the increased overhead that AH would incur for packets that are already adequately protected by ESP. ESP protects everything but the IP header, and modifying the IP header does not provide a valuable target for attackers. Generally, the only valuable information in the header is the addresses, and these cannot be spoofed effectively because ESP guarantees data origin authentication for the packets

Protocol	Requirement	Usage
AH	The data and the header need to be protected from modification and authenticated, but remain readable.	Use for data integrity in situations where data is not secret but must be authenticated — for example, where access is enforced by IPSec to trusted computers only, or where network intrusion detection, QoS, or firewall filtering requires traffic inspection.
ESP	Only the data needs to be protected by encryption so it is unreadable, but the IP addressing can be left unprotected.	Use when data must be kept secret, such as file sharing, database traffic, RADIUS protocol data, or internal Web applications that have not been adequately secured by SSL.
Both AH and ESP	The header and data, respectively, need to be protected while data is encrypted.	Use for the highest security. However, there are very few circumstances in which the packet must be so strongly protected. When possible, use ESP alone instead.

Reference
Server help

QUESTION NO: 124

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








Many users share files on their client computers with other users. All client computers also access shared resources on both the Windows Server 2003 computers and the UNIX servers, which use a third-party

Server Message Block (SMB) server product. The written security policy for TestKing requires that SMB packet signing must be used whenever possible.








You need to edit the Computer Configuration section of the Default Domain Policy Group Policy object (GPO) to ensure that all computers in the domain meet the written security policy requirement.

Which two security settings should you enable?

To answer, select the appropriate security settings in the Group Policy Object Editor Results Pane.

Policy ▲	Policy Setting
 Microsoft network client: Digitally sign communications (always)	Disabled
 Microsoft network client: Digitally sign communications (if server agrees)	Disabled
 Microsoft network client: Send unencrypted password to third-party SMB servers	Disabled
 Microsoft network server: Amount of idle time required before suspending session	0
 Microsoft network server: Digitally sign communications (always)	Disabled
 Microsoft network server: Digitally sign communications (if client agrees)	Disabled
 Microsoft network server: Disconnect clients when logon hours expire	Disabled

Answer:

Policy ▲	Policy Setting
 Microsoft network client: Digitally sign communications (always)	Disabled
 Microsoft network client: Digitally sign communications (if server agrees)	Enabled
 Microsoft network client: Send unencrypted password to third-party SMB servers	Disabled
 Microsoft network server: Amount of idle time required before suspending session	0
 Microsoft network server: Digitally sign communications (always)	Disabled
 Microsoft network server: Digitally sign communications (if client agrees)	Enabled
 Microsoft network server: Disconnect clients when logon hours expire	Disabled

Microsoft network client: Digitally sign communications (if server agrees) – Enabled

Microsoft network server: Digitally sign communications (if client agrees) - Enabled

Explanation:

All Windows operating systems support both a client-side SMB component and a server-side SMB component. To take advantage of SMB packet signing, both the client-side SMB component and server-side SMB component that are involved in a communication must have SMB packet signing either enabled or required.

For Windows 2000 and above, enabling or requiring packet signing for client and server-side SMB components is controlled by the following four policy settings:

Microsoft network client: Digitally sign communications (always) - Controls whether or not the client-side SMB component requires packet signing.

Microsoft network client: Digitally sign communications (if server agrees) - Controls whether or not the client-side SMB component has packet signing enabled.

Microsoft network server: Digitally sign communications (always) - Controls whether or not the server-side SMB component requires packet signing.

Microsoft network server: Digitally sign communications (if client agrees) - Controls whether or not the server-side SMB component has packet signing enabled.

If server-side SMB signing is required, a client will not be able to establish a session with that server unless it has client-side SMB signing enabled. By default, client-side SMB signing is enabled on workstations, servers, and domain controllers.

Similarly, if client-side SMB signing is required, that client will not be able to establish a session with servers that do not have packet signing enabled. By default, server-side SMB signing is enabled only on domain controllers.

If server-side SMB signing is enabled, SMB packet signing will be negotiated with clients that have client-side SMB signing enabled.

Using SMB packet signing can impose up to a 15 percent performance hit on file service transactions.

Reference
Serve help
Group policies

QUESTION NO: 125

You are a network administrator for TestKing. All client computers on the network run Windows XP Professional.

You administer a Windows Server 2003 file server named TestKingB. On TestKingB, you create a shared folder named SharedDocs. SharedDocs contains data files. All client computers connect to the shared folder by using a mapped drive connected to \\TestKingB\SharedDocs.

TestKingB is configured to support volume shadow copies. You install the Previous Versions client software on all client computers.

You perform a full normal backup of TestKingB every day, seven days per week.

You need to document the recovery process to be used if a user accidentally deletes a file from SharedDocs. The process must allow you to recover the file as quickly as possible and to minimize data loss.

Which process should you use?

- A. On TestKingB, restore the file from the normal backup that was performed on the day before the file was deleted.
Use the advanced restore options to select the **Replace existing files** check box.
- B. On TestKingB, restore the file from the normal backup that was performed on the day before the file was deleted.
Use the advanced restore options to select the **Preserve existing volume mount points** check box.
- C. Run the volume shadow copy command-line tool to list all shadow copies.
Instruct the user to open the mapped drive and use the folder view options to expose hidden files.
- D. Instruct the user to open the mapped drive and navigate to the folder from which the file was deleted.
In the properties for the shared folder, select the **Previous Versions** tab.
View the most recent version and navigate until the file is located.
Restore the file by copying it to its new location.

Answer: D

Note: This will only work if the deleted file was in a subfolder in the shared folder.

Explanation

Although shadow copies are taken for an entire volume, users must use shared folders to access shadow copies. Administrators on the local server must also specify the `\\servername\sharename` path to access shadow copies. If you or your users want to access a previous version of a file that does not reside in a shared folder, you must first share the folder.

Designing a Shadow Copy Strategy

You can give users access to previous versions of files by enabling shadow copies, which provide point-in-time copies of files stored on file servers running Windows Server 2003. By enabling shadow copies, you can reduce the administrative burden of restoring previously backed up files for users who accidentally delete or overwrite important files. Shadow copies work for both open and closed files; therefore, shadow copies can be taken even when files are in use.

Shadow copies work by making a block-level copy of any changes that have occurred to files since the last shadow copy. Only the changes are copied, not the entire file. As a result, previous versions of files do not usually take up as much disk space as the current file, although the amount of disk space used for changes can vary depending on the application that changed the file. For example, some applications rewrite the entire file when a change is made, whereas other applications append changes to the existing file. If the entire file is rewritten to disk, the shadow copy contains the entire file. Therefore, consider the type of applications in your

organization, as well as the frequency and number of updates, when you determine how much disk space to allocate for shadow copies.

Important

Shadow copies do not eliminate the need to perform regular backups, nor do shadow copies protect you from media failure. In addition, shadow copies are not permanent. As new shadow copies are taken, old shadow copies are purged when the size of all shadow copies reaches a configurable maximum or when the number of shadow copies reaches 64, whichever is sooner. As a result, shadow copies might not be present for as long as users expect them to be. Be sure to consider user needs and expectations when you configure shadow copies. Shadow copies are designed for volumes that store user data, such as home directories and My Documents folders that are redirected by using Group Policy, or other shared folders where users store data. Shadow copies work with compressed or encrypted files, and they retain whatever permissions were set on the files when the shadow copies were taken. For example, if a user is denied permission to read a file, that user would not be able to restore a previous version of the file, nor would the user be able to read the file after it has been restored.

Reference:

**MS Windows Server 2003 Deployment Kit
Designing a Shadow Copy Strategy**

QUESTION NO: 126

You are a network administrator for TestKing. TestKing is developing a new Web application that connects to an SQL back-end environment. The design team decides that the new application must be fault tolerant. You interview the Web developers and the SQL administrators to establish the size of the environment.

The Web developers state that they need at least three Web servers to share the load. Each Web server requires two processors and 1 GB of RAM. The Web developers state if one of the Web servers fails, the Web application can run for several hours in a degraded state. Responsiveness will be below specifications in a degraded state.

The SQL administrators state that they need two Microsoft SQL Server computers to support the new application. They want the SQL server environment to be redundant. Each SQL Server computer requires four processors and 3 GB of RAM. The SQL administrators state that only one SQL Server computer is required to maintain the application.

You need to ensure that two of the Web servers and one of the SQL Server computers are always available. You need to select the lowest edition of Windows Server 2003 that meets the requirements in order to minimize costs.

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

- A. Install Windows Server 2003, Web Edition on all three Web servers.
Connect all three servers by using Network Load Balancing.
- B. Install Windows Server 2003, Standard Edition on all three Web servers.
Connect all three servers by using Network Load Balancing.
- C. Install Windows Server 2003, Enterprise Edition on all three Web servers.
Install a shared fiber-attached disk array for the Web servers.
Implement a three-node server cluster for the Web servers.
Configure the cluster so that all three nodes are active.
- D. Install Windows Server 2003, Standard Edition on both SQL Server computers.
Connect the SQL Server computers by using Network Load Balancing.
- E. Install Windows Server 2003, Enterprise Edition on both SQL Server computers.
Connect the SQL Server computers by using Network Load Balancing.
- F. Install Windows Server 2003, Enterprise Edition on both SQL Server computers.
Install a shared fiber-attached disk array for the SQL Server computers.
Implement a two-node server cluster for the SQL servers.
Configure the cluster so that one node is active and the second node is a hot standby node.

Answer: A, F

Explanation: For the web servers we can three servers connected using Network Load Balancing. We can use Network Load Balancing because the content will be the same on the web servers. Windows Server 2003 Web Edition supports Network Load Balancing.

For the SQL servers we need a two-node server cluster. For a server cluster, we need Windows Server 2003 Enterprise edition.

Incorrect Answers:

B: Windows Server 2003 Web Edition supports Network Load Balancing. We don't need Windows Server 2003, Standard Edition:

C: We can use Network Load Balancing because the content will be the same on the web servers. We don't need a server cluster.

D: We can't use Network Load Balancing for the SQL servers. Network Load Balancing should only be used when you have static content.

E: We can't use Network Load Balancing for the SQL servers. Network Load Balancing should only be used when you have static content.

QUESTION NO: 127

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

You are responsible for planning the backup and recovery of all servers and services for TestKing. A Windows Server 2003 computer named TestKing4 runs the enterprise root certification authority (CA). No subordinate CAs are installed on the network.

You need to create a plan to back up and restore the CA database. Your plan must ensure that the database and log files can be completely recovered in the event that the database is corrupted.

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

- A. On TestKing4, use the Certificates console to export all Trusted Root Certification Authorities certificates.
On TestKing4, use the Certificates console to import the certificates to the Trusted Root Certification Authorities node.
- B. On TestKing4, run the **certreq** command with the **–submit** option.
On TestKing4, run the **certreq** command with the **–retrieve** option.
- C. On TestKing4, use the Certification Authority snap-in to back up the CA.
On TestKing4, use the Certification Authority snap-in to restore the CA.
- D. On TestKing4, run the **certutil** command with the **–backup** option.
On TestKing4, run the **certutil** command with the **–restore** option.

Answer: C, D

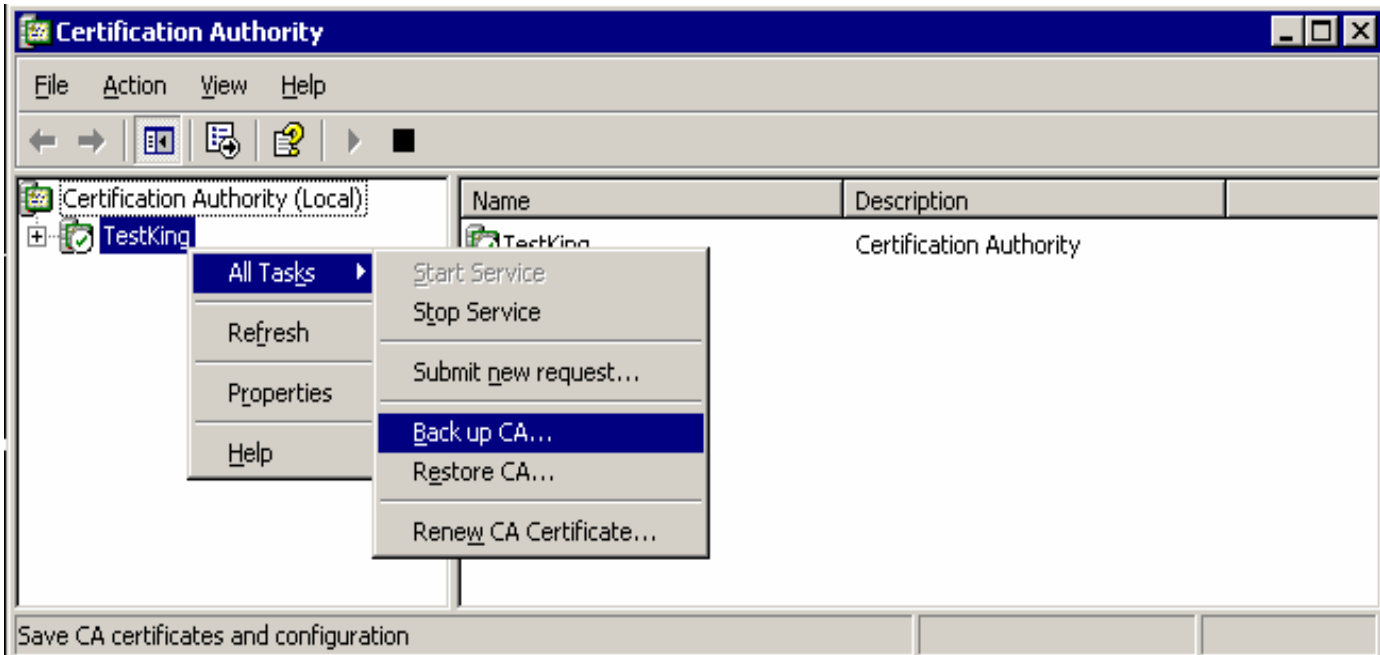
Explanation:

You can backup and restore the database and keys with the certutil command line utility

certutil

-backupDB	-- Backup Certificate Services database
-backupKey	-- Backup Certificate Services certificate and private key
-restore	-- Restore Certificate Services
-restoreDB	-- Restore Certificate Services database
-restoreKey	-- Restore Certificate Services certificate and private key

Or GUI

**QUESTION NO: 128**

You are a network administrator for TestKing. You administer a file server named TestKingSrvC. The file server stores all data files on a logical volume.

You perform a full normal backup of the file server every Saturday. You perform a differential backup of the file server each day on Sunday through Friday. You perform a copy backup of the file server every Wednesday after the differential backup is complete. The copy backup is sent to an off-site facility that requires two hours for tape delivery.

The logical volume fails on Friday morning.

You need to restore the data that was stored on the failed volume. You need to minimize the loss of data and the time required to perform the restoration.

What should you do?

- A. Restore the tapes from the copy backup that was performed on Wednesday and from the differential backup that was performed on Thursday.
- B. Restore the tapes from the normal backup that was performed on Saturday and from the differential backup that was performed on Thursday.

- C. Restore the tapes from the normal backup that was performed on Saturday and from the differential backups that were performed on Monday through Thursday
- D. Restore the tapes from the normal backup that was performed on Saturday, from the copy backup that was performed on Wednesday, and from the differential backup that was performed on Thursday.

Answer: B

Explanation:

The logical volume fails on Friday morning. The most recent backup of all the files was Wednesday's copy backup. However, if we restored this, we would lose and new or changed data between the copy backup and Friday morning. The correct answer is to restore the normal backup that was performed on Saturday and the differential backup that was performed on Thursday. This would ensure that the restored files will be up to date as of Thursday.

Types of backup

The Backup utility supports five methods of backing up data on your computer or network.

Copy backup

A copy backup copies all the files you select, but does not mark each file as having been backed up (in other words, the archive attribute is not cleared).

Copying is useful if you want to back up files between normal and incremental backups because copying does not affect these other backup operations.

Daily backup

A daily backup copies all the files that you select that have been modified on the day the daily backup is performed.

