



Exam : 070-297

Title : Designing a Microsoft Windows Server ☐☐☐☐☐☐☐☐☐☐

2003 Active Directory and Network Infrastructure

Ver : 09-10-07

Topic 1, Stanford Finance, Scenario

Background

Stanford Finance is a private company that specializes in the provision of investment and asset management services for its clients. Stanford Finance operates across two continents, namely Europe and North America.

Physical Locations

The Stanford Finance headquarters are located in New York, USA, and its branch office is in London, Europe. The following table shows the number of employees in these offices:

Office type	Location	Employees
Headquarters	New York	120
Branch office	London	110

Anticipated growth foreseen for Stanford Finance is estimated at approximately 50 percent in employee numbers over the next five years.

Each office has a full complement of IT personnel.

Current situation:

Business processes

1. All Stanford Finance customers commission their funds for investments to be purchased by Stanford Finance via e-mail.
2. Stanford Finance prepares the necessary documentation and legislative procedures required in investing the customers' funds: the administrative staff records all the necessary details of the customers and the brokers invest the funds on behalf of the customers.
3. All Stanford Finance customers can keep track of their investments and investment accounts by logging on to the Web site.
4. From time to time surveys are conducted to gauge customer satisfaction level.

Active Directory services

The current network is based on Active Directory and is operative in a Microsoft Windows 2000 environment. Unfortunately the network was set up as an interim measure and as such has not been properly designed to support the business operations. To this end the network has to be redesigned.

Network infrastructure and connectivity

The Stanford Finance network uses an internal DNS namespace of finance.com and a NetBIOS domain name of FINANCE.

All servers on the Stanford Finance network run Microsoft Windows 2000 Server and all client computers run either Microsoft Windows 2000 Professional or Microsoft Windows XP Professional.

Some applications, used by the Stanford Finance employees, still require NetBIOS over TCP/IP.

The New York and London offices are connected by a dedicated T1 link.

The Stanford Finance network is connected to the Internet via a firewall.

Web Services

When Stanford Finance decided to establish its Web presence, it was brought to their attention that the name finance.com was already taken as it was registered by another company. To this end Stanford Finance then registered the name stanfordfinance.com and outsourced the hosting of its Web site to an Internet Service Provider (ISP).

Future situation:

Planned Changes

1. The entire network needs to be redesigned. This will enable Stanford Finance to offer its clients better service and to better support business operations.
2. The new network is to be based on Microsoft Windows Server 2003.
3. The Web site is to be redesigned to enable customers to:
 - o submit their information
 - o track the status of their investments
 - o access their billing / administration fees data
1. The Web site is to be hosted by Stanford Finance staff and not the ISP.

Problem Statements

Chief Executive Officer (CEO)

"I have received some feedback from a survey that we ran last month and the results raised some concerns that we need to address. The main concern that surfaced from this survey is that our customers find it extremely inconvenient to exchange important and confidential data by using regular e-mail. We need to provide our customers with secure Internet access to our new Web site which will be used as a front-end interface for accessing all the other relevant services such as tracking the status of customer investments, accessing their billing/administration fee data, etc."

Chief Information Officer (CIO)

"The redesign of our network is a great opportunity to make a clean start. But although we are going to make a clean start it does not necessarily mean a clean slate: we are not going to register any additional names with Internet Authorities. The internal namespace must be intuitive and should not cause any confusion or conflicts with any registered names on the Internet."

"We will implement two distinct networks: one internal and the other external. I suggest that the two networks be administratively independent from each other. As such they will have to be managed separately by two independent groups of IT personnel."

"Our employees should be able to access resources on both networks and on the Internet. Our Customers should be able to access only the external network over the Internet. It so happens that some of our customers are also companies in their own right and not just individuals. For these customer companies we should designate an IT team that will support that customer's access to the external network. This will include the creation and management of the necessary user accounts and assigning permissions for the appropriate resources."

"Our staff that visit the customers will connect to the internal network through virtual private networks (VPNs). They must be provided with the necessary, appropriate access to the resources anywhere on our network."

Chief Security Officer (CSO)

"A new phenomenon has surfaced. We have a situation where end users are installing their own software on the Stanford Finance network client computers. This is a practice that should not be allowed to carry over to our new network. We must ensure that our users do not install unauthorized software on the company client computers."

"We must ensure that all our servers that provide connections to our network are secure. All connections to these servers must be authenticated."

Information Technology (IT) manager

"We need the new DNS infrastructure to be secure. I suggest that only authorized computers should be allowed to register with our DNS servers. Absolutely no DNS information regarding the internal network should be exposed to the external network or the Internet. We should also endeavor to keep name resolution traffic through the firewalls to a minimum."

"We also need to keep network traffic between New York and London to a minimum. We should therefore configure the firewalls to block all unauthorized traffic to both the internal and external networks."

"We should only make use of DHCP-assigned IP addresses for all our client computers on the internal network. Also if we are to maintain the existing line-of-business applications currently in use, we cannot discontinue supporting NetBIOS over TCP/IP on the internal network. To this end all client computers on the internal network will be configured to use DHCP to obtain the addresses of DNS and WINS servers. Furthermore we need to ensure that all network services are implemented in a fault tolerant way. We cannot allow having a situation where one of our servers fails then we do not have access to that service."

"I also want to suggest that we enable our internal users to access all the necessary resources by using a single set of logon credentials. For security reasons we cannot extend the single set of credential-access to the customer companies. They will not be allowed access to our internal network. However, they will be provided with a user name and a password to access resources on the external network."