The backed-up files are not marked as having been backed up (in other words, the archive attribute is not cleared).

Differential backup

A differential backup copies files that have been created or changed since the last normal or incremental backup.

It does not mark files as having been backed up (in other words, the archive attribute is not cleared).

If you are performing a combination of normal and differential backups, restoring files and folders requires that you have the last normal as well as the last differential backup.

Incremental backup

An incremental backup backs up only those files that have been created or changed since the last normal or incremental backup.

It marks files as having been backed up (in other words, the archive attribute is cleared).

If you use a combination of normal and incremental backups, you will need to have the last normal backup set as well as all incremental backup sets to restore your data.

Normal backup

A normal backup copies all the files you select and marks each file as having been backed up (in other words, the archive attribute is cleared).

With normal backups, you only need the most recent copy of the backup file or tape to restore all of the files. You usually perform a normal backup the first time you create a backup set.

Backing up your data using a combination of normal backups and incremental backups requires the least amount of storage space and is the quickest backup method.

However, recovering files can be time-consuming and difficult because the backup set might be stored on several disks or tapes.

Backing up your data using a combination of normal backups and differential backups is more time-consuming, especially if your data changes frequently
it is easier to restore the data because the backup set is usually stored on only a few disks or tapes.

Reference: Server Help**Incorrect Answers:**

A: This would work but the copy backup is offsite. It's quicker to use Saturday's full backup.

C: This is more than necessary. We only need the last differential backup with the full backup.

D: This is more than necessary. We only need the last differential backup with the full backup.

QUESTION NO: 129

You are the systems engineer for Acme Inc. The network consists of a single Active Directory domain named acme.com. All servers run Windows Server 2003. The network is not currently connected to the Internet.

Acme enters into a partnership with Testking. The Testking network consists of a single Active Directory domain named testking-ad.com. All servers in the testking-ad.com domain run Windows Server 2003. 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 running the latest version of BIND.

Both companies require that users from each company must be able to access resources in either network. A new dedicated T1 line is established between the two offices to provide connectivity. The Active Directory project team plans to create a forest trust relationship between the two forests. Both companies' written security policies state that resources located on the internal network must never be exposed to the Internet. The Testking written security policy also states that the internal network's DNS namespace must never be exposed to the Internet.

You need to plan a name resolution strategy for internetwork connectivity. You need to configure both Windows Server 2003 DNS servers so that they comply with both companies' requirements and restrictions. Your plan must provide for minimal disruption of network connectivity in both networks.

What should you do?

- A. Create a conditional forwarder on the acme.com DNS server to forward all requests for hosts in the testking-ad.com domain to the testking-ad.com DNS server.
Create a conditional forwarder on the testking-ad.com DNS server to forward all requests for hosts in the acme.com domain to the acme.com DNS server.
- B. Create a conditional forwarder on the acme.com DNS server to forward all requests for hosts in the testking-ad.com domain to the testking.com UNIX-based DNS server.
Configure the testking.com UNIX-based DNS server to forward all requests for hosts in the acme.com domain to the acme.com DNS server.
- C. Configure root hints on each Windows Server 2003 DNS server.
Configure each Windows Server 2003 DNS server to forward requests to the testking.com UNIX-based DNS server.
- D. Configure a secondary zone on the testking.com UNIX-based DNS server for each company's domain.
Configure each company's Windows Server 2003 DNS server to allow zone transfers to only the testking.com UNIX-based DNS server.

Answer: A

Explanation:

Using Conditional Forwarding to Query for Names in Other Namespaces

If your internal network does not have a private root and your users need access to other namespaces, such as a network belonging to a partner company, use conditional forwarding to enable servers to query for names in other namespaces. Conditional forwarding in Windows Server 2003 DNS eliminates the need for secondary zones by configuring DNS servers to forward queries to different servers based on the domain name.

For example, the Contoso Corporation includes two namespaces: Contoso and Trey Research. Computers in each division need access to the other namespace. In addition, computers in both divisions need access to computers in the Supplier private namespace.

Before upgrading to Windows Server 2003, the Trey Research division created secondary zones to ensure that computers in both the Contoso and Trey Research namespace can resolve names in the Contoso, Trey Research, and Supplier namespaces. After upgrading to Windows Server 2003, the Trey Research division deleted its secondary zones and configured conditional forwarding instead.

QUESTION NO: 130

You are the network administrator for TestKing. TestKing's Web site is hosted at a local ISP. TestKing needs to move the Web site from the ISP to TestKing's perimeter network.

The design team specifies that five servers will be needed to host the Web site. The five servers must balance the network load of requests from the Internet. The Web site must remain available in the event that up to three servers fail at the same time. Each server will have four processors and 4 GB of RAM. Discussions with the design team and the Web developers reveal that the site can be implemented by using either shared storage or local server storage.

You need to select the proper operating system to install on each server. You need to select the proper Windows Server 2003 technology to provide fault tolerance. You need to select the lowest edition of Windows Server 2003 that meets the requirements in order to minimize costs.

What should you do?

- A. Install Windows Server 2003, Enterprise Edition on all five servers.
Connect all five servers to a shared fiber-attached disk array.
Configure the five servers as a server cluster.
Configure the cluster so that all five nodes are active.
- B. Install Windows Server 2003, Enterprise Edition on all five servers.
Connect all five servers to a shared fiber-attached disk array.
Configure the five servers as a server cluster.
Configure the cluster so that three nodes are active and two nodes are hot standby nodes.
- C. Install Windows Server 2003, Standard Edition on all five servers.
Connect all five servers by using Network Load Balancing.
- D. Install Windows Server 2003, Web Edition on all five servers.
Connect all five servers by using Network Load Balancing.

Answer: C

Explanation: The question states that you need to select the lowest edition of Windows Server 2003 that meets the requirements in order to minimize costs. Windows 2003 Standard Edition supports up to 4 processors and 4 GB of RAM. If three server fail, we will still have two servers serving the web site.

Incorrect Answers:

A: The question states that you need to select the lowest edition of Windows Server 2003 that meets the requirements in order to minimize costs. We can use Windows 2003 Standard Edition with NLB.

B: The question states that you need to select the lowest edition of Windows Server 2003 that meets the requirements in order to minimize costs. We can use Windows 2003 Standard Edition with NLB.

D: Web server edition only supports two-way symmetric multiprocessing (SMP) and 2 gigabytes (GB) of RAM.

Reference

Overview of Windows Server 2003, Web Edition

<http://www.microsoft.com/windowsserver2003/evaluation/overview/web.mspix>

Overview of Windows Server 2003, Standard Edition

<http://www.microsoft.com/windowsserver2003/evaluation/overview/standard.mspix>

Introducing the Windows Server 2003 Family

<http://www.microsoft.com/windowsserver2003/evaluation/overview/family.mspix>

QUESTION NO: 131

You are the network administrator for TestKing. All servers run Windows Server 2003. TestKing has 1,000 users that need to use certificates for secure e-mail. TestKing also uses certificates for Encrypting File Systems (EFS) and for authentication to Web-based applications that are located in the perimeter network.

TestKing is legally required to maintain access to files and e-mail messages even after employees leave TestKing. TestKing also has internal requirements stating that administrators must be able to restore lost certificate keys for network users.

You need to provide a backup and recovery plan to be used in the event that users accidentally delete or lose their certificates and the associated private keys.

You need to plan the steps for configuring the certification authority (CA) to issue user certificates for EFS, secure e-mail, and client authentication. Your plan must also provide all requirements for recovering private keys for user certificates. Your plan must minimize administrative effort.

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

- A. Create a key recovery agent and acquire the Key Recovery Agent certificate for the account.
- B. Configure the CA with a policy module that requires the administrator to explicitly issue certificates.
- C. Configure the CA to allow key archival.
- D. Create a new certificate template that has the proper application policies and allows key archiving.
Add the certificate template to the CA.
Allow authenticated users to enrol for certificates by using the new certificate template.
- E. Configure the certificate template to supersede the Domain Controller Authentication certification template.

Answer: A, C, D

Explanation:

Key archival and recovery

Windows Server 2003, Enterprise Edition can be configured to archive the private key of specific certificates when they are issued. This private key archive allows the key to be recovered at a later time if the private key is lost. This process is implemented in two separate phases: key archival and key recovery.

Key archival

The process of obtaining a certificate includes the subject locating the appropriate certificate template gathering the information required by that template, and supplying it to a certification authority. This information normally contains information such as the subject name, public key and supported cryptographic algorithms. When key archival is configured, the subject will also provide their private key to the certification authority. The certification authority stores that private key in its database until you want to perform key recovery.

By default, the private key of issued certificates is not archived. This is because the storage of the private key in multiple locations, by definition, allows more attacks against it.

Key recovery

Subjects can lose their private key in a variety of ways such as accidental deletion or deliberate misuse. An administrator may also want to recover the key of a particular subject to access data protected by that key. Key recovery can be used whenever the key archival process has stored the subject's private key.

The key recovery process requires an administrator to retrieve the encrypted certificate and private key and then a key recovery agent (KRA) to submit to the certification authority. When a correctly signed key recovery request is received, the subject's certificate and private key are provided to the requestor. The requestor would then use the key as appropriate or securely transfer the key to the subject for continued use. No recertification or rekeying is necessary, as the private key is not necessarily compromised.

Reference:

<http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windowsserver2003/maintain/operate/kyacws03.asp?frame=true#d>

QUESTION NO: 132

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.

You need to implement the capabilities and requirements listed in the following table for the users and computers in the domain.

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

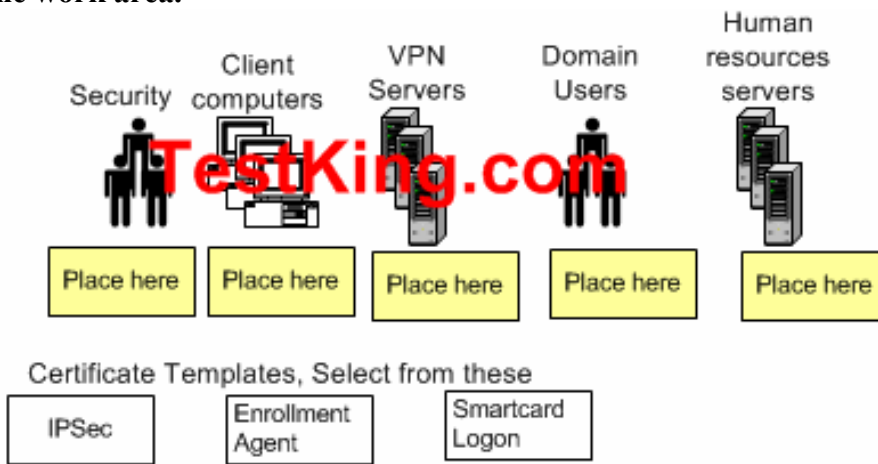
Human resources servers	Certificate-based IPSec encryption required for all data transmissions
VPN servers	L2TP required

All client computers are portable computers and need to connect to the VPN servers and to the human resources servers.

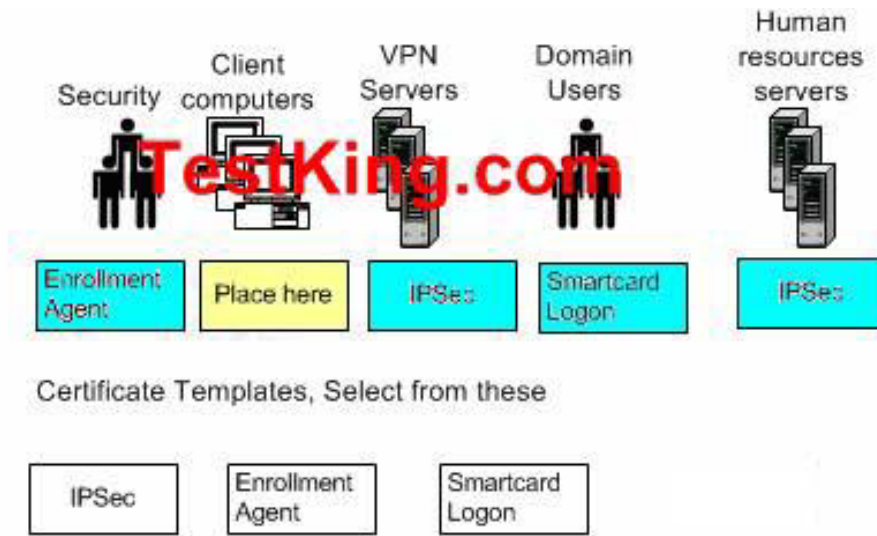
You configure a public key infrastructure (PKI) to support the domain users and computers. You need to specify which type of certificate, if any, each type of user or computer requires.

What should you do?

To answer, drag the appropriate certificate template or templates to the correct location or locations in the work area.



Answer:

**Explanation:**

IPSec should be enabled on the HR servers and the VPN servers.

The Smart Card certificates are issued to the users, not the computers.

The Security group need Enrollment Agents certificates.

Smart Card Logon

Smart card logon is integrated with the Kerberos version 5 authentication protocol implemented in Windows Server 2003. When smart card logon is enabled, the system recognizes a smart-card insertion event as an alternative to the standard Ctrl + Alt + Del secure attention sequence to initiate a logon. The user is then prompted for the smart card PIN code, which controls access to operations performed by using the private key stored on the smart card. In this system, the smart card also contains a copy of the certificate of the user (issued by an enterprise CA). This allows the user to roam within the domain.

Smart cards enhance the security of your organization by allowing you to store extremely strong credentials in an easy-to-use form. Requiring a physical smart card for authentication virtually eliminates the potential for spoofing the identities of your users across a network. In addition, you can also use smart card applications in conjunction with virtual private networks and certificate mapping, and in e-commerce. For many organizations, the potential to use smart cards for logon is one of the most compelling reasons for implementing a public key infrastructure.

Enroll clients.

To participate in a PKI, users, services, and computers must request and receive certificates from an issuing CA.

Typically, enrollment is initiated when a requester provides unique identifying information and a newly generated public key.

The CA administrator or enrollment agent uses this unique identifying information to authenticate the identity of the requester before issuing a certificate.

Secure VPN

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

QUESTION NO: 133

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 TestKing. TestKing's written security policy states that the private keys that are used to encrypt files must be archived for later recovery.

You install an enterprise certification authority (CA) on a server that runs Windows Server 2003. You create a new certificate template for file encryption. You configure the certificate template so that the private key is archived. All users on the domain are issued certificates from this template.

You separate the roles of key recovery agent and certificate manager. As part of the planning of the CA deployment, you want to document the procedure for how to recover a private key for a user.

Which three actions should you include in your procedure?

Possible actions, select from these	Required actions in the following order
Key recovery agent: Run the certreq command to retrieve a Key Recovery Agent certificate.	Place first action here
Key recovery agent: Run the certutil command to recover the private key into a .pfx file.	Place second action here
Certificate manager: Run the certutil command to retrieve the private key into a binary large object file.	Place third action here
Certificate manager: Reenroll all certificate holders.	
User: Import the private key	

Answer:

Possible actions, select from these	Required actions in the following order
Key recovery agent: Run the certreq command to retrieve a Key Recovery Agent certificate.	Certificate manager: Run the certutil command to retrieve the private key into a binary large object file.
Key recovery agent: Run the certutil command to recover the private key into a .pfx file.	Key recovery agent: Run the certutil command to recover the private key into a .pfx file.
Certificate manager: Run the certutil command to retrieve the private key into a binary large object file.	User: Import the private key
Certificate manager: Reenroll all certificate holders.	
User: Import the private key	

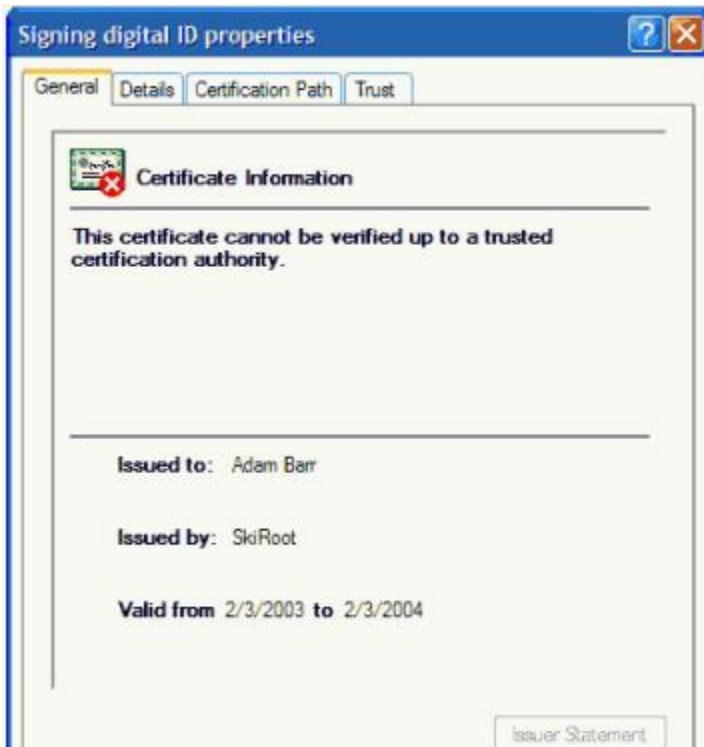
Reference:

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

QUESTION NO: 134

You are a network administrator for TestKing. TestKing participates in a joint venture with Acme. Each company's network consists of a single Active Directory forest. The functional level of each forest is Windows 2003. Two-way forest trust relationship exists between both companies. Each company maintains its own certification authority (CA).

Users are required to encrypt and digitally sign all e-mail messages relating to the joint venture that are sent between the companies. Users in the testking.com domain report that when they open e-mail messages sent by users in the acme.com domain, they receive a security warning. The warning indicates an error in the certificate used to sign the e-mail message. You examine several e-mail messages and discover the error shown in the exhibit.



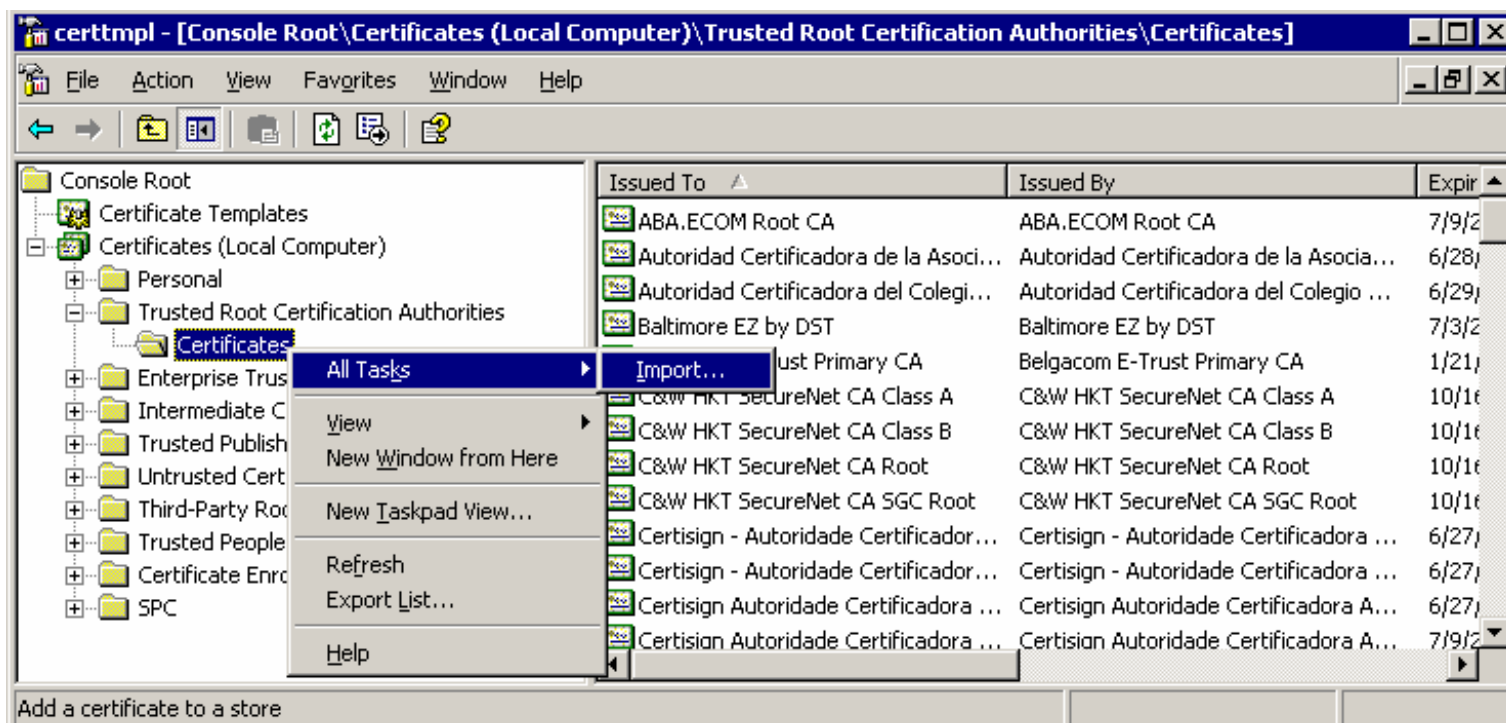
You need to ensure that users in the testking.com domain receive e-mail messages without receiving any error messages. You need to accomplish this task by using the minimum amount of administrative effort.

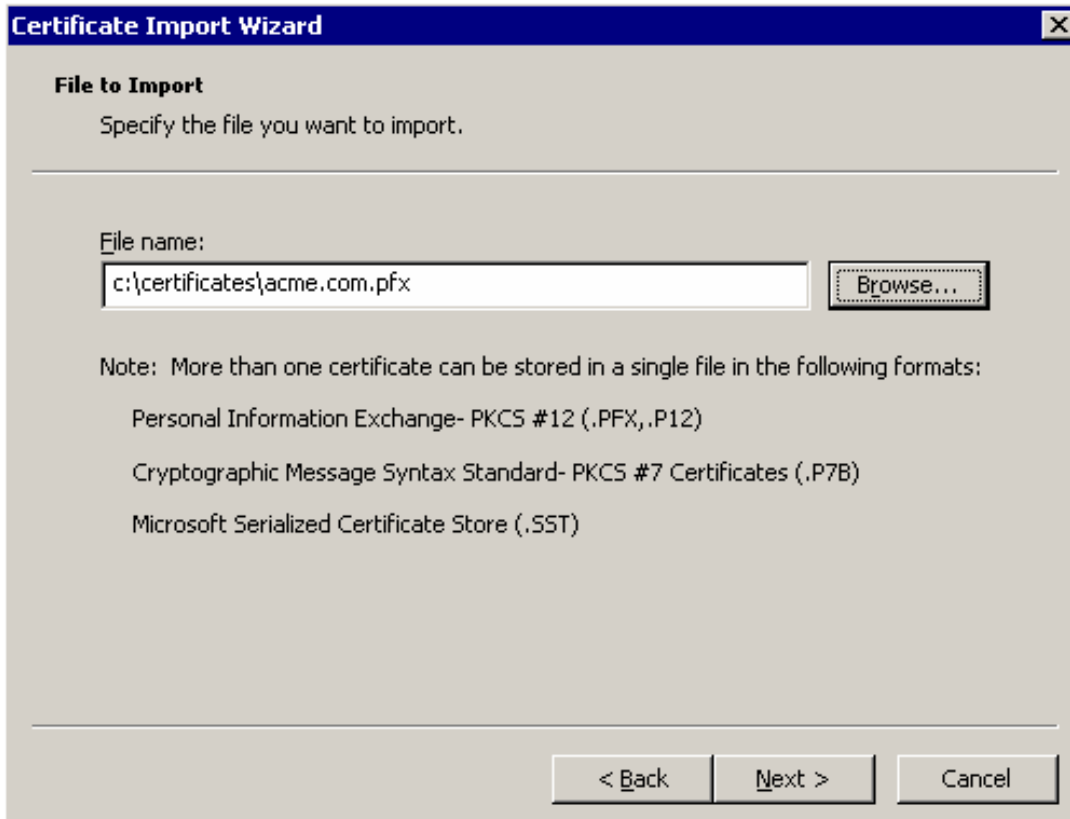
What should you do?

- A. Add the computer account for the enterprise root CA in the acme.com domain to the Cert Publishers domain local group in the testking.com domain.
- B. In the acme.com domain, delegate the **Allow – Read userCertificate** permission for contact objects to the Domain Users global group in the testking.com domain.
- C. In the acme.com domain, export the enterprise root certificate to a file.
On the enterprise root CA in the testking.com domain, import the enterprise root certificate from the acme.com domain.
- D. In the acme.com domain, export the enterprise root certificate to a file.
On the enterprise root CA in the testking.com domain, run the **certutil** command to publish the root certificate to Activate Directory.

Answer: C

Explanation: We need the users in testking.com to trust the acme.com CA. We can do this by exporting the acme.com enterprise root certificate to a file, and using certutil to publish the root certificate to the testking.com Activate Directory or we can configure the testking.com CA to trust the acme.com CA. Answers C and D would work but answer C is less administrative effort.





We will need to import this certificate into the Trusted Root Certification Authorities on the testking.com CA.

QUESTION NO: 135

You are the network administrator for TestKing. The network contains a single Active Directory domain named testking.com. All computers on the network are members of the domain.

TestKing 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.

Leading the way in IT testing and certification tools, www.testking.com

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

- 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 from 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: 136

You are a network administrator for TestKing. The network consists of a single Active Directory domain named testking.com. The network contains two Windows Server 2003 domain controllers named TestKingA and TestKingB, which both run the DNS Server service. All of the resource servers on the network are DHCP clients, including a Windows Server 2003 file server named TestKingC.

The DNS configuration consists of a primary forward lookup zone that allows dynamic updates on TestKingA and a secondary zone on TestKingB. Users report that they cannot connect to TestKingC. You discover that the IP address that is associated with the host (A) resource record for TestKingC is assigned to a test computer that is not a member of the domain. This computer is also named TestKingC.

You need to configure DNS to ensure that A records resolve to the IP addresses of the computers that made the original registration.

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

- A. Configure the **Secure Only** dynamic updates setting on the forward lookup zone on TestKingA.
- B. Configure the **None** dynamic updates setting on the forward lookup zone on TestKingA.
- C. Manually create A record entries for each server on TestKingA.

- D. Convert the zone type on TestKingA to Active Directory-integrated.
- E. Convert the zone type on TestKingB to primary.

Answer: A, D

Explanation:

By configuring Secure only updates, only domain members can register their A records with DNS. The zone is currently a primary zone; we need to convert the zone to Active Directory integrated to enable “secure only” updates.

Incorrect Answers:

- B:** It is not necessary (or recommended) to disable dynamic updates on the zone.
- C:** This would only be necessary if we disabled dynamic updates on the zone.
- E:** You can't have two primary zones for one domain.

QUESTION NO: 137

You are the network administrator for TestKing. TestKing is deploying a public Web server farm on Windows Server 2003 computers. This Web server farm will allow the public to view company information. The Web servers in the Web server farm will be placed in TestKing's perimeter network, which uses a public Internet address space.

TestKing wants to reduce the probability of external unauthorized users breaking into the public Web servers.

You need to make the Web servers less vulnerable to attack. You also want to ensure that the public will be able to view information that is placed in TestKing's perimeter network.

What should you do?

- A. Configure each Web server's IP address to a private reserved Internet address.
- B. Configure the Web servers to allow only IPSec communications.
- C. Disable any unneeded services on the Web servers.
- D. Disable TCP/IP filtering on all adapters in the Web servers.

Answer: C

Explanation: We should disable any unneeded services on the Web servers. This includes unneeded web services and unneeded server services. This will also ensure that no unnecessary ports are open on the servers.

Reducing the Attack Surface of the Web Server

Immediately after installing Windows Server 2003 and IIS 6.0 with the default settings, the Web server is configured to serve only static content. If your Web sites consist of static content and you do not need any of the

other IIS components, then the default configuration of IIS minimizes the attack surface of the server. When your Web sites and applications contain dynamic content, or you require one or more of the additional IIS components, you will need to enable additional features. However, you still want to ensure that you minimize the *attack surface* of the Web server. The attack surface of the Web server is the extent to which the server is exposed to a potential attacker.

However, if you reduce the attack surface of the Web server too much, you can eliminate functionality that is required by the Web sites and applications that the server hosts. You need to ensure that only the functionality that is necessary to support your Web sites and applications is enabled on the server. This ensures that the Web sites and applications will run properly on your Web server, but that the attack surface is minimized.

Incorrect Answers:

A: The public web servers need public IP addresses.

B: You can't use IPSec on public web servers. No one would be able to access the web pages.

D: TCP/IP filtering should be enabled, not disabled.

Reference

MS Windows Server 2003 Deployment Kit
Deploying Internet Information Services (IIS) 6.0
Reducing the Attack Surface of the Web Server

QUESTION NO: 138

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. You support 100 mobile users who have portable computers that run Windows NT Workstation 4.0, Windows 98, Windows 2000 Professional, Windows XP Professional, or Windows ME.

TestKing's written security policy requires that any remote access solution must provide both data integrity and data origin authentication.

You need to implement a VPN-based remote access solution.

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

- A. Install certificates on all VPN client computers.
- B. Install a certificate on the VPN server computer.
- C. Implement L2TP-based connections on the Windows 2000 Professional computers and the Windows XP Professional computers.
Implement PPTP-based connections on all other portable computers.

- D. Install the L2TP/IPSec VPN client on the portable computers that run Windows NT Workstation 4.0 or earlier.
Implement L2TP-based connections on all portable computers.
- E. Install the L2TP/IPSec VPN client on the portable computers that run Windows NT Workstation 4.0 or earlier.
Implement PPTP-based connections on all portable computers.

Answer: A, B, D

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.

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)

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

QUESTION NO: 139

You are the network administrator for TestKing. Your network consists of a single Active Directory forest that contains a forest root domain named testking.com.com and one child domain named mombasa.testking.com.com. All domain controllers run Windows 2000 Server. The mombasa.testking.com.com domain contains one Windows Server 2003 member server named TestKing3.

You attempt to promote TestKing3 to be an additional domain controller of the mombasa.testking.com.com domain. The promotion fails and you receive the error message shown in the exhibit.

*******MISSING*******

You need to resolve the error in order to promote TestKing3 to be an additional domain controller of the mombasa.testking.com.com domain.

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

- Force replication between the schema master and the PDC emulator of only the testking.com.com domain.
- Force replication between the schema master and the PDC emulator of the testking.com.com domain and the mombasa.testking.com.com domain.

- C. Run the **adprep /forestprep** command on the schema master of the testking.com.com domain.
- D. Run the **adprep /domainprep** command on the infrastructure master of only the testking.com.com domain.
- E. Run the **adprep /domainprep** command on the infrastructure masters of the testking.com.com domain and the mombasa.testking.com.com domain.

Answer: C, E

Explanation: We have a Windows 2000 forest. To install a Windows 2003 Domain Controller, you need to modify the schema using the adprep command.

Adprep

Prepares Windows 2000 domains and forests for an upgrade to Windows Server 2003, Standard Edition; Windows Server 2003, Enterprise Edition; or Windows Server 2003, Datacenter Edition. Among its tasks, **adprep** extends the schema, updates default security descriptors of selected objects, and adds new directory objects as required by some applications.

Syntax

adprep{/forestprep | /domainprep}

Parameters

/forestprep

Prepares a Windows 2000 forest for an upgrade to a Windows Server 2003 forest.