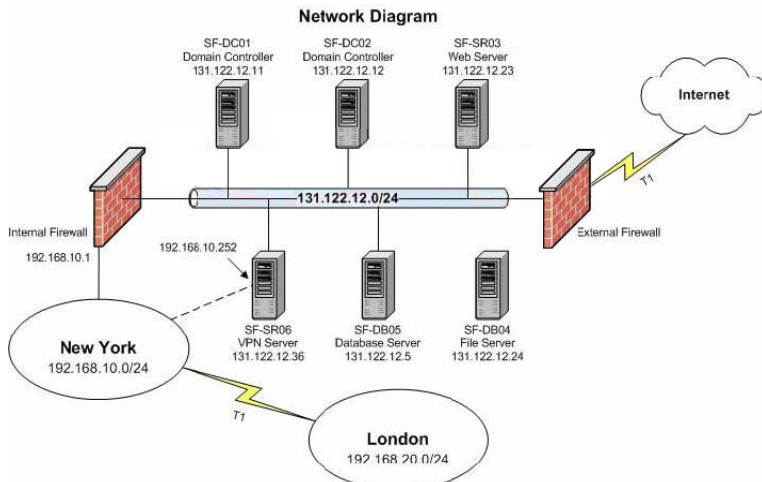
End User

"The current environment is difficult to use. Information is scattered on the network, making it difficult to find. There does not seem to be any clear definition as to who is responsible for responding to network and computer problems. Because of this confusion, most users manage their own computers."

"Also, we want to be able to connect to the network when working remotely. Very often we need to visit customers to service their needs and then we cannot capture their details immediately because we are unable to access an ISP when we are out of office."

Envisaged network infrastructure

1. Customers will be able to connect to a secure Web site.
 2. The secure Web site will be hosted on the external network.
 3. A Web application will provide a Web-based, front-end client interface to all the necessary resources on the external network.
 4. Stanford Finance users will log on to the internal network from their client computers.
 5. Stanford Finance users will also be allowed to establish VPN connections over the Internet.
 6. Stanford Finance users issued with laptop computers to service customers in the customer locations will be allowed to use their laptop workstations to establish VPN connections over the Internet using the local phone numbers of a global ISP.
 7. All Stanford Finance VPN users will be provided with the same scope of access to the network as the Stanford Finance users who work from the offices.
 8. An Exchange Server 2003 organization will be deployed on the internal network.
- The envisaged network is shown in the Network Infrastructure exhibit:



Topic 1, Stanford Finance (13 Questions)

QUESTION 1

You need to create the Active Directory structure to address the concerns voiced by the Chief Information Officer.

What should you do?

- A. Create one forest with two domains.
- B. Create one forest with a single domain.
- C. Create two forests, each with a single domain.
- D. Create three forests, each with a single domain.
- E. Implement a workgroup environment on both networks.

Answer: C

Explanation: You need to implement two forests: One for the internal network and the other for the external network. The internal forest must be a single domain because the amount of internal users, in both the Stanford Finance offices, is relatively low. And there is no mention made of creating a separate domain for each location. Typically with a T1 connection between geographically dispersed offices, a single domain is considered appropriate, even if there are more than 100,000 users and only 1 % of WAN bandwidth is available for Active Directory replication.

1. We will implement two distinct networks: one internal and the other external. I suggest that the two networks be administratively independent from each other. As such they will have to be managed separately by two independent groups of IT personnel

2. We enable our internal users to access all the necessary resources by using a single set of logon credentials.

1. An Exchange Server 2003 organization will be deployed on the internal network.

Incorrect answers:

A: A single forest for both these networks will not work because then you cannot have two complete separate networks as is required because then all domains in the same forest must trust each other.

B: A single forest for both these networks will not work because then you cannot have two complete separate networks as is required because then all domains in the same forest must trust each other. Also the Enterprise Admins group members will have authority over both domains in the forests which violate the one requirement of independent management of the networks.

D: If you were to create three forests, then you will not be able grant all users on the internal network access to all appropriate resources, regardless of their physical location since an Exchange server will be deployed on the internal network, and an Exchange Server organization cannot span forests.

E: If you were to implement a workgroup environment on each of the networks, then you will fail to meet the single sign-on requirements for the Stanford Finance users.

Reference:

Walter Glenn, and Michael T. Simpson, MCSE 70-297 Training Kit - Designing a Windows server 2003 Active Directory and Network Infrastructure, Chapter 4, pp. 4-10.
Microsoft Windows Server 2003 Deployment Kit: Designing Active Directory - designing the Active Directory Logical Structure: Creating a Forest Design

QUESTION 2

You need to create the Active Directory structure to address the concerns voiced by the Chief Information Officer. A decision has then been made to implement two forests, each with a single domain. Now you need to implement this new Active Directory logical structure.

What should you do? (Each answer presents part of the solution. Choose THREE.)

- A. Upgrade domain controllers to Microsoft Windows Server 2003.
- B. Use Active Directory Migration Tool (ADMT).
- C. Create a pristine forest.
- D. Create an external trust.
- E. Create a child domain.
- F. Upgrade member servers.

Answer: B, C, D

Explanation: First you need to create a pristine forest as stipulated by:

1. The current network is based on Active Directory and is operative in a Microsoft Windows 2000 environment. Unfortunately the network was set up as an interim measure and as such has not been properly designed to provide support the business operations. To this end the network has to be redesigned.

Your next step would be to create an external trust between the old and the new domains so as to ensure that users will continue to have access to the resources that remain in the old domain as their users accounts are being migrated to the new domain.

The next step will involve migrating the user accounts from the existing domain to the new domain. Make use of Active Directory Migration Tool (ADMT) which will automate the migration process.

Incorrect answers:

A: Upgrading domain controllers is required if you were performing an in-place upgrade

of the domain. However, then you will not be able to migrate domain controllers without first demoting them to member servers.

E: There is no need to create a child domain as there is no requirement that states the necessity of a child domain.

F: Upgrading member servers to Windows Server 2003 might be desirable, but this is not an explicit requirement of the scenario.

Reference:

Walter Glenn, and Michael T. Simpson, MCSE 70-297 Training Kit - Designing a Windows server 2003 Active Directory and Network Infrastructure, Chapter 4, pp. 4-10.
Microsoft Windows Server 2003 Deployment Kit: Designing Active Directory - designing the Active Directory Logical Structure: Active Directory between Forests

QUESTION 3

You need to create the Active Directory structure to address the concerns voiced by the Chief Information Officer. A decision has then been made to implement two forests, each with a single domain. Now you need to implement this new Active Directory logical structure. You already decided on the creation of a pristine forest. What should you do next?

- A. Raise the functional level of the new domain to Windows 2000 native.
- B. Use Active Directory Migration Tool (ADMT).
- C. Create an external trust.
- D. Create a child domain.

Answer: A

Explanation: By default, the functional levels of the new forest and domain will be set to the lowest levels after creating the pristine forest. You should raise the domain functional level to either Windows 2000 native or Windows Server 2003 because only a domain at either of these levels can be a target for migration using ADMT.

1. The current network is based on Active Directory and is operative in a Microsoft Windows 2000 environment. Unfortunately the network was set up as an interim measure and as such has not been properly designed to provide support the business operations. To this end the network has to be redesigned.

Incorrect answers:

B: This is the logical consequential step to use after you created an external trust between the old and the new domains. This is not done directly after creating the pristine forest.

C: Your next step would be to create an external trust between the old and the new domains so as to ensure that users will continue to have access to the resources that remain in the old domain as their users accounts are being migrated to the new domain. But this can only be done after you ensure that the domain can be a target for migration.

D: There is no need to create a child domain as there is no requirement that states the necessity of a child domain.

Reference:

Walter Glenn, and Michael T. Simpson, MCSE 70-297 Training Kit - Designing a Windows server 2003 Active Directory and Network Infrastructure, Chapter 4, pp. 4-10.

Microsoft Windows Server 2003 Deployment Kit: Designing Active Directory -
designing the Active Directory Logical Structure: Active Directory between Forests

QUESTION 4

You are designing a DNS implementation strategy to meet the business and technical requirements on the new network.

What should you do?

- A. Implement a private root zone on the internal network.
- B. Create a stub zone on the external network DNS servers for the DNS zone on the internal network.
- C. Implement primary zones and secondary zones on the internal network.
- D. Configure forwarding on the internal network DNS servers to the DNS servers on the external network.
- E. Configure a delegation on the external network DNS servers to the DNS zone on the internal network.

Answer: D

Explanation

: you need to configure forwarding on the internal network DNS servers to the DNS servers on the external network as this will ensure that clients on the internal network can resolve the external and Internet names.

1. Our employees should be able to access resources on both networks and on the Internet.
2. We are not going to register any additional names with Internet Authorities. The internal namespace must be intuitive and should not cause any confusion or conflicts with any registered names on the Internet

Incorrect Answers:

A: A private root zone is ideal for a very large network that included multiple domains that is organized in a multi layered hierarchy. However using a private root zone in this scenario will not provide any advantage and will result in complicating DNS administration.

B: A stub zone is a zone that contains information only about the authoritative servers for a particular zone. Implementing a stub zone in this scenario as suggested here will cause the DNS servers on the internal network to respond to the DNS queries for names on the external network by returning a referral to the authoritative DNS server. This is not what is required:

1. Absolutely no DNS information regarding the internal network should be exposed to the external network or the Internet.

C: For standard primary zones, only a single server can host and load the master copy of the zone. If you create a zone and keep it as a standard primary zone, no additional primary servers for the zone are permitted. The standard primary model implies a single point of failure.

E: If you created a delegation to the internal zone, then the external DNS servers could be used for referrals to the internal DNS servers to Internet users. This will be unacceptable:

1. Absolutely no DNS information regarding the internal network should be exposed to the external network or the Internet.

Reference:

Walter Glenn, and Michael T. Simpson, MCSE 70-297 Training Kit - Designing a Windows server 2003 Active Directory and Network Infrastructure, Chapter 6, pp. 6-12 to 6-13.

Microsoft Windows Server 2003 Online Help - Network services - Understanding DNS, domain names, how DNS query works, understanding forwarders

QUESTION 5

You need to decide on a strategy to design DNS name resolution for the internal users. The internal users need to be able to resolve names on the external network in this scenario.

What should you do? (Each correct answer presents a complete solution. Choose THREE.)

- A. On the external DNS servers configure delegations to the ISP's DNS servers.
- B. On the external network implement a private root zone.
- C. On the internal DNS servers create a secondary stanfordfinance.com zone.
- D. On the internal DNS servers create a stub zone for the stanfordfinance.com zone.
- E. On the internal DNS servers configure forwarding to the external DNS servers.
- F. On the internal DNS servers create delegations for the stanfordfinance.com zone.
- G. Configure internal DNS servers to perform conditional forwarding to the external DNS servers and to forward queries for all Internet names to the ISP's DNS server.

Answer: C, D, E

Explanation: You could create a secondary stanfordfinance.com zone on the internal DNS servers and configure the external DNS servers to allow zone transfers to the internal DNS servers to enable internal users to resolve names on the external network. A stub zone is a zone that contains information only about the authoritative servers for a particular zone. Implementing a stub zone in this scenario as suggested here will allow the internal users the ability to resolve names on the external network.

You should configure forwarding to the external DNS servers on the internal DNS servers. This will result in the internal DNS servers forwarding queries for external and Internet names to the DNS servers on the external DNS network.

Incorrect answers:

A: A delegation is a name server (NS) record in a parent zone that points to a DNS server that is authoritative for the child zone. You should not create a delegation on the external network.

B: A private root zone is ideal for a very large network that included multiple domains that is organized in a multi layered hierarchy. However using a private root zone in this scenario will not provide any advantage and will result in complicating DNS administration since both the internal and the external network each consists of a single domain.

F: A delegation is a name server (NS) record in a parent zone that points to a DNS server

that is authoritative for the child zone. In this scenario the DNS zone on the internal network should then be a child of the zone on the external network. Therefore you should not create a delegation from a child zone to a parent zone.

G: Configuring internal DNS servers to perform conditional forwarding to the external DNS servers and to forward queries for all Internet names to the ISP's DNS server, will work, however it will also result in excessive name resolution traffic across the firewalls. This will be because the internal DNS server would have to pass traffic to a DNS server behind the firewall to query at least three DNS servers across the firewall to be able to resolve an Internet name.

Reference:

Walter Glenn, and Michael T. Simpson, MCSE 70-297 Training Kit - Designing a Windows server 2003 Active Directory and Network Infrastructure, Chapter 6, pp. 6-12 to 6-13.