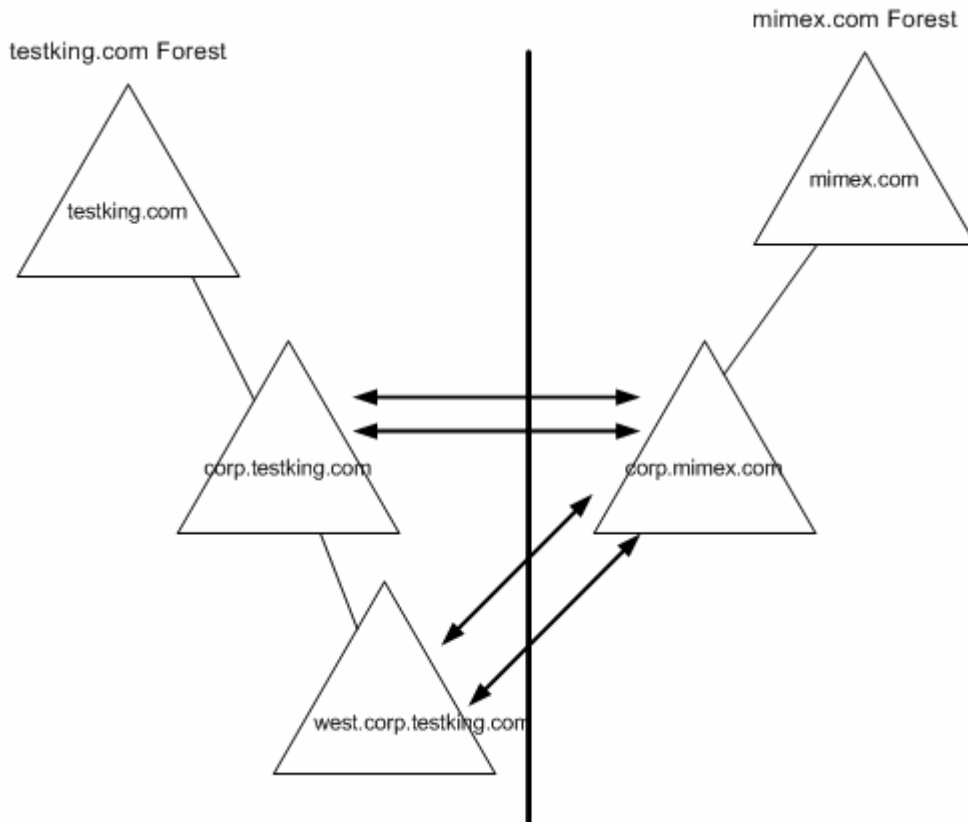
/domainprep

Prepares a Windows 2000 domain for an upgrade to a Windows Server 2003 domain.

- **Adprep /forestprep** must be run on the schema master
- **Adprep /domainprep** must be run on each infrastructure master in each domain, and only after **adprep /forestprep** has been run successfully for the forest.

QUESTION NO: 140

You are the network administrator for Acme. Acme consists of two subsidiaries named Testking, Ltd, and Mimex. The network contains two Active Directory forests. The functional level of each domain is Windows 2000 native. All domain controllers run Windows 2000 Server. External relationships exist between domains, as shown in the exhibit.



User accounts and resources are located in the child domains. All user principal names (UPNs) in each forest comply with a standard company e-mail address.

Each domain controller functions as a DNS server. All DNS zones are Active Directory-integrated zones. The testking.com and mimex.com DNS zones have no root (".") zone. DNS servers in each forest root DNS zone are configured with root hints to Internet root servers.

You upgrade each domain controller in both forests to Windows Server 2003. You raise the functional level for each domain to Windows Server 2003. You plan to implement a smart-card authentication strategy for the entire company.

You need to ensure that users are able to access resources in all domains in each forest and on the Internet. You want to accomplish this task by using the minimum amount of administrative effort. You also need to ensure that access to resources is not disrupted.

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

- A. Create a two-way external trust relationship between the two forest root domains.
Raise the functional level of the forest to Windows Server 2003.

- B. Raise the functional level of the forest to Windows Server 2003.
Replace existing trust relationships with a two-way forest trust relationship between the two forest root domains.
- C. Create root hints between DNS servers in each child domain and DNS servers in the root domain for the opposite forest.
- D. Create conditional DNS forwarders between domain controllers in each root domain.

Answer: B, D

Explanation

To have a complete trust between all the testking domains and all the mimex domains, we need to create a forest trust relationship between the two forest root domains. This can only be done after the functional level of the forests has been raised to Windows Server 2003.

In order to avoid traffic and get the resources from any of the forest we need to configure conditional forwarding in each zone.

We will create in testking.com a conditional forwarder to mimex.com

We will create in mimex.com a conditional forwarder to testking.com

Raise the Forest Functional Level to Windows Server 2003

After all domains are operating at the Windows Server 2003 functional level, raise the forest functional level to Windows Server 2003. This enables you to take advantage of all Windows Server 2003 forest-level features.

If any domains in the forest are still operating at the Windows Server 2003 interim functional level, you will be unable to raise the forest functional level to Windows Server 2003. Ensure that all domains are operating at the Windows Server 2003 functional level before you raise the forest functional level.

Enabling Windows Server 2003 Functional Levels in a Native Windows 2000 Environment

If the domains in your Windows 2000 forest include only Windows 2000 domain controllers and are in Windows 2000 native mode, deploy a Windows Server 2003–based domain controller to enable functional levels.

In an environment that contains only domain controllers running Windows 2000, you can introduce a Windows Server 2003–based domain controller in one of two ways:

- By installing a new Windows Server 2003–based domain controller.
- By upgrading an existing Windows 2000 domain controller in the forest to Windows Server 2003.

Functional levels are set by default to the following levels, and they remain at these levels until they are raised manually:

- Windows 2000 native domain functional level
- Windows 2000 forest functional level

To take advantage of the Windows Server 2003 domain-level features without waiting to complete the upgrade of your Windows 2000 forest to Windows Server 2003, raise only the domain functional level to

Windows Server 2003. Before you raise the domain functional level, you must upgrade all Windows 2000–based domain controllers in the domain to Windows Server 2003.

After you upgrade all Windows 2000–based domain controllers in the forest to Windows Server 2003, make sure that the domain functional level of each domain is set to Windows 2000 native or higher. Then raise the forest functional level to Windows Server 2003. Raising the forest functional level to Windows Server 2003 automatically raises the functional level of all domains in the forest that are set to Windows 2000 native or higher to Windows Server 2003.

Using Conditional Forwarding to Query for Names in Other Namespaces

If your internal network does not have a private root and your users need access to other namespaces, such as a network belonging to a partner company, use conditional forwarding to enable servers to query for names in other name spaces. Conditional forwarding in Windows Server 2003 DNS eliminates the need for secondary zones by configuring DNS servers to forward queries to different servers based on the domain name.

For example, the Contoso Corporation includes two namespaces: Contoso and Trey Research. Computers in each division need access to the other namespace. In addition, computers in both divisions need access to computers in the Supplier private namespace.

Before upgrading to Windows Server 2003, the Trey Research division created secondary zones to ensure that computers in both the Contoso and Trey Research namespace can resolve names in the Contoso, Trey Research, and Supplier namespaces. After upgrading to Windows Server 2003, the Trey Research division deleted its secondary zones and configured conditional forwarding instead.

Reference:

MS Windows Server Deployment Kit

Designing and Deploying Directory and Security Services

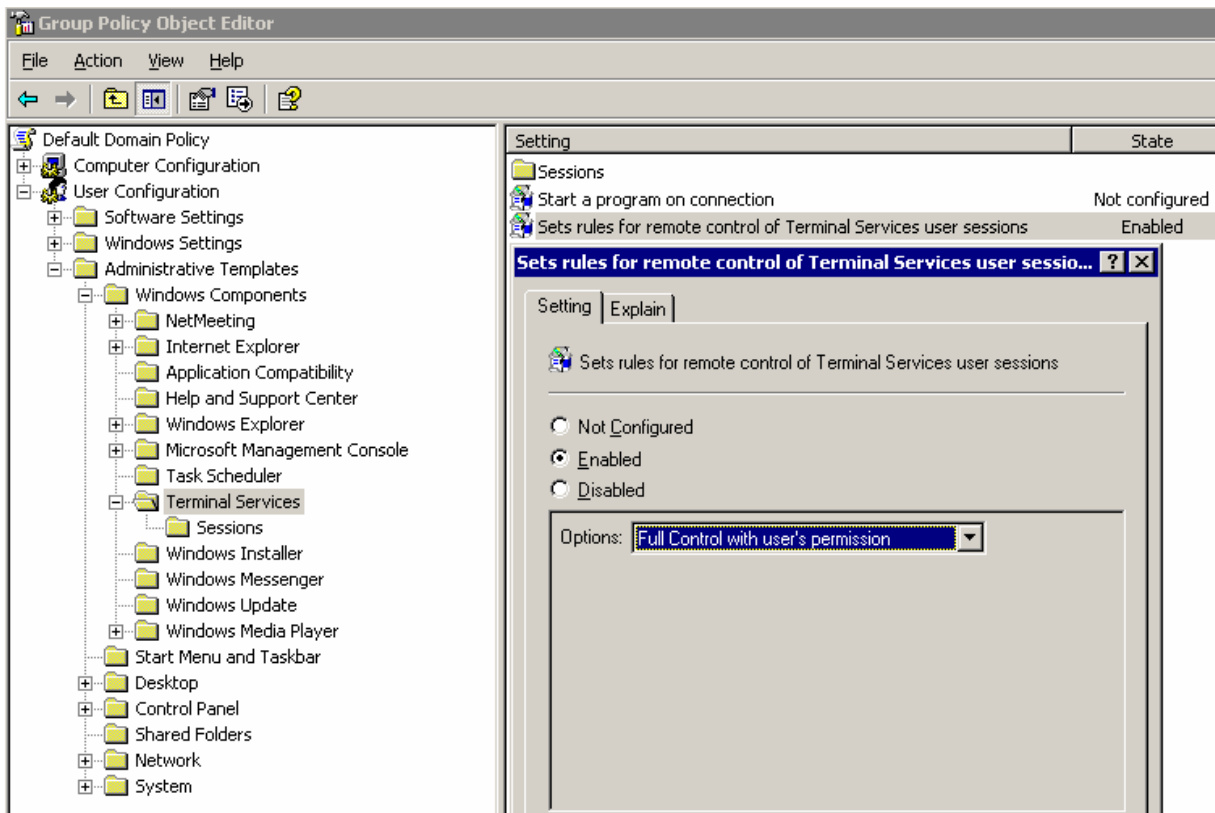
Raise the Forest Functional Level to Windows Server 2003

QUESTION NO: 141

You are a systems engineer 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 network contains 20 servers that run Terminal Services. All user productivity applications are hosted on these servers. Several of these applications are legacy applications that require users to control the file system and application registry settings.

Currently, Terminal Services is configured to allow administrators to remotely view and control users' Terminal Services sessions for support and training purposes. The managers of the human resources and finance departments inform you that confidential information was compromised when administrative personnel viewed user sessions without the knowledge or permission of the users. The managers direct

you to change the Terminal Services configuration to ensure that administrators can never view or control a user's session without the user's permission. You modify the Default Domain Policy Group Policy object (GPO) as shown in the exhibit.



You attempt to establish remote control of user's Terminal Services session and find out that you can do so without the user's permission.

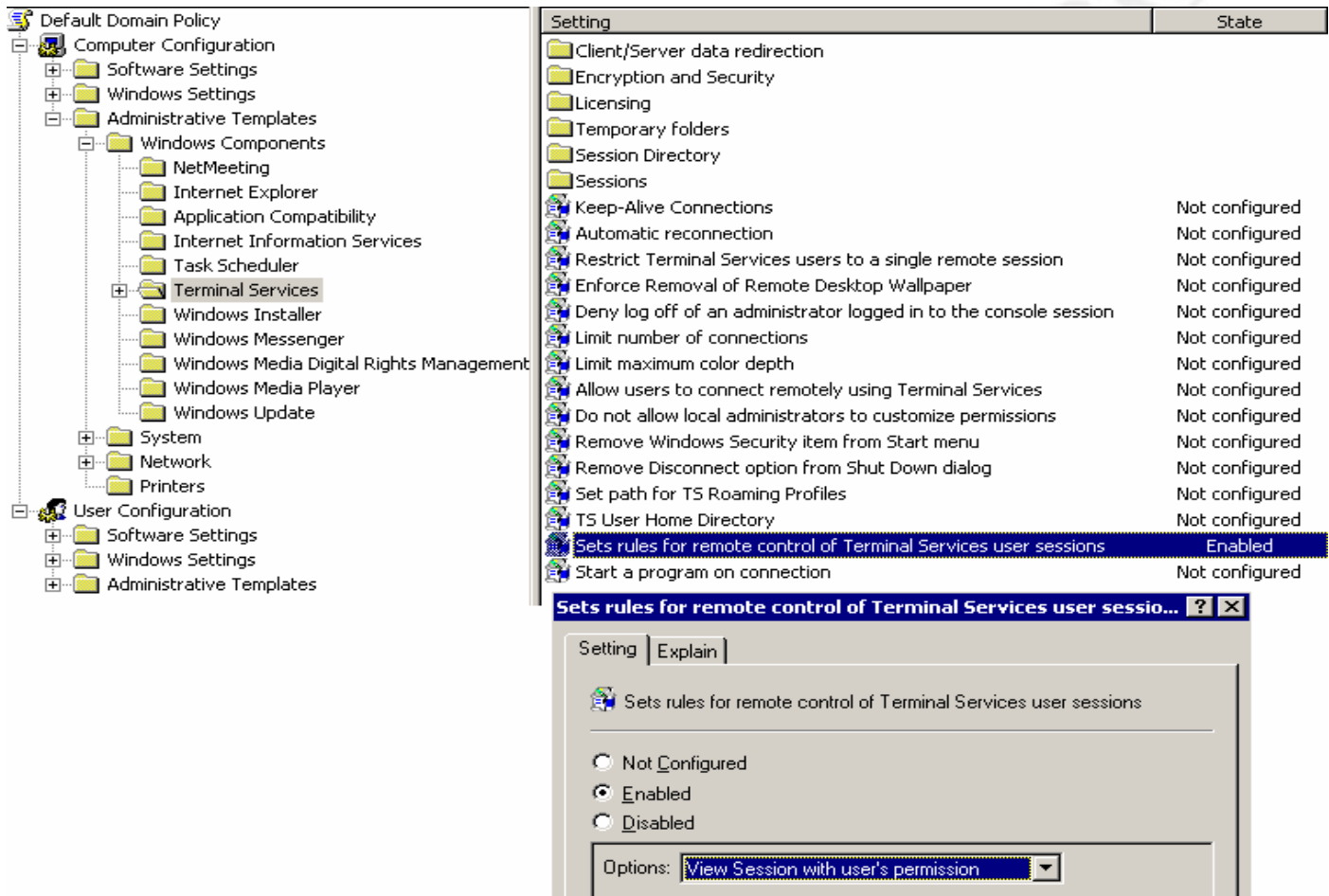
You need to configure Terminal Services to require the users' permission before an administrator can remotely view or control the session. You need to accomplish this task as quickly as possible and by using the minimum amount of administrative effort. Your configuration must also automatically apply to any new terminal servers that are installed in the network.

What should you do?

- A. In the Computer Configuration section of the Default Domain Policy GPO, disable the **Users can connect remotely using Terminal Services** option.
- B. In the Computer Configuration section of the Default Domain Policy GPO, enable the **Sets rules for remote control of Terminal Services user sessions** option and specify **Full Control with user's permission**.

- C. In the Terminal Services Configuration tool, select the **Use remote control with the following settings** option and select the **Require user's permission** check box.
- D. In the Terminal Services Configuration tool, set the **Permission compatibility** option to **Full Security**. In the connection properties, remote the **Allow – Full Control** permission from the Administrators group.

Answer: B



QUESTION NO: 142

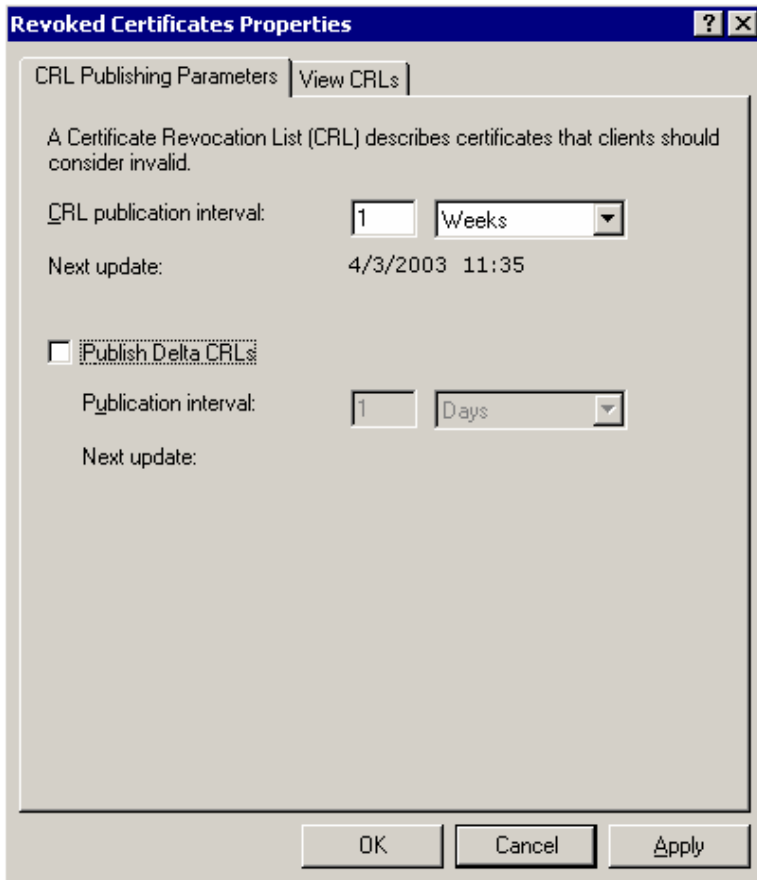
You are a network administrator for TestKing. All servers run Windows Server 2003.

The company uses a public key infrastructure (PKI) enabled sales application that enforces strong certificate revocation list (CRL) checking.

On average, 100,000 users require access to this application.

A stand-alone root certification authority (CA) is configured to issue certificates to users.

Certificate Services is configured as shown in the exhibit.



Certificates you issue are valid for three years.

You issue and revoke approximately 10,000 certificates per month for 12 months.

After 12 months, users begin to report delays when they open the sales application.

You discover that the delays occur periodically.

You need to improve the performance when users open the sales application.

What should you do?

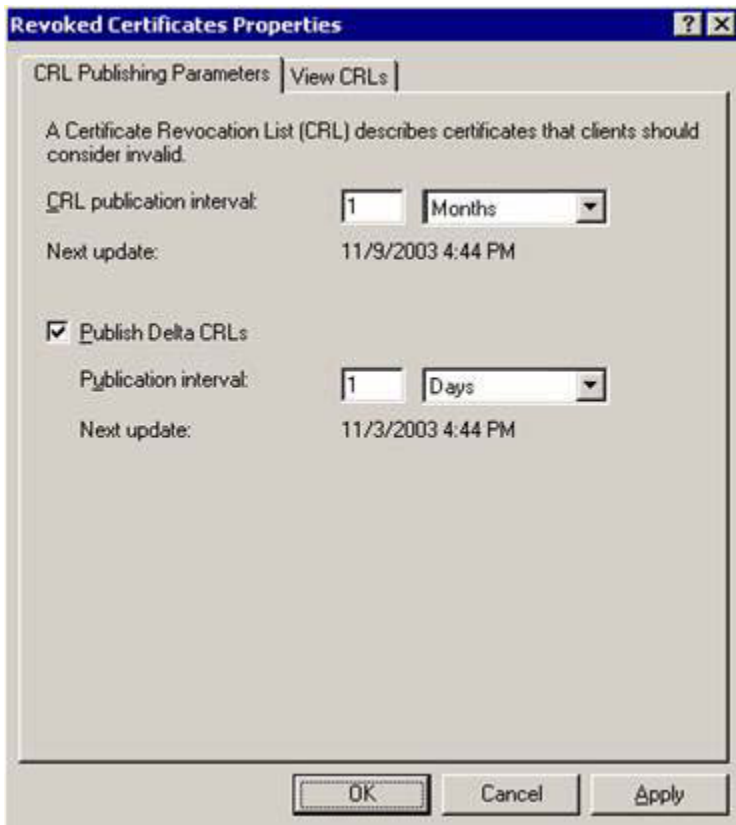
- A. Configure Certificate Services to publish the delta CRL daily and the base CRL monthly.
- B. Configure Certificate Services to publish the base CRL to a Web server on the network.

Include this location in the CRL distribution point of certificates.

- C. Configure a subordinate CA.
Instruct new users to enroll for certificates by using this CA.
- D. Configure Certificate Services to publish the base CRL daily and the delta CRL monthly.

Answer: A

Explanation:



To configure CRL and delta CRL overlap period

1. Open Command Prompt.
2. Type:

```
certutil -setreg ca\CRLOverlapUnits Value
certutil -setreg ca\CRLOverlapPeriod Units
certutil -setreg ca\CRLDeltaOverlapUnits Value
certutil -setreg ca\DeltaOverlapPeriod Units
```

- The maximum value for either the CRL or delta CRL overlap period is 12 hours.

Leading the way in IT testing and certification tools, www.testking.com

- The overlap period for CRLs is the amount of time at the end of a published CRLs lifetime that a client can use to obtain a new CRL before the old CRL is considered unusable. The default setting for this value is 10% of the CRL lifetime. Because some environments may require longer periods to replicate a CRL, this setting can be configured manually.
- When both a base CRL and delta CRL have been recently published, a revoked certificate may appear in both. This is because the newer delta CRL may still point at the older base CRL while the new base CRL is being replicated. Having the certificate appear in both CRLs ensures the revocation information is available.

Using delta certificate revocation lists

CRLs can become very long on large CAs that have experienced significant amounts of certificate revocation. This can become a burden for clients to download frequently. To **help minimize frequent downloads of lengthy CRLs, delta CRLs can be published. This allows the client to download the most current delta CRL and combine that with the most current base CRL to have a complete list of revoked certificates.** Because the **client will normally have the CRL cached locally, the use of delta CRLs can potentially improve performance.**

To use delta CRLs, the client application must be aware of and explicitly use delta CRLs for revocation checking. If the client does not use delta CRLs, it will retrieve the CRL from the CA every time it refreshes its cache, regardless of whether a delta CRL exists or not. For this reason, you should verify that the intended applications use delta CRLs and configure the CA accordingly. If the clients do not support the use of delta CRLs, you should either not configure the CA to publish delta CRLs or configure it so CRLs and delta CRLs are published at the same interval. This would still allow future applications that support delta CRLs to use them, while providing current CRLs to all applications. Note that all applications that use CryptoAPI in Windows XP and the Windows Server 2003 family use delta CRLs.

Publishing a CRL before the next scheduled publish period

You can also publish a CRL on demand at any time, such as when a valuable certificate becomes compromised. Choosing to publish a CRL outside the established schedule resets the scheduled publication period to begin at that time. In other words, if you manually publish a CRL in the middle of a scheduled publish period, the CRL publish period is restarted.

It is important to realize that clients that have a cached copy of the previously published CRL will continue using it until its validity period has expired, even though a new CRL has been published. Manually publishing a CRL does not affect cached copies of CRLs that are still valid; it only makes a new CRL available for systems that do not have a cached copy of a valid CRL.

Reference:
Server Help

QUESTION NO: 143

You are the network administrator for TestKing. The network includes a perimeter network. The perimeter network consists of a single Active Directory domain named testking.com. The domain contains four Windows Server 2003 Web servers configured as a Network Load Balancing cluster. The cluster hosts an Internet e-commerce Web site.

You upgrade the Web site to require users to log on in order to gain full access to the site. You will use Active Directory to store the user accounts. Web site users may access the site by using various Web browsers.

You need to enable and require SSL when users log on to the Web site. You need to minimize the administrative impact for users of the Web site.

What should you do?

- A. Obtain a Web server certificate from an external certification authority (CA) that is widely trusted on the Internet.
Install the certificate on each Web server in the cluster.
- B. Configure a stand-alone certification authority (CA) in the perimeter network.
Obtain a Web certificate from the CA.
Install the certificate on each Web server in the cluster.
- C. Install Certificate Services on each Web server in the cluster, and configure each Web server as enterprise certification authority (CA).
Configure certificate autoenrollment for all users.
- D. Install Certificate Services on each Web server in the cluster, and configure each Web server as a stand-alone certification authority (CA).
Configure Web-based certificates enrollment for users.

Answer: A

Explanation: To enable SSL on the web cluster we need a Web server certificate. The web site is a publicly accessible site, so the Web server certificate needs to be trusted by the public computers. We should use a Web server certificate from an external certification authority (CA) that is widely trusted on the Internet such as Verisign.

Incorrect Answers:

B: The public client computers will display a message saying that the server certificate isn't trusted.

C: The web server needs a Web server certificate from an external certification authority. It doesn't need to be a CA.

D: The web server needs a Web server certificate from an external certification authority. It doesn't need to be a CA.

Reference

How to Configure Certificate Server for Use with SSL on IIS KB 218445

HOW TO: Configure IIS Web Site Authentication in Windows Server 2003 KB 324274

HOW TO: Load Balance a Web Server Farm Using One SSL Certificate in IIS KB 313299

QUESTION NO: 144

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.

The users in the accounting department use their client computers to access confidential files over the network. The files must not be altered by unauthorized users as the files traverse the network.

You need to secure the data transmissions to and from client computers in the accounting department. You also need to be able to monitor the traffic on the network and report to IT management the percentage of bandwidth used for each protocol.

What should you do?

- A. Use IPsec encryption.
- B. Use Server Message Block (SMB) signing.
- C. Use NTLMv2 authentication.
- D. Use the Kerberos version 5 authentication protocol.

Answer: B

Explanation: We can't use IPsec "encryption" because this uses ESP to encrypt the IP header. If we use IPsec encryption, we won't be able to monitor the traffic. We could use IPsec "integrity" but that isn't listed as an option. Instead, we should use Server Message Block (SMB) signing.

Server Message Block (SMB) signing

Determines whether the computer always digitally signs client communications.

The Windows 2000 Server, Windows 2000 Professional, and Windows XP Professional authentication protocol Server Message Block (SMB) supports mutual authentication, which closes a "man-in-the-middle" attack and supports message authentication, which prevents active message attacks. SMB signing provides this authentication by placing a digital signature into each SMB, which is then verified by both the client and the server.

To use SMB signing, you must either enable it or require it on both the SMB client and the SMB server. If SMB signing is enabled on a server, clients that are also enabled for SMB signing use the packet signing protocol during all subsequent sessions. If SMB signing is required on a server, a client is not able to establish a session, unless it is at least enabled for SMB signing.

If this policy is enabled, it requires the SMB client to sign packets. If this policy is disabled, it does not require the SMB client to sign packets.

QUESTION NO: 145

You are the systems engineer for TestKing.

The network consists of a single Active Directory domain named testking.com.

All servers on the network run Windows Server 2003. All client computers run either Windows XP Professional or Windows 2000 Professional.

All servers that are not domain controllers are located in an organizational unit (OU) named Servers. All client computers used by administrative personnel are located in an OU named AdminDesktops. Both the Domain Controllers OU and the Servers OU have the Server (Request Security) IPsec policy applied. The AdminDesktops OU has the Client (Respond Only) IPSec policy applied.

You implement remote administration for all servers on the network. All servers are configured to allow Remote Desktop connections for administration. The company's written security policy requires that the highest security levels possible must be enforced during remote administration of the servers. The Terminal Services encryption settings are set to High in the Default Group Policy object (GPO).

Administrators who use Windows 2000 Professional computers soon report that they cannot establish Remote Desktop connections to the servers. Administrators can successfully establish network connections to shared resources on the servers. Administrators who use Windows XP Professional computers do not experience the same problem.

You verify that the servers to which the administrators are attempting to connect are online and have Remote Desktop connections enabled. You also verify that the maximum number of remote connections has not been exceeded on any server.

You need to ensure that all administrators can establish Remote Desktop connections to the servers regardless of which operating system is running on their client computers.

What should you do?

- A. In the properties for the Remote Desktop Protocol (RDP) connection on each server, set the encryption level to **FIPS Compliant**.
- B. Deploy the Remote Desktop Protocol (RDP) 5.2 client software to the AdminDesktops OU.
- C. On each server, use Terminal Services Manager to configure the servers to use standard Windows authentication.
- D. Configure the Terminal Services permission compatibility to **Relaxed Security**.

Answer: B

Incorrect Answers

- A.** If this setting is enabled, the security channel provider of the operating system is forced to use only the following security algorithms: TLS_RSA_WITH_3DES_EDE_CBC_SHA. This behaviour forces the security channel provider to negotiate only the stronger Transport Layer Security (TLS) 1.0
- C.** Specifies whether the connection defaults to the standard Windows authentication when another authentication package has been installed on the server.
- D. they ask you.** Provide the highest level of security

Explanation

Computers running earlier versions of Microsoft Windows, including Windows 2000 Server, Windows 2000 Professional, Windows NT 4.0, Windows 98, and Windows 95 can not connect to a Windows Server 2003 Terminal Services if they are using the old client Terminal server.

Client can not connect because they are using the full security. But when install the new version allows older Windows platforms to remotely connect to a computer running Windows XP Professional with Remote Desktop enabled

In Windows Server 2003 you do not need to install Terminal Server. Instead, you can use Remote Desktop for Administration (formerly Terminal Services in Remote Administration mode), which is installed by default on computers running one of the Windows Server 2003 operating systems. After you enable remote connections, Remote Desktop for Administration allows you to remotely manage servers from any client over a LAN, WAN, or dial-up connection. Up to two remote sessions, plus the console session, can be accessed at the same time, without requiring Terminal Server Licensing.

Application compatibility considerations

You should install programs from the console session of the terminal server. You can install programs from a remote console session, but this is not the preferred method for installing programs.

Some programs require an application compatibility script to be run after the program is installed. The scripts are stored in the *systemroot*\Application Compatibility Scripts\Install directory on the terminal server.

You should be aware of the implications of the security mode in which the terminal server operates. There are two security modes:

- **Full security** provides the most secure environment for users connecting to a terminal server. To run in this mode, applications must be written to run in the security context of an ordinary user. For Windows Server 2003 operating systems and Windows 2000, full security is the default.
- **Relaxed security** enables you to run programs that otherwise might not work at all in the more rigorous Full security mode. However, in Relaxed security mode (also known as Windows NT 4.0/Terminal Server Edition permissions compatibility mode), any user on the system can change files and registry settings in many places throughout the system, although others users' data files might not be visible. A malicious user could exploit this situation by replacing a known and trusted program with a program of

the same name but some harmful intent. If the operating system on your terminal server was installed using the Upgrade method, the security mode might be set to Relaxed security. When in doubt, you should choose Full security, test your applications in that mode, and change the security mode only if your test results indicate the need to do so.

Deploying client software

Remote Desktop Connection, formerly known as the Terminal Services Client, is installed automatically on computers running Windows XP and Windows Server 2003 operating systems.

For performance and security reasons, computers running earlier versions of Microsoft Windows, including Windows 2000 Server, Windows 2000 Professional, Windows NT 4.0, Windows 98, and Windows 95, should have the latest version of Remote Desktop Connection installed.

References:

Server Help
Terminal Server Help

Remote Desktop Connection Software Download

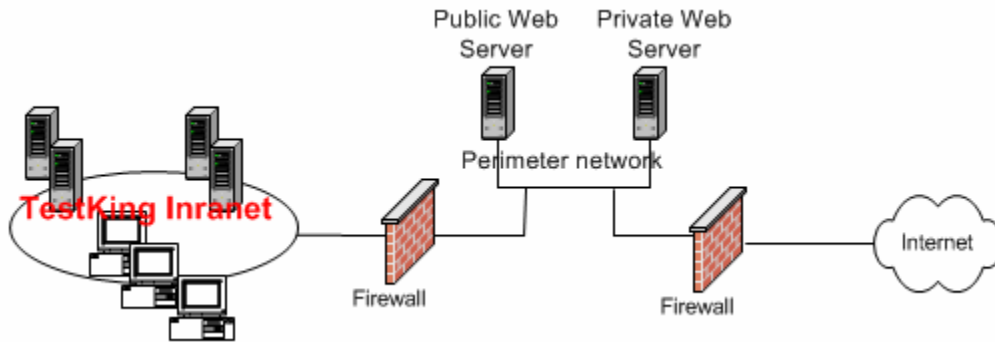
Download site for new TS client

<http://www.microsoft.com/windowsxp/pro/downloads/rdclientdl.asp>

This software package will install the client portion of Remote Desktop on any of the following operating systems: Windows 95, Windows 98 and 98 Second Edition, Windows Me, Windows NT® 4.0, or Windows 2000. (This is the same version of the client software as in Windows XP Service Pack 1.) When run, this software allows older Windows platforms to remotely connect to a computer running Windows XP Professional with Remote Desktop enabled.