Microsoft Windows Server 2003 Online Help - Network services - Understanding DNS, domain names, how DNS query works, understanding forwarders

Jerry Honeycutt, Introducing Microsoft Windows Server 2003, Microsoft Press, Chapter 6.

QUESTION 6

You need to create the physical design for the Active Directory and Network Infrastructure for the new Stanford Finance network. To this end you need to decide what type of traffic should be allowed to pass through the external firewall. What should you do? (Each correct answer presents part of the solution. Choose TWO)

- A. Allow DNS, VPN, RPC and WINS traffic to pass through the external firewall.
- B. Allow DNS, VPN and HTTP traffic to pass through the external firewall.
- C. Allow POP3, SMTP and DHCP traffic to pass through the external firewall.
- D. Allow HTTPS and SMTP traffic to pass through the external firewall.
- E. Allow DNS and POP3 traffic to pass through the external firewall.

Answer: B, D

Explanation: it is stated in the scenario that:

1. We should therefore configure the firewalls to block all unauthorized traffic to both the internal and external networks.

Therefore you should allow DNS, VPN, HTTP, HTTPS and SMTP traffic to pass through the external firewall.

DNS - depending on the particular DNS implementation on the external network, you could block or allow incoming DNS traffic through the external firewall.

VPN - the Stanford Finance users with laptop workstation will make use of VPNs to connect to the resources on the internal network

HTTP - the general public will use HTTP to connect to the Stanford Finance public Web site.

HTTPS - the external network users will use HTTPS to connect to the Stanford Finance secure Web site.

SMTP - this will be required for Internet e-mail delivery.

Incorrect answers:

A: This option is partly correct except for RPC and WINS traffic. RPC is a means of interprocess communication which is commonly used within a protected environment, not over the Internet. This will make the network vulnerable. Wins traffic should actually be blocked since you should not allow Internet users the ability to resolve the NetBIOS names of any of the computers on the internal or the external network.

C: This option is partly correct except for POP3 and DHCP traffic because POP3 is used to retrieve mail and messages from mailboxes, and DHCP across the external firewall is not a requirement.

E: This option is partly correct except for POP3 traffic that should not be allowed to pass through the external firewall. POP3 is a protocol commonly used by e-mail clients for retrieving messages from mailboxes.

Reference:

TechNet - IT solutions Microsoft Systems Architecture Version 2.0 - reference Architecture Kit.

QUESTION 7

You need to create the physical design for the Stanford Finance Active Directory and Network Infrastructure. To this end you need to take a decision as to which routing solution to implement so as to support VPN clients as suggested in the scenario.

What should you do?

- A. Configure SF-SR06 as a dynamic router.
- B. Create a static route that points to the London subnet on SF-SR06.
- C. Create a static route that points to the New York internal subnet on SF-SR06.
- D. Configure the New York DHCP server to assign the default gateway address 192.168.10.1.

Answer: B

Explanation: A client computer connects to the Internet through an ISP and is configured with a primary IP address and the default gateway is automatically assigned by the ISP. Upon establishing a VPN connection with a VPN server, the VPN server assigns another IP address to the client computer. In this particular scenario this address assignment is done by the DHCP scope that corresponds to the New York subnet. By default a new route is automatically created on the VPN client to ensure that all packets that are not directed to the subnet to which the primary address belongs are sent to the VPN server. The VPN server then uses its routing table to route those packets to their destinations. Therefore to ensure that all VPN client can access resources in the London subnet, you should create a static entry that points to the London subnet in the routing table on the VPN server.

1. Stanford Finance users will also be allowed to establish VPN connections over the Internet.
2. Stanford Finance users issued with laptop computers to service customers in the

customer locations will be allowed to use their laptop workstations to establish VPN connections over the Internet using the local phone numbers of a global ISP.

3. All Stanford Finance VPN users will be provided with the same scope of access to the network as the Stanford Finance users who work from the offices.

Incorrect answers:

A: Dynamic routing would be unnecessary in this scenario and will only contribute to excessive network traffic between routers. Besides, only if the other routers on the network supported dynamic routing would you need to configure the VPN server as a dynamic router.

C: The VPN server is directly connected to the New York internal subnet. Therefore the VPN server's routing table already includes an entry that points to the New York subnet.

D: All computers on the New York internal subnet should be configured with the default gateway address 192.168.10.1, which is the internal interface of the internal firewall. But if you configured the New York DHCP server to assign the default gateway address 192.168.10.1 then some client computers on the New York subnet might not be configured with a default gateway address because they might get their configuration from the London DHCP server. This will not help the VPN client to access resources on the London subnet.

Reference:

Microsoft Windows Server 2003 Deployment Kit: Deploying dial-up and VPN remote Access Services - designing and providing support for remote access clients.

Walter Glenn, and Michael T. Simpson, MCSE 70-297 Training Kit - Designing a Windows server 2003 Active Directory and Network Infrastructure, Chapter 4 , pp. 4-26.

QUESTION 8

You need to design the NetBIOS name resolution strategy on the internal network. What should you do?

- A. Install a WINS server in both the New York and the London offices.
- B. Install two WINS server in the New York office.
- C. Install one WINS server in the New York office.
- D. Configure all DNS servers to perform WINS lookup.

Answer: A

Explanation: each office should have a WINS server that will support NetBIOS name resolution. Although Windows 2000 and later do not require NetBIOS, you need to provide NetBIOS name resolution capabilities for the Exchange Server 2003 application that will be deployed.

1. An Exchange Server 2003 organization will be deployed on the internal network.
2. We cannot discontinue supporting NetBIOS over TCP/IP on the internal network. To this end all client computers on the internal network will be configured to use DHCP to obtain the addresses of DNS and WINS servers.

On a small non-routed network, NetBIOS name resolution can be performed using local broadcasts, however, NetBIOS broadcasts cannot pass through routers on a routed network.