QUESTION NO: 146

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. All client computers run Windows XP Professional. All administrative staff use portable computers. The relevant portion of the network is shown in the exhibit.



The private Web server uses non-standard ports for connections. The external firewall is configured to allow inbound connections on these non-standard ports.

Company policy requires that all administrative tasks must be performed remotely. You enable Remote Desktop connections on all servers on the company intranet. Each administrative client computer has two Windows Server 2003 Administrative Tools and Remote Desktops snap-in installed.

The administrators request that they be able to use Remote Desktop connections to administer the servers when they are at home. The company's written security policy requires that connections originating from the Internet are not allowed into the company intranet. Currently, only the Web servers are accessible from the Internet. The written security policy does not allow any other connections to the perimeter network from the Internet.

You need to provide a solution that allows Remote Desktop connections to the company intranet and that complies with the written security policy.

What should you do?

- A. Install the Remote Administration Web site on the private Web server.
Configure the external firewall to allow inbound connections on the IIS Remote Administration port.
Configure the internal firewall to allow inbound connections on the Remote Desktop Protocol (RDP) port.
- B. Install the Remote Administration Web site on the private Web server.
Configure the external firewall to allow inbound connections on the Remote Desktop Protocol (RDP) port.
Configure the internal firewall to allow inbound connections on the IIS Remote Administration port.
- C. Install the Remote Desktop Web Connection Web site on the private Web server.

Configure the internal firewall to allow inbound connections on the Remote Desktop Protocol (RDP) port.

- D. Install the Remote Desktop Web connection Web site on the Private Web server.

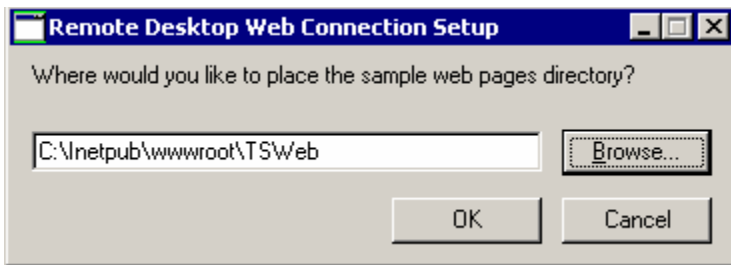
Configure the internal firewall to allow inbound connections on the IIS Remote Administration port.

Answer: C

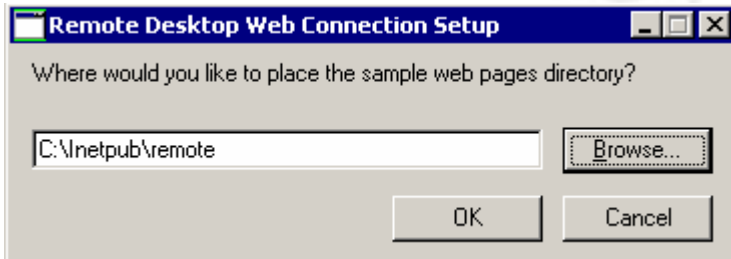
Explanation:

With this solution, we can access the private web server from the internet over a non-standard port by configuring RDP to listen on the non-standard port. Then we can open a remote desktop connection from the private web server to the intranet servers.

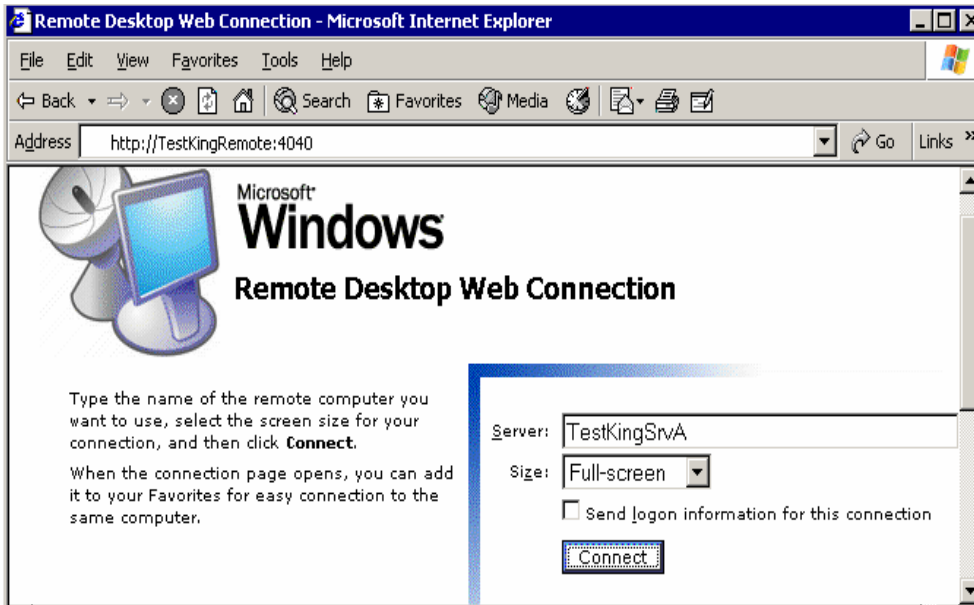
Default path Picture



Modified path over 4040port



In this way you now can connect to this site from external site over non standard port



And from here to the default port over RDP, also this can be changed but this is another topic

Web-based Remote Administration

Using a Microsoft ActiveX® control, a Terminal Services session can run on an Internet Explorer Web page. This lets the technology consultant gain access to the server from any desktop without needing to install the Terminal Services client.

It is also possible to expose the ActiveX control to the Internet, allowing the technology consultant to log on from any computer connected to the Internet and running the Internet Explorer browser. However, this is not considered a best practice because it potentially exposes the Windows Server 2003 network to the Internet in unintended ways.

Configure Terminal Services Port

Terminal Services is a useful tool for network administrators because it enables remote server and end – user computer management. The Remote Desktop client installs by default on all Windows Server 2003 and Windows XP systems, and it is available as an optional component on the Windows 2000 Server installation media. There is also a downloadable Microsoft ActiveX® client that runs within Internet Explorer or the Microsoft Management Console (MMC). These are collectively known as the Terminal Services Advanced Client (TSAC).

Vulnerability

Terminal Services listens on TCP port 3389 by default, and all versions of the Remote Desktop clients attempt to connect to this port. Although the entire session including the user authentication is encrypted, the Terminal Services clients do not perform server authentication. An attacker who was able to spoof a legitimate Terminal Services server could trick users into connecting to the attacker's server rather than the genuine system. An attacker could trick the user into connecting to their server by altering DNS records to redirect users to their own system or some other means.

Countermeasure

Change the TCP port used by Terminal Services or implement an IPSec policy to require trust and negotiate either Authentication Header (AH) or Encapsulation Security Payload (ESP) using IPSec transport mode (not IPSec tunnel mode). In some scenario, it may be feasible to isolate the Terminal Server behind a VPN gateway so that either Point to Point Tunneling Protocol (PPTP) or L2TP/IPSec secured VPN tunnels are required to gain access to the Terminal Server.

For information on how to change the port used by Terminal Services and the Remote Desktop Client, see the Microsoft Knowledgebase article, "How to Change Terminal Server's Listening Port," at <http://support.microsoft.com/default.aspx?scid=187623>. This article will show you how to do this for the regular desktop client. To do this in the Terminal Services Advanced Client Web client you need to add the following script line to the Web page MsRdpClient.RDPport = xxx, where xxx is the desired TCP port number. For more information on how you can use and customize

Remote Desktop Web Connection to run Terminal Services sessions within Microsoft Internet Explorer, see "Providing for RDP Client Security" at

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/termserv/termserv/providing_for_rdp_client_security.asp.

Remote Desktop Web Connection Security

The Remote Desktop Web Connection is a high-encryption, Remote Desktop Protocol (RDP) 5.0 client and uses RSA Security's RC4 cipher with a key strength of 40-, 56-, or 128-bit, as determined by the computer to which it is connecting.

The Remote Desktop Web Connection uses the well-known RDP TCP port (3389) to communicate to the host. Unlike some other display protocols, which send data over the network using clear text or with an easily decodable "scrambling" algorithm,

Remote Desktop Web Connection's built-in encryption makes it safe to use over any network—including the Internet—as the protocol cannot be easily sniffed to discover passwords and other sensitive data.

References:

How to Change the Listening Port for Remote Desktop MS Knowledge Base article 306759

How to Manually Open Ports in Internet Connection Firewall in Windows XP MS Knowledge Base article 308127

Configuring the Remote Desktop Client to Connect to a Specific Port MS Knowledge Base article 304034

Remote Desktop Web Connection

<http://www.microsoft.com/windowsxp/pro/downloads/rdwebconn.asp>

Server Help

QUESTION NO: 147

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

You install a wireless network. You configure the network to use Wired Equivalent Privacy (WEP). You install Windows Server 2003 on a server named TestKingSrv3. You install a wireless network adapter in TestKingSrv3.

The company's written security policy for implementing wireless devices includes the following requirements:

- **Administrators must be able to identify unauthorized wireless devices that attempt to connect to the wireless network.**
- **Administrators must be able to monitor wireless network device status, including radio channels information and signal strength, for wireless devices.**

You need to comply with the security monitoring requirements.

Leading the way in IT testing and certification tools, www.testking.com

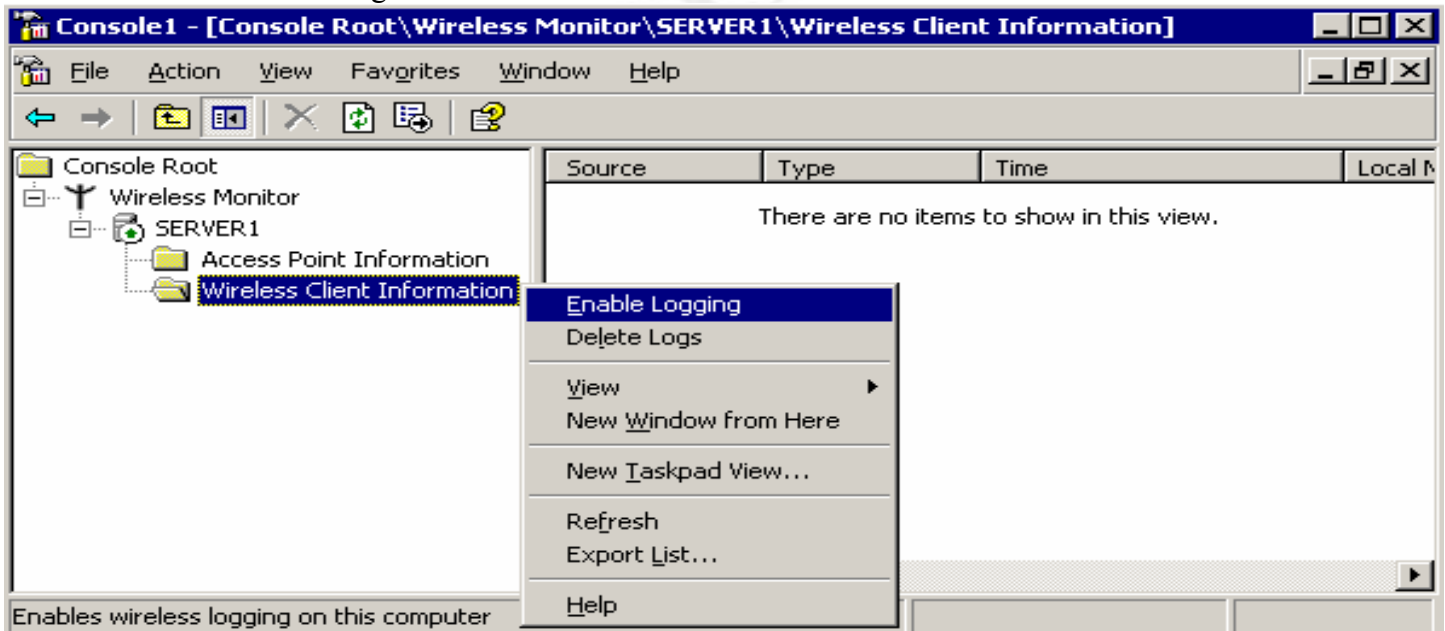
What should you do?

- A. Add the Wireless Monitor snap-in to enable logging and to view Wireless Client Information.
- B. Configure preferred networks in the wireless network policy for the Default Domain Policy Group Policy object (GPO).
- C. Install and configure Network Monitor on TestKingSrv3 to capture and analyze network traffic.
- D. In the wireless network policy for the Default Domain Policy Group Policy object (GPO), in the Networks to access list, select **Any available network (access point preferred)**.

Answer: A**Logging and viewing wireless network activity**

Wireless Monitor allows you to view details about access points and wireless clients. You can use this information to troubleshoot your wireless service. The Wireless Configuration service logs information in Wireless Monitor that allows you to:

- Identify service configuration changes.
- Check the events logged in the Wireless Configuration service log that are generated from outside of your network, such as media event notifications, 802.1X events, and timer expiration events.
- Check how the Wireless Configuration service reacts to external events by following transitions, as they are reflected in the log.

**To view details about wireless network access points**

1. Create a console containing Wireless Monitor. Or, open a saved console file containing Wireless Monitor.

2. Double-click **Access Point Information**.

Where?

- Wireless Monitor
- *ServerName*
- Access Point Information

Security information for wireless networks

Wireless networking technologies provide convenience and mobility, but they also introduce security risks on your network. For example, unless authentication and authorization mechanisms are implemented, anyone who has a compatible wireless network adapter can access the network. Without encryption, wireless data is sent in plaintext, so anyone within sufficient distance of a wireless access point can detect and receive all data sent to and from a wireless access point.

The following security mechanisms enhance security over wireless networks:

802.11 identity verification and authentication

802.11 Wired Equivalent Privacy (WEP) encryption

802.1X authentication

IAS support for 802.1X authentication

Selecting a wireless network type

When you configure new or existing wireless network connections or connect to an available wireless network, you can choose from the following wireless network types:

- **Access point (infrastructure)**

In access point wireless networks, wireless clients (computing devices with wireless network adapters, such as your portable computer or personal digital assistant) connect to wireless access points. The access points function as bridges between wireless clients and the existing network backbone. As you move from one location to another, and the signal for one wireless access point weakens, or the access point becomes congested with traffic, you can connect to a new access point. For example, if you work in a large corporation, you might connect to several different wireless access points as you move between different floors of a building or different buildings in a campus, while still maintaining uninterrupted access to network resources.

- **Computer-to-computer (ad hoc)**

In computer-to-computer wireless networks, wireless clients connect to each other directly, rather than through wireless access points. For example, if you are in a meeting with co-workers, and you do not need to gain access to network resources, your wireless device can make direct connections to the wireless devices of your co-workers, and you can form a temporary network.

- **Any available network (access point preferred)**

In access point preferred wireless networks, a connection to an access point wireless network is always attempted first, if there are any available. If an access point network is not available, a connection to a computer-to-computer wireless network is attempted. For example, if you use your laptop at work in an access point wireless network, and then you take your laptop home to use in your computer-to-computer home network, the Windows Configuration service will change your wireless network settings as needed so that you can connect to your home network.

Reference Server Help

QUESTION NO: 148

You are the network administrator for your company. The network contains Windows Server 2003 computers and Windows XP Professional computers. The company deploys two DNS servers. Both DNS servers run Windows Server 2003. One DNS server is inside of the corporate firewall, and the other DNS server is outside of the firewall. The external DNS server provides name resolution for the external Internet name of the company on the Internet, and it is configured with root hints.

The internal DNS server hosts the DNS zones related to the internal network configuration, and it is not configured with root hints.

You want to limit the exposure of the client computers to DNS-related attacks from the Internet, without limiting their access to Internet-based sites.

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

- A. Configure the client computers to use only the internal DNS server.
- B. Configure the client computers to use both DNS servers.
List the internal DNS server first.
- C. Configure the firewall to allow only network traffic on the DNS ports.
- D. On the internal DNS server, disable recursion.
- E. On the internal DNS server, configure the external DNS server as forwarder.
- F. On the internal DNS server, add the external DNS server as the only root hint.

Answer: A, E

Explanation

With this solution, the internal DNS servers will resolve any host resolution requests from its zone file. Any host resolution requests that the internal DNS server is unable to resolve will be forwarded to the external DNS server. The external DNS server will then go through the DNS hierarchy to resolve the request and return the answer to the internal DNS server.

Keep forwarder configuration uncomplicated.

For every DNS server configured with a forwarder, queries can be sent to a number of different places. Each forwarder and each conditional forwarder must be administered for the benefit of DNS client queries, and this process can be time consuming. Use forwarders strategically, where they are needed the most, such as resolving offsite queries or sharing information between namespaces.

Incorrect answers:

B: This is not necessary and is insecure. The internal DNS server can forward external requests to the external DNS server.

C: This is not necessary. The firewall should have other ports open such as port 80 for http etc.

F: In this way DNS can resolve internet queries, but its not a best practice because can give negative answers to domain.

Reference**Server Help****Directing queries through forwarders****QUESTION NO: 149**

You are the network administrator for Testking. The network consists of two physical subnets connected by a hardware-based router. Each subnet contains two domain controllers running Windows 2000 Advanced Server. All other servers run Windows 2000 server.

TestKing is in the process of migrating to a Windows Server 2003 Active Directory domain-based network. You plan to install two new Windows Server 2003 computers as domain controllers in the domain. The migration plan does not currently allow for upgrading the Windows 2000 domain controllers or changing any operations master roles.

Currently, host name resolution is performed by one of the Windows 2000 domain controllers that is running the DNS Server service. The DNS server hosts a standard primary zone for the domain. The migration plan requires that the DNS zone must be implemented as an Active Directory-integrated zone.

You need to redesign the DNS infrastructure to comply with the requirements of the migration plan. You need to ensure that the Active Directory-integrated zone will be loaded and hosted on all domain controllers.

What should you do?

- A. Configure the zone replication scope to replicate the zone to all DNS servers in the Active Directory forest.
- B. Configure the zone replication scope to replicate the zone to all DNS servers in the Active Directory domain named testking.com.
- C. Configure the zone replication scope to replicate the zone to all domain controllers in the Active Directory domain named testking.com.
- D. Configure the zone replication scope to replicate the zone to all domain controllers specified for a separate DNS application directory partition.

Answer: C

Explanation

The question states that **You need to ensure that the Active Directory-integrated zone will be loaded and hosted on all domain controllers.** This is the only answer that states “all domain controllers”.

This option replicates zone data to all domain controllers in the Active Directory domain. If you want Windows 2000 DNS servers to load an Active Directory zone, this setting must be selected for that zone.

Active Directory Replication

Active Directory replication propagates zone changes between domain controllers. Replication processing differs from DNS full zone transfers, in which the DNS server transfers the entire zone. Replication processing also differs from incremental zone transfers, in which the server transfers all changes made since the last change.

Active Directory zone replication provides the following additional benefits:

- Network traffic is reduced because the domain controllers only send the final result of all changes.
- When a zone is stored in Active Directory, replication occurs automatically. No additional configuration is required.
- When Active Directory zone replication occurs between sites, zone data that is greater than the default transfer size is automatically compressed before it is transferred. This compression decreases the network traffic load.

After careful analysis, you can partition and delegate your DNS zones based on what is required for providing efficient and fault-tolerant name service to each location or site.

If you are using Active Directory–integrated zones in a Windows Server 2003 domain, you must select an Active Directory–integrated zone replication scope. When selecting a replication scope, note that network traffic increases as you broaden the replication scope. For example, if you choose to replicate Active Directory–integrated DNS zone data to all DNS servers in the forest, this produces greater network traffic than replicating the DNS zone data to all DNS servers in a single Active Directory domain in that forest. Balance your need to minimize replication traffic against your need to minimize zone query traffic. The DNS administrators in your organization are responsible for managing zone replication.

Zone replication scope	Description
All DNS servers in the Active Directory forest	Replicates zone data to all DNS servers running on domain controllers in the Active Directory forest. Usually, this is the broadest scope of replication.
All DNS servers in the Active Directory domain	Replicates zone data to all DNS servers running on domain controllers in the Active Directory domain. This option is the default setting for Active Directory–integrated DNS zone replication in the Windows Server 2003 family.
All domain controllers in the Active Directory	Replicates zone data to all domain controllers in the Active Directory domain. If you want Windows 2000 DNS servers to load an Active Directory zone, this

domain

All domain controllers in a specified application directory partition

setting must be selected for that zone.

Replicates zone data according to the replication scope of the specified application directory partition. For a zone to be stored in the specified application directory partition, the DNS server hosting the zone must be enlisted in the specified application directory partition.

Migrating Zones to Windows Server 2003 DNS Servers

You can migrate zones to DNS servers running Windows Server 2003 in one of two ways:

- By using zone transfer.
- By copying the zone files.

If you copy the zone files, you must manually verify the integrity of the zones. Regardless of the method that you use to migrate zones, you must decide whether to take the original DNS server offline, or to use it as a secondary server. If you determine that the original third-party DNS server causes interoperability problems on your network, or if you need to use that server hardware for another purpose, take the server offline. Otherwise, keep the server on your network to provide backup for your primary DNS server running Windows Server 2003.

Reference**Server Help**

DNS zone replication in Active Directory

QUESTION NO: 150

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.

The network contains servers that have Terminal Server enabled. The terminal servers host legacy applications that currently require users to be members of the Power Users group.

A new requirement in the company's written security policy states that the Power Users group must be empty on all resource servers.

You need to maintain the ability to run the legacy applications on the terminal servers when the new security requirement is implemented.

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 template into the Default Domain Controllers Policy Group Policy object (GPO).
- 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: This is a trick question because answers A and B would enable the users to use Terminal Services. However, the question doesn't state whether the users can already use Terminal Services. The question asks how we can run the application without the users being in the power users group. The answer would therefore be D.

Incorrect Answers:

- A:** This would enable the users to use Terminal Services. However, this is not what the question is asking. The question is asking how we can run the application without the users being in the power users group.
- B:** This would enable the users to use Terminal Services. However, this is not what the question is asking. The question is asking how we can run the application without the users being in the power users group.
- C:** The Compatws.inf security template should be applied to the servers running the application, not the domain controllers.

Compatws.inf

Default permissions for workstations and servers are primarily granted to three local groups: Administrators, Power Users, and Users. Of the three, the Administrators group has the most permission, while the Users group has the least. Because of this, you can significantly improve security, reliability, and the total cost of system ownership by:

- Making sure that end users are members of the Users group.
- Deploying applications that can be run successfully by members of the Users group.

Members of the Users group can successfully run applications that are a part of the Windows Logo Program. However, members of the Users group might not be able to run applications that do not meet the requirements of the program. If other applications must be supported, there are two options:

- Permit members of the Users group to be members of the Power Users group.
- Relax the default permissions that are granted to the Users group.

Because Power Users have additional permissions such as creating users, groups, printers, and shares, some administrators prefer to relax the default User permissions instead of permitting members of the Users group to be members of the Power Users group. This is precisely what the Compatible template is for.

The Compatible template changes the default file and registry permissions that are granted to the Users group in a way that is consistent with the requirements of most applications that do not belong to the Windows Logo Program.

Additionally, because it is assumed that the administrator who is applying the Compatible template does not want members of the Users group to be Power Users, the Compatible template also removes all members of the Power Users group

Reference:

**MS Windows Server 2003 Deployment Kit
Designing a Managed Environment
Selecting Predefined Security Templates**

QUESTION NO: 151

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 computer named TestKing4 that functions as a mail server. TestKing4 is configured as a member server in the domain.

To improve service to users, TestKing launched a single sign-on initiative. Currently, users need to authenticate to the mail server after they log on to the domain to send or receive e-mail messages. You use IIS Manager to configure the properties for the Default SMTP Virtual Server on TestKing4.

You need to allow users to send e-mail messages without explicitly logging on to TestKing4. You need to prevent unauthorized users from sending e-mail messages.

What should you do?

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



Answer: Uncheck anonymous access, Check Integrated Windows Authentication

Integrated Windows Authentication

Select this option to enable the standard security mechanism that is provided with servers running Windows Server.

This security feature makes it possible for businesses to provide secure logon services for their customers. Virtual servers that already use Integrated Windows Authentication in an internal system can benefit by using a single, common security mechanism.

Integrated Windows Authentication uses a cryptographic technique for authenticating users and does not require the user to transmit actual passwords across the network.

Note: Using Integrated Windows Authentication requires a mail client that supports this authentication method. Microsoft Outlook and Microsoft Outlook Express support Integrated Windows Authentication.

QUESTION NO: 152

You are the network administrator for TestKing. The network consists of a single Active Directory domain named testking.com. The company has an internal network and a perimeter network. The internal network is protected by a firewall. Application servers on the perimeter network are accessible from the Internet.

You are deploying 10 Windows Server 2003 computers in application server roles. The servers will be located in the perimeter network and will not be members of the domain. The servers will host only publicly available Web pages.

The network design requires that custom security settings must be applied to the application servers. These custom security settings must be automatically refreshed every day to ensure compliance with the design.

You create a custom security template named Baseline1.inf for the application servers. You need to comply with the design requirements.

What should you do?

- A. Import Baseline1.inf into the Default Domain Policy Group Policy object (GPO).
- B. Create a task on each application server that runs Security and Configuration Analysis with Baseline1.inf every day.
- C. Create a task on each application server that runs the **secedit** command with Baseline1.inf every day.
- D. Create a startup script in the Default Domain Policy Group Policy object (GPO) that runs the **secedit** command with Baseline1.inf.

Answer: C

Explanation:

You will need to use the secdit command line tool with the switch “/configure”.

Allows you to configure a system with security settings stored in a database.

The syntax of this command is:

```
secdit /configure /db filename [/cfg filename] [/overwrite][/areas area1 area2...] [/logfilename] [/quiet]
```

/db filename Specifies the database used to perform the security configuration.

/cfg filename Specifies a security template to import into the database prior to configuring the computer.

Security templates are created using the Security Templates snap-in.

/overwrite Specifies that the database should be emptied prior to importing the security template. If this parameter is not specified, the settings in the security template are accumulated into the database. If this parameter is not specified and there are conflicting settings in the database and the template being imported, the template settings win.

/areas Specifies the security areas to be applied to the system. If this parameter is not specified, all security settings defined in the database are applied to the system. To configure multiple areas, separate each area by a space. The following security areas are supported:

SECURITYPOLICY Includes Account Policies, Audit Policies, EventLog Settings and Security Options.

GROUP_MGMT Includes Restricted Group settings

USER_RIGHTS Includes User Rights Assignment

REGKEYS Includes Registry Permissions

FILESTORE Includes File System permissions

SERVICES Includes System Service settings

/log filename Specifies a file in which to log the status of the configuration process. If not specified, configuration processing information is logged in the scesrv.log file which is located in the %windir%\security\logs directory.

/quiet Specifies that the configuration process should take place without prompting the user for any

Leading the way in IT testing and certification tools, www.testking.com

confirmation.

Example:

```
secdit /configure /db hisecws.sdb /cfg hisecws.inf /overwrite /log hisecws.log
```

For all filenames, the current directory is used if no path is specified.

Incorrect Answers:

A: The application servers are not domain members, so we cannot use group policy.

B: The Security Configuration and Analysis console is a graphical tool. We need to use the command line version in order to schedule it.

D: The application Servers are not domain members, so we cannot use group policy.

QUESTION NO: 153

You are a network administrator for TestKing. You install Windows Server 2003 on a server named TestKingA. You install a production application on TestKingA. You create a shared folder named ProdData on TestKingA to support the needs of the production application. All critical data files for the application are stored in the ProdData shared folder on TestKingA.

You install Windows Server 2003 in another server named TestKingB. You create a shared folder on TestKingB named ProdDataBackup.

The production application keeps many data files open. All the files in the ProdData folder must be backed up during each shift change. You are not allowed to stop and restart the production application without special approval.

You need to provide a backup solution for the critical files in the ProdData on TestKingA. Your solution must not affect the production application.

What should you do?

- A. On TestKingA, use the Backup or Restore Wizard to select the ProdData folder. Type \\TestKingB\ProdDataBackUp for the backup destination, and the advanced backup options to select the **Disable volume shadow copy** check box.
- B. On TestKingB, use the Backup or Restore Wizard to select the ProdData folder. Type \\TestKingA\ProdData for the backup destination, and use the advanced backup options to select the **Disable volume shadow copy** check box.
- C. On TestKingA, use the Backup or Restore Wizard to select the ProdData folder. Type \\TestKingB\ProdDataBackUp for the backup destination.
- D. On TestKingA, use the Backup or Restore Wizard to select the ProdData folder.

Type **\\TestKingA\ProdData** for the backup destination.

Answer: C

Explanation: To back up open files, the backup needs to be configured to use Shadow Copies. This is the default behaviour for the Windows Server 2003 backup program. Therefore, we just need to configure the backup program to backup the files to **\\TestKingB\ProdDataBackUp**.

Incorrect Answers:

A: We need to use Shadow Copies. This is enabled by default. We should not select the **Disable volume shadow copy** check box.

B: We need to use Shadow Copies. This is enabled by default. We should not select the **Disable volume shadow copy** check box.

D: **\\TestKingA\ProdData** is the wrong backup destination.

QUESTION NO: 154

You are a network administrator for TestKing. The network contains a Windows Server 2003, Enterprise Edition file server named TestKing3 that contains two volumes configured as drive H and drive J. Drive H contains 40 GB of unused space and drive J contains 12 GB of unused space.

TestKing3 contains the shared folders shown in the following table.

File system path	Share name	Disk space used by shared folders
H:\HomeFolders	HomeFolders	20 GB
H:\GroupFolders	GroupFolders	20 GB
J:\TestKingData	TKData	16 GB

Each file in the TestKingData folder is modified or deleted every seven days on average, and new files are added frequently. Users often request that prior versions of files be restored from backup tapes. All users have Windows XP Professional computers.

You want to enable users to restore prior versions of modified or deleted files in the TestKingData folder.

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

- A. Enable Shadow Copies of Shared Folders on drive J and configure an 8-GB storage area on drive J.
- B. Enable Shadow Copies of Shared Folders on drive J and configure a 20-GB storage area on drive H.
- C. Enable automatic caching of documents for TKData.
- D. Enable manual caching of documents for TKData.
- E. Install Twcli32.msi on each user's client computer.

F. Install Adminpak.msi on each user's client computer.

Answer: B, E

Explanation: The client software to access previous versions of files is Twcli32.msi. This needs to be installed on every client computer.

This is a difficult question because answer A or B will work. We need to decide which disk to store the shadow copies on. Drive H has enough spare space. With more space, we can store more shadow copies. Also, placing the shadow copies on a separate disk or volume provides better performance.

Determining Which Disk to Use to Store Shadow Copies

To store the shadow copies of another volume on the same file server, a volume can be dedicated on separate disks. For example, if user files are stored on H:\, another volume such as S:\ can be used to store the shadow copies. Using a separate volume on separate disks provides better performance and is recommended for heavily used file servers.

Important: If shadow copies are stored on the same volume as the user files, note that a burst of disk input/output (I/O) can cause all shadow copies to be deleted. If the sudden deletion of shadow copies is unacceptable to administrators or end users, it is best to use a separate volume on separate disks to store shadow copies.

QUESTION NO: 155

You are a network administrator for TestKing. The design team provides you with the following list of requirements for server disaster recovery:

- No more than two sets of tapes can be used to restore to the previous day.
- A full backup of each server must be stored off-site.
- A full backup of each server that is no more than one week old must be available on-site.
- Backups must never run during business hours.
- Tapes may be recalled from off-site storage only if the on-site tapes are corrupted or damaged.