Incorrect answers:

B: A typical WINS server in Windows Server 2003 can support up to 10,000 clients. In this scenario the number of users will not exceed a few hundred. Two WINS servers in the New York office would be overkill. You should rather have the offices each with a WINS server.

C: Though a Windows Server 2003 WINS server is capable of supporting 10,000 clients, the network consists of two sites that are connected through a relatively slow WAN link. Therefore to minimize NetBIOS name registration and resolution traffic over the WAN link and to provide some measure of fault tolerance you should rather have both the offices have a WINS server each.

D: WINS lookup in DNS is used to enable DNS servers to resolve DNS names of the legacy computers whose NetBIOS names are registered on WINS. But it cannot register themselves with DNS.

Reference:

Walter Glenn, and Michael T. Simpson; MCSE 70-297 Training Kit - Designing a Windows server 2003 Active Directory and Network Infrastructure, Chapter 7, pp. 7-16 to 7-24.

Microsoft Windows Server 2003 Deployment Kit: Integrating DNS with other Windows Server 2003 Services - Integrating DNS with WINS

QUESTION 9

You need to design security for remote access users. To this end you must configure the firewalls to support VPN users.

What should you do?

- A. Allow all VPN traffic to traverse both firewalls.
- B. Block all VPN traffic on the internal firewall.
- C. Allow all VPN traffic to traverse the external firewall.
- D. Allow only VPN traffic that originates from 192.168.10.252 by configuring the external firewall accordingly.
- E. Allow only VPN traffic that originates from 131.122.12.0/24, the London office, by configuring the internal firewall accordingly.

Answer: B, C

Explanation: All Internet traffic that is destined for the Stanford Finance network has to pass the external firewall and be directed to the VPN server on the external network. The other computers are not configured as VPN servers and will therefore not accept VPN connection requests. The VPN server will route authorized requests directly to the New York office subnet on the internal network, bypassing the internal network. The return VPN traffic with responses to VPN client requests will follow the same path in the opposite direction. This means that you should configure the external firewall to allow all VPN traffic to pass through. And all VPN traffic on the internal firewall should be blocked because no legitimate VPN traffic will be directed to the internal firewall.

Incorrect answers:

A: This will not meet the requirements since there will not be any legitimate VPN traffic

that will be directed to the internal firewall. Therefore you should not allow all VPN traffic to traverse both firewalls.

D: This VPN server is already behind the external firewall and this option is therefore incorrect.

E : If you allow VPN traffic that originate from the London offices by configuring the internal office accordingly, then you will be allowing illegitimate VPN traffic to pass.

Reference:

Microsoft Windows Server 2003 Deployment Kit: Deploying dial-up and VPN remote Access Services - designing and providing support for remote access clients

Jerry Honeycutt: Introducing Microsoft Windows Server 2003, Microsoft Press, Chapter 6

QUESTION 10

You must design the Stanford Finance IP address assignment strategy. To this end you need to implement the DHCP service on the internal network.

What should you do?

- A. Install a DHCP server in both the New York and London offices. Then configure a single scope and an exclusion range.
- B. Install a DHCP server in both the New York and London offices. Then configure two scopes: Then configure an exclusion range for each scope.
- C. Install two DHCP servers in the New York office. Then configure a superscope with two member scopes on each DHCP server. Then configure an exclusion range that corresponds to one of the member scopes.
- D. Install a DHCP server in both the New York and London offices. Then configure a superscope with two member scopes on each DHCP server. Then configure an exclusion range that corresponds to one of the member scopes.

Answer: B

Explanation: DHCP is responsible for the provision of dynamic address allocation and TCP/IP configuration parameters to client computers. You need to implement a DHCP server in each office then configure it to provide addresses to clients on both subnets. Therefore you should configure one scope for the local subnet and one scope for the other subnet. In New York you need to exclude 20% of the addresses from the scope that corresponds to the New York subnet and exclude 80% of the addresses from the scope that corresponds to the London subnet. And in London you should exclude 20% of the addresses from the scope that corresponds to the London subnet and exclude 80% of the addresses from the scope that corresponds to the New York subnet. This is required to ensure that each server has a unique pool of addresses and no address conflicts can occur. Then (not mentioned here) you should enable clients on each subnet to use DHCP server on the other subnet, you should implement DHCP Relay Agent either on the routers or on one server on each subnet.

1. We should only make use of DHCP-assigned IP addresses for all our client computers on the internal network. Also if we are to maintain the existing line-of-business applications currently in use, we cannot discontinue supporting NetBIOS over TCP/IP on

the internal network. To this end all client computers on the internal network will be configured to use DHCP to obtain the addresses of DNS and WINS servers

Incorrect answers:

A: A DHCP client accepts TCP/IP settings from the DHCP server that is the first one to respond to the client's request. Therefore, normally, each DHCP server will service only the clients in the local subnet. Should one of the servers be temporarily unavailable, the remaining server will service clients on both subnets. Therefore this option is not as efficient.

C: A superscope is a set of one or more member scopes that is used to support multiple logical subnets on the same physical network segment. In Stanford Finance there is no mention made of any network segments that includes multiple logical subnets. Therefore this option is irrelevant.

D: A superscope is a set of one or more member scopes that is used to support multiple logical subnets on the same physical network segment. In Stanford Finance there is no mention made of any network segments that includes multiple logical subnets. Therefore this option is irrelevant.

Reference:

Microsoft Windows Server 2003 Deployment Kit: Deploying DHCP - creating your DHCP server design, defining scopes.

Walter Glenn, and Michael T. Simpson; MCSE 70-297 Training Kit - Designing a Windows server 2003 Active Directory and Network Infrastructure, Chapter 4 , pp. 4-26.

QUESTION 11

You need to design the remote access infrastructure for the Stanford Finance network. To this end you need to configure the VPN server the meet the stated requirements.

What should you do? (Each correct answer presents part of the solution. Choose TWO.)

- A. On the VPN server create a static pool of addresses for assignment to VPN clients.
- B. On the VPN server enable Bandwidth Allocation Protocol (BAP).
- C. On the VPN server configure DHCP Relay Agent.
- D. Configure the VPN server to use the DHCP server to assign IP addresses to VPN clients.

Answer: C, D

Explanation: In the Stanford Finance network the VPN clients must be assigned IP addresses. This can be done either by using a static pool of addresses or using a DHCP server. In this scenario it is stated the all client computers use DHCP to acquire their IP addresses. Therefore you should configure the VPN server to use the DHCP server to assign IP addresses to the VPN clients. And then configure the DHCP Relay Agent on the VPN server.

1. We should only make use of DHCP-assigned IP addresses for all our client computers.

Incorrect answers:

A: The scenario states pertinently that all client computers are to use DHCP-assigned IP

addresses. Therefore you should not make use of a static pool of addresses even though it will also work.

B: BAP cannot be used on an entire VPN tunnel between a VPN client and a server, therefore you cannot use this option.

Reference:

Microsoft Windows Server 2003 Deployment Kit: Deploying DHCP - creating your DHCP server design, defining scopes.

Walter Glenn, and Michael T. Simpson; MCSE 70-297 Training Kit - Designing a Windows server 2003 Active Directory and Network Infrastructure, Chapter 4 , pp. 4-26.

Jerry Honeycutt: Introducing Microsoft Windows Server 2003, Microsoft Press, Chapter 6.

QUESTION 12

You need to design a solution to address the concern of the Chief Security officer regarding the installation of unauthorized software on domain computers.

What should you do? (Each correct answer presents a complete solution. Choose TWO.)

- A. Disable the Disable Windows Installer policy in the Default Domain GPO.
- B. Enable the Disable Windows Installer policy and select the For non-managed apps only setting in the Default Domain GPO.
- C. Enable the Disable Windows Installer policy and select the Never setting in the Default Domain GPO.
- D. Enable the Disable Windows Installer policy and select the Always setting in the Default Domain GPO.
- E. Configure software restriction policy at domain level by creating the appropriate rules.

Answer: B, E

Explanation: Enabling the Disable Windows Installer policy and selecting the For non-managed apps only setting in the Default Domain GPO will ensure that only administrator approved applications will be installed.

You can also control the software deployment by means of configuring a software restriction policy at domain level.

1. No unauthorized software must be installed on any of the computers on the Stanford Finance network.
2. We must also ensure that our users do not install unauthorized software on the company client computers."

Incorrect answers:

A: If you disable the Disable Windows Installer policy because it will allow any application to be installed.

C: Selecting the Never setting on the Disable Windows Installer policy on the Default Domain GPO will prevent the installation of any applications, but will also prevent the administrator-approved applications from being installed.

D: Selecting the Always setting on the Disable Windows Installer policy on the Default

Domain GPO will prevent the installation of any applications, but will also prevent the administrator-approved applications from being installed.

QUESTION 13

You must create the physical design for the Stanford Finance Active Directory and Network Infrastructure. You need to decide on a method to use for installing Microsoft Windows Server 2003 on the domain controllers.

What should you do?

- A. Use Sysprep to install Windows Server 2003 on the domain controllers.
- B. Use an answer file to install Windows Server 2003 on the domain controllers.
- C. Use Systems Management Server (SMS) to install Windows Server 2003 on the domain controllers.
- D. Use Remote Installation Services (RIS) to install Windows Server 2003 on the domain controllers.

Answer: B

Explanation: You can use it to perform an automated or unattended installation. In this scenario you are to perform a fresh installation of domain controllers on new computers. An answer file allows one to specify the responses that an administrator is required to provide during an installation. It is not necessary to perform an in-place upgrade.

1. The current network is based on Active Directory and is operative in a Microsoft Windows 2000 environment. Unfortunately the network was set up as an interim measure and as such has not been properly designed to provide support the business operations. To this end the network has to be redesigned.
2. The entire network must be redesigned.
3. The redesign of our network is a great opportunity to make a clean start.

Incorrect answers:

A: Sysprep allows one to transform an existing installation of an operating system and applications on a sample computer into a form that can be cloned by using disk-imaging. Sysprep should not be used to clone domain controllers.

C: SMS is a server application that allows one to automate the maintenance of hardware and software inventory and the deployment of software on a large network. SMS relies on sophisticated infrastructure which has not yet been implemented on the existing network. There is no mention made of such an infrastructure on the new Stanford Finance network. Therefore you should not implement SMS. Besides, SMS can only be used to perform operating system upgrades, not clean installations of operating systems as will be the case here.

D: RIS is almost similar to Sysprep and should not be used in this scenario.

Reference:

Walter Glenn, and Michael T. Simpson, MCSE 70-297 Training Kit - Designing a Windows server 2003 Active Directory and Network Infrastructure, Chapter 3, pp. 3-4 to 3-7.

Microsoft Windows Server 2003 Installation Kit: Automating and Customizing Installations - choosing an automated installation method.

Topic 2, Willow Bridge, Inc., Scenario

Background

Willow Bridge, Inc. is a company that specializes in the provision of investment and financial services for its clients. Willow Bridge, Inc. operates across the United States of America.

Physical Locations

The Willow Bridge, Inc. head quarters are located in New York and its regional offices are located in Los Angeles and Chicago.

Each office has in excess of 100 privately-owned agencies. These agencies are contracted by Willow Bridge, Inc. to service customers in their respective local areas.

Office Type	Location	Users
Head Quarters	New York	2,300
Regional office	Los Angeles	700
Regional office	Chicago	800
Agencies	Across USA	5 – 90 per agency

Planned Changes

1. As part of its initiative to streamline the IT environment and increase network security, the company has decided to implement a Windows Server 2003 Active Directory environment.
2. The Research and Development Department will create a new Web Based application. The Web-based application will serve to extend the services that Willow Bridge, Inc. offers its customers over the Internet. Customers will have the ability to purchase policies on-line.
3. The Web server that will be designated to host this new application must provide an interface to a background SQL Server database.
4. The anticipated growth in customer numbers for the next five years is estimated at 5 million.
5. Custom classes will be used to store customer's personal information in Active Directory.
6. The SQL Server database will only store information about the policies that have been sold.

Business Processes

Only authorized sales personnel sell the policies to customers.