A full backup of all servers requires approximately 24 hours. Backing up all files that change during one week requires approximately 4 hours. Business hours for the company are Monday through Friday, from 6:00 A.M. to 10:00 P.M.

You need to provide a backup rotation plan that meets the design team's requirements.

Which two actions should you include in your plan? (Each correct answer presents part of the solution. Choose two)

- A. Perform a full normal backup for on-site storage on Friday night after business hours.

- Perform a full copy backup for off-site storage on Saturday night after the Friday backups is complete.
- B. Perform a full normal backup for on-site storage on Friday night after business hours.
Perform another full normal backup for off-site storage on Saturday after the Friday backup is complete.
- C. Perform a full copy backup for on-site storage on Friday night after business hours.
Perform a full copy backup for off-site storage on Saturday night after the Friday backup is complete.
- D. Perform differential backups on Sunday, Monday, Tuesday, Wednesday, and Thursday nights after business hours.
- E. Perform incremental backups on Sunday, Monday, Tuesday, Wednesday, and Thursday nights after business hours.
- F. Perform incremental backups on Sunday, Tuesday, and Thursday nights after business hours.
Perform differential backup on Monday and Wednesday nights after business hours.

Answer: A, D

Explanation:

We do a normal backup on Friday, and the archive bit is cleared. We do a copy backup on Saturday and the archive bit is not cleared. We do a differential backup from Sunday, Monday, Tuesday, Wednesday, and Thursday. This way, we just need two tapes to restore, the full backup and the last differential backup.

Types of backup

The Backup utility supports five methods of backing up data on your computer or network.

Copy backup

A copy backup copies all the files you select, but does not mark each file as having been backed up (in other words, the archive attribute is not cleared). Copying is useful if you want to back up files between normal and incremental backups because copying does not affect these other backup operations.

Daily backup

A daily backup copies all the files that you select that have been modified on the day the daily backup is performed. The backed-up files are not marked as having been backed up (in other words, the archive attribute is not cleared).

Differential backup

A differential backup copies files that have been created or changed since the last normal or incremental backup. It does not mark files as having been backed up (in other words, the archive attribute is not cleared). If you are performing a combination of normal and differential backups, restoring files and folders requires that you have the last normal as well as the last differential backup.

Incremental backup

An incremental backup backs up only those files that have been created or changed since the last normal or incremental backup. It marks files as having been backed up (in other words, the archive attribute is cleared). If you use a combination of normal and incremental backups, you will need to have the last normal backup set as well as all incremental backup sets to restore your data.

Normal backup

A normal backup copies all the files you select and marks each file as having been backed up (in other words, the archive attribute is cleared). With normal backups, you only need the most recent copy of the backup file or tape to restore all of the files. You usually perform a normal backup the first time you create a backup set.

Backing up your data using a combination of normal backups and incremental backups requires the least amount of storage space and is the quickest backup method.

However, recovering files can be time-consuming and difficult because the backup set might be stored on several disks or tapes.

Backing up your data using a combination of normal backups and differential backups is more time-consuming, especially if your data changes frequently, but it is easier to restore the data because the backup set is usually stored on only a few disks or tapes.

QUESTION NO: 156

You are a network administrator for TestKing. The network design team decides that the DNS Server service must always be available.

The network design team requires that all computers on the network must always access the DNS Server service by using a single IP address. TCP/IP configurations for client computers and servers will contain a single DNS entry. The DNS Server service must be authoritative for all host (A) and service locator (SRV) resource records for the network. The DNS Server service must maintain all records in the event that there is a hardware failure of the DNS server.

You need to deploy DNS on the network. You need to comply with the network design team's requirements.

What should you do?

- A. Deploy DNS by using the Cluster service to configure a two-node server cluster in a failover configuration.
- B. Deploy DNS by using the Cluster service to configure a two-node server cluster that hosts DNS on both nodes simultaneously.
- C. Deploy DNS stub zones by using Network Load Balancing.
- D. Deploy multiple DNS servers that host secondary zones that are load balanced by using Network Load Balancing.

Answer: A

Explanation: We can use the Cluster service to configure a two-node server cluster in a failover configuration. Using the failover configuration, if one machine fails, the other machine will continue to run.

Incorrect Answers:

B: This configuration won't work.

C: We need a primary zone, not a stub zone. The DNS Server service must be authoritative for all host (A) and service locator (SRV) resource records for the network.

D: We need a primary zone, not secondary zones. The DNS Server service must be authoritative for all host (A) and service locator (SRV) resource records for the network.

QUESTION NO: 157

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: 158

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: 159

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: 160

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: 161**

You are the network administrator for TestKing. Your network consists of a single Active Directory domain named testking.com. There is an organizational unit (OU) named DocProcessing. The DocProcessing OU contains user accounts for users in the document processing department.

You create a Group Policy object (GPO) and link it to the DocProcessing OU. You configure the GPO to publish a graphics application. Some of the users in the document processing department report that the

application is not available from the Start menu, and other users report that the graphics application was installed successfully after they double-clicked a graphics application document.

You need to ensure that all users in the DocProcessing OU can successfully run the graphics application.

What should you do?

- A. Instruct users who report a problem to run the **gpupdate** command on their computers.
- B. Instruct users who report a problem to install the application by using Add or Remove Programs in Control Panel.
- C. Run the Resultant Set of Policy (RSOP) tool on the domain controllers on the network.
- D. Run the **gpresult** command on each client computer and domain controller on the network.

Answer: B

Explanation: You have **published** the applications to users. This setting makes the application available for users to install. In order to install a published application, users need to use the Add or Remove Programs applet in Control Panel, which includes a list of all published applications that are available for them to install.

Users in the document processing department report that the application is not available from the **Start menu**. It won't be available in the start menu because the application was published, not assigned.

Group Policy Management

Software installation

You can use the Software Installation extension of Group Policy to centrally manage software distribution in your organization. You can assign and publish software for groups of users and computers using this extension.

Assigning Applications

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.

Publishing Applications

You can also publish applications to users, making the application available for users to install. To install a published application, users can use **Add or Remove Programs** in Control Panel, which includes a list of all published applications that are available for them to install. Alternatively, if the administrator has selected the **Auto-install this application by file extension activation** feature, users can open a document file associated with a published application. For example, double clicking an .xls file will trigger the installation of Microsoft Excel, if it is not already installed. Publishing applications only applies to user policy; you cannot publish applications to computers.

Reference Server Help

Incorrect Answers:

- A: This will refresh the group policy. It won't make the application available in the start menu.
- C: This will display the resultant policy. It won't make the application available in the start menu.
- D: This will display the resultant policy. It won't make the application available in the start menu.

QUESTION NO: 162

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: 163

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 caused by DNS replication.

B: The PDC emulator isn't used in the logon process (except for down-level clients).

QUESTION NO: 164

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 (or A)

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: 165

You are the network administrator for your company. 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: 166

You are the network administrator for TestKing. The network consists of a single Active Directory forest that contains five domains and 30 remote sites located in cities throughout the world. There are a total of 40,000 users in the five domains. All remote sites are connected to the company network by unreliable 56-Kbps WAN connections.

Each site contains at least one domain controller and one global catalog server. All domain controllers in the forest run Windows Server 2003. The functional level of all the domains in the forest is Windows 2000 native.

You plan to deploy several Active Directory-enabled applications over the next six months. Each of these applications will add attributes to the global catalog or modify existing attributes in the global catalog.

You need to make modifications to the Active Directory infrastructure in order to prepare for these deployments. You plan to accomplish this task during off-peak hours. You need to ensure that you can minimize any potential network disruption that would be caused by the deployment of these applications in the future. You also need to ensure that the modifications do not disrupt user access to resources.

What should you do?

- A. Decrease the tombstone lifetime attribute in the Active Directory Schema NIDS-Service object class.
- B. Remove the global catalog role from the global catalog servers in each remote site.
- C. Raise the functional level of the forest to Windows Server 2003.
- D. Configure universal group membership caching in each remote site.

Answer: C

Explanation

To prepare for the new application the best option is to raise the forest functional level. This will enable us to deactivate any wrong schema class, and make DNS and AD partitions for the new applications

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: 167

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: 168

You are a network administrator for TestKing. The network consists of a single Active Directory domain named testking.com. Password resets are performed on user accounts on all servers regularly throughout each day. The Windows Server 2003 computers named TestKingA, TestKingB, and TestKingC are configured as shown in the following table.

Server name	Site	Server role	Backup schedule
TestKingA	Toronto	Global catalog server	Daily
TestKingB	San Francisco	Domain controller, forest-wide and domain-wide operations master roles	Daily
TestKingC	Boston	Global catalog server	Weekly on Fridays

One Wednesday morning, another network administrator in Boston connects to TestKingC and deletes an organizational unit (OU) named BostonUsers. The change replicates to all sites in the forest.

Users in Boston report that they can no longer log on to the network.

You need to provide the users in Boston with the ability to log on to the network as soon as possible. You must also ensure that there is minimal disruption to the users in Toronto and San Francisco.

What should you do?

- A. Restore the BostonUsers OU on TestKingA from backup.
Use the Ntdsutil utility to mark the BostonUsers OU as authoritative.
Allow replication to take place.
- B. Restore the BostonUsers OU on TestKingB from backup.
Allow replication to take place.
- C. Restore the Ntdsutil utility to connect to TestKingA.
Use the **metadata cleanup** command to remove TestKingC from Active Directory.
Force replication.
- D. Use the Ntdsutil utility on TestKingC to mark the domain context as authoritative.
Force replication.

Answer: A

Explanation: We need to restore the BostonUsers OU. We should restore it on TestKingA because that domain controller has a more recent backup. We need to mark the BostonUsers OU as authoritative so that it gets replicated to the other domain controllers. If we didn't mark the BostonUsers OU as authoritative, it would get deleted again at the next AD replication.

Incorrect Answers:

B: We need to mark the BostonUsers OU as authoritative so that it gets replicated to the other domain controllers. If we didn't mark the BostonUsers OU as authoritative, it would get deleted again at the next AD replication.

C: We need to restore the BostonUsers OU. This won't restore the OU.

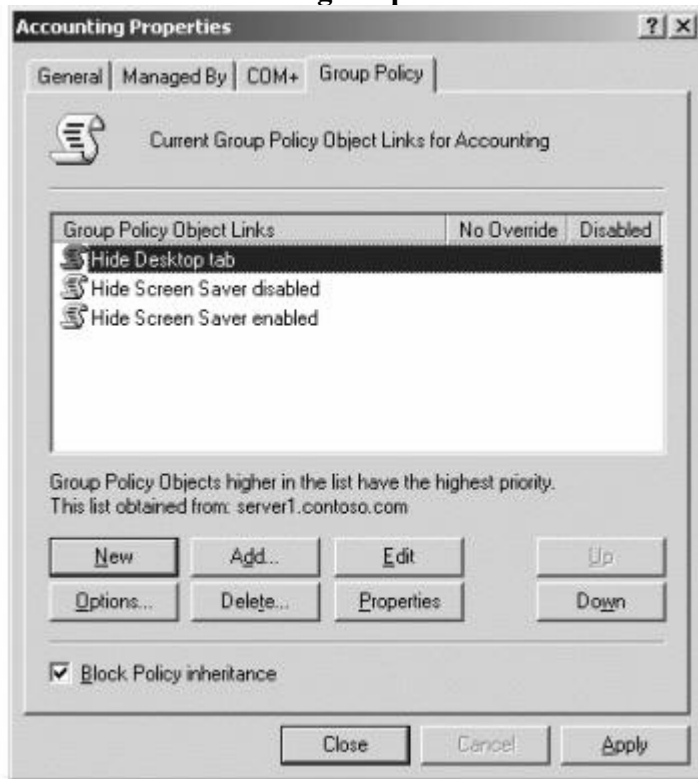
D: We need to restore the BostonUsers OU. This won't restore the OU.

QUESTION NO: 169

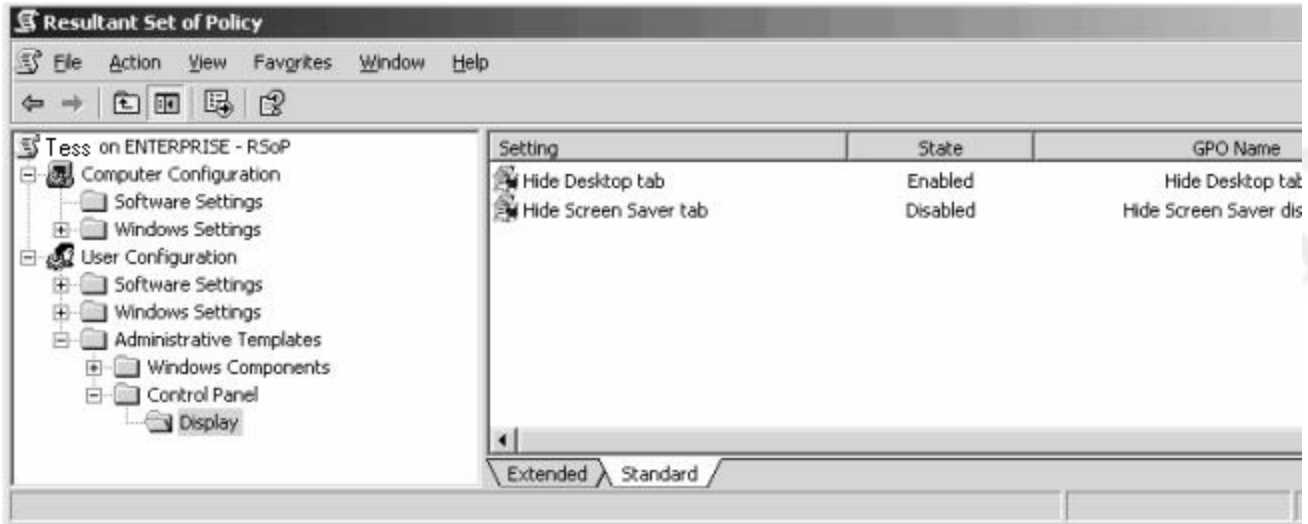
You are the network administrator for TestKing. The network consists of a single Active Directory domain named testking.com. The domain contains an organizational unit (OU) named Accounting.

A user named Tess works in the accounting department. A user account for Tess is located in the Accounting OU.

You create three Group Policy objects (GPOs) and link them to the Accounting OU. The three policies are shown in the Accounting Properties exhibit.



You run Resultant Set of Policy (RSoP) in logging mode for Tess's user account. The results for the policies that apply to Tess's user account are shown in the RSoP Settings exhibit.



You need to ensure that the Desktop tab and the Screen Saver tab are disabled.

What should you do?

- A. Move the Hide Screen Saver disabled GPO higher in the priority list in the **Group Policy Object Links** area of the **Accounting Properties** dialog box.
- B. Move the Hide Screen Saver disabled GPO lower in the priority list in the **Group Policy Object Links** area of the **Accounting Properties** dialog box.
- C. Disable the **Block Policy inheritance** setting on the Accounting OU.
- D. Click the **Options** button in the **Accounting Properties** dialog box and enable the **No Override** setting on the Hide desktop tab GPO.

Answer: B

Explanation: The Desktop tab is hidden, so we just need to hide the Screen Saver tab. With the current settings, the Hide Screen Saver Enabled policy is applied first. It is then overwritten by the Hide Screen Saver Disabled policy. The result being that that the Screen Saver tab is not hidden. We can rectify this by moving the Hide Screen Saver disabled GPO lower in the priority list in the **Group Policy Object Links** area of the **Accounting Properties** dialog box. This will mean that that the Hide Screen Saver Disabled policy is applied first and is then overwritten by the Hide Screen Saver Enabled policy.

Incorrect Answers:

- A:** The Hide Screen Saver disabled GPO is already higher in the priority list than the Hide Screen Saver Enabled GPO. It needs to be lower.
- C:** The problem is caused by the OU policies. Unblocking inheritance won't affect the OU policies.
- D:** This won't affect the policies applied at this OU level. This would only affect child OUs if they existed.

QUESTION NO: 170

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