The sale process is as follows:

1. Customers come to the Willow Bridge, Inc. offices.
2. Sales staff members use their workstations to register the policies they sold.

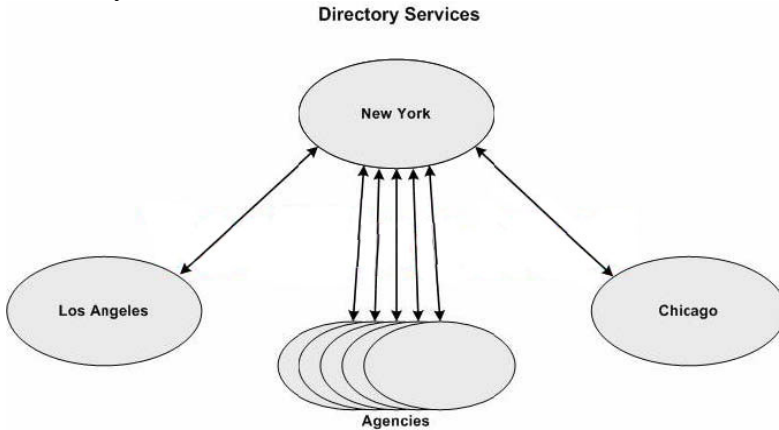
Alternatively

1. Sales staff members visit the customers and sell policies at customer locations.
2. Sales staff members use laptop workstations to remotely register their transactions.
3. They make use of either dial-up connections or directly from customer locations, or over VPN connections from their homes.

All customer information and policy transactions are stored in a database at the New York office. The database holds approximately 1 million records at present.

Existing network:

Currently each location is configured as a Windows NT 4.0 domain as illustrated in the Directory Services exhibit below:



There is a two-way trust between the New York domain and all the other domains. Every office is equipped with its own Internet access. Each office also has one or more remote dial-in and VPN servers. The large agencies are also equipped with a VPN server, a remote dial-in server and Internet connectivity.

There are no third party operating systems on the network. All servers on the Willow Bridge, Inc. network run Windows NT Server 4.0. The Willow Bridge, Inc. client computers run various Microsoft Windows operating systems.

The Sales department users have been issued laptop computers to connect to the Willow Bridge, Inc. network by dialing in to their respective offices. These connections are usually effected from either the customer location or from their homes via VPN connection over the Internet.

Problem Statements

Chief Executive Officer

"It has come to my attention that the government legislation that governs all companies dictates that we all comply with the new anti-discriminatory laws. We need to show our commitment and employ a handicapped person in an anti-handicapped job. I have given some thought to this issue and decided that we will not discriminate against people with poor eyesight in our company. We will employ someone who, according to the government qualifies for handicap status and employ that person in one of our departments."

Chief Information Officer

"We have a Research and Development Department whose responsibility it is to create custom software. This software will be used to conduct our business. The Research and Development Department will create a new Web Based application. The Web-based application will serve to extend the services that Willow Bridge, Inc. offers its customers over the Internet. Customers will have the ability to purchase policies on-line. To this end the Research and Development Department will have to be placed on a separate network. Something akin to a test network as we do not want them to interfere with the production environment. A test network will be the ideal situation where the Research and Development Department users can perform tests. It will after all be up to them to perform and test Active Directory schema modifications. This will be a necessity since we are going to save customer data in Active Directory. New government legislation that

governs our line of business also dictates that only the Willow Bridge, Inc. personnel that deal directly in servicing the customers, i.e. services and processing customer data, should have access to the customers' personal information."

Information Technology Manager

"Any Willow Bridge, Inc. office, whether it be a corporate office or agency, that has in excess of 60 employees has IT personnel on the staff. To this end we will only place domain controllers and servers in the offices that have IT staff on the premises. For control purposes I want the IT staff to report to me since I am ultimately the responsible person whose duty it is to manage the new network."

"My greatest concern is the Research and Development Department. It is their responsibility to create a Web-based application that will serve to extend the services that Willow Bridge, Inc. offers its customers over the Internet. They need to test the custom software that they create, but they always want to run their tests on the production servers. This causes many disruptions for all the other Willow Bridge, Inc. employees. They need an isolated test environment. We do not want any interference from them on the production network. We will take responsibility for the deployment of the new programs that they have developed after they have tested it in the test environment. We will deploy the new programs on the production servers ourselves."

Research and Development manager

"We are currently developing a new Web-based application as well as other custom programs that are necessary for the maintenance of business information. We have a problem in that we always end up disrupting existing services since it is of the utmost importance that we test Active Directory Schema, SQL Server databases, access permissions, as well as group policies. All these activities form an integral part of our work. However, this leads to a very unstable, experimental environment. We need a test environment that mimics the production environment to conduct our tests and make it valid. We agree full-hearted with the Willow Bridge, Inc. management who want to isolate the production environment from our tests. We have our own personnel that will maintain our test environment. Our personnel does not form part of the Willow Bridge, Inc. IT department. They are Research and Development department members. Therefore we will not interfere with the production network. All we want then is that the Willow Bridge, Inc. IT department does not interfere with our work."

Sales Department - End User

"We want to be able to access the internal network from our home computers."

Active Directory Requirements

The following Active Directory requirements must be considered:

1. The network administrators in the IT department and Research and Development department will retain their current responsibilities. There should be no overlap or interference between their administrative authority.
2. Each office must continue to use their own Internet access providers.
3. Their ISPs must be separate from the one used by the New York office.
4. All Willow Bridge, Inc. computers are to be registered with DNS.
5. All Willow Bridge, Inc. servers are to be configured with static IP addresses.
- 6.

All Willow Bridge, Inc. client computers are to be configured to receive their addresses via DHCP

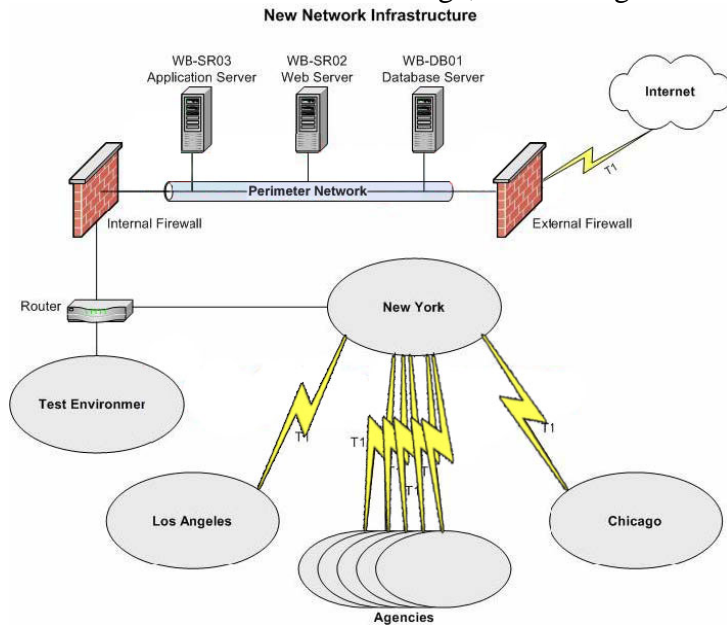
Security requirements

The following Security requirements must be considered:

1. Group Policy is to be used to configure the Web-server named WB-SR01; and the SQL server named WB-DB01.
2. Security requirements for WB-SR01 differ from the WB-DB01 security requirements.
3. The internal DNS namespace should not be exposed to the Internet.
4. All DNS information regarding the internal network is to be stored in Active Directory.
5. Only authorized users and computers should have the ability to modify DNS resource records.
6. The Sales department members using laptop workstations must log on to Active Directory only by making use of smart cards. They will not be able to establish a remote access dial-in or VPN connection to the Willow Bridge, Inc. network if they do not use the smart card authentication.

Envisaged Network Infrastructure

The New Network Infrastructure exhibit illustrates the relevant portion of the network infrastructure that the Willow Bridge, Inc. Management wants implemented.



Topic 2, Willow Bridge, Inc. (13 Questions)

QUESTION 14

You are designing a forest and domain structure to address the concerns of the Information Technology manager, and to meet the business and technical requirements. You want to use the minimum number of domains and forests that are required.

What should you do?

- A. Use a one forest structure.
- B. Use a two forest structure.
- C. Use a three forest structure.

D. Use a four forest main structure.

Answer: B

Explanation: This question addresses a concept Microsoft has recently adopted for Windows 2003: isolation vs. autonomy: One for the production network and one for the Research and Development department.

1. We need a test environment that mimics the production environment to conduct our tests and make it valid. We agree full-hearted with the Willow Bridge, Inc. management who wants to isolate the production environment from our tests.

2. We have our own personnel that will maintain our test environment. Our personnel does not form part of the Willow Bridge, Inc. IT department. They are Research and Development department members.

The scope of an Active Directory schema is a forest. To enable the research and development department to modify schema independently of the production network, you should implement a separate forest. By creating the two new forests, you are providing isolation. This satisfies the requirements.

Incorrect Answers:

A: To provide autonomy or isolation to a unit within a company, you need multiple forests. One would be too little in this scenario.

C, D: This would be excessive and will lead to unnecessary complications in the Active Directory structure.

Reference:

Walter Glenn, and Michael T. Simpson; MCSE 70-297 Training Kit - Designing a Windows server 2003 Active Directory and Network Infrastructure, Chapter 3, pp. 3-2 to 3-15.

Microsoft Windows Server 2003 Deployment Kit - Designing and Deploying Directory and Security Services, Creating a forest design

QUESTION 15

You are designing an IP addressing strategy for the Willow Bridge, Inc. network.

You need to take a decision as to which subnet mask you will use in the New York office.

What should you do?

A. You should use 255.248.0.0 on the New York office.

B. You should use 255.255.252.0 on the New York office.

C. You should use 255.255.248.0 on the New York office.

D. You should use 255.255.255.128 on the New York office.

E. You should use 255.255.240.0 on the New York office.

F. You should use 255.255.192.0 on the New York office.

G. You should use 255.255.128.0 on the New York office.

Answer: E

Explanation: A subnet mask is the leftmost bits in an IP address that are used for

network identification. The remaining rightmost bits of an IP address are used for identification of hosts on the network. To be able to determine the correct subnet mask for a network, you need to take into account the number of network devices on the network. Since there are 2,300 users in the New York office, you should provide for 2,300 IP addresses, therefore you should use the 20 bit mask 255.255.240.0 subnet mask. Under this mask, 12 bits are reserves for host IDs, which allows for 4,094 host IDs, which would be sufficient in this scenario for the New York office.

Incorrect answers:

A: This 255.248.0.0 subnet mask would be excessive as it allows for over a half million host IDs.

B: This subnet mask would work for the Los Angeles office or even the Chicago office, under the 255.255.252.0 subnet mask, 10 bits are reserved for host IDs, which allows for 1,022 host IDs. This would be ideal for the Los Angeles or Chicago offices.

C: 255.255.248.0 allows for 2,046 Host IDs. This is excessive for the branch offices but insufficient for the New York office.

D: 255.255.255.128 allows for 126 host IDs because only 7 bits under this mask is reserved for host IDs which would be ideal for any of the agencies.

F: 255.255.192.0 allows for over 16,000 host IDs which is way too excessive for any of the Willow Bridge, Inc. offices or agencies.

G: 255.255.128.0 allows for 32,000 host IDs which is way too excessive for any of the Willow Bridge, Inc. offices or agencies,

Reference:

Microsoft Windows Server 2003 Deployment Kit: Deploying network services - designing a TCP/IP Network.

QUESTION 16

You are designing an IP addressing strategy for the Willow Bridge, Inc. network. You need to take a decision as to which subnet mask you will use in the agencies. What should you do?

- A. You should use 255.248.0.0 on the agencies.
- B. You should use 255.255.252.0 on the agencies.
- C. You should use 255.255.248.0 on the agencies.
- D. You should use 255.255.255.128 on the agencies.
- E. You should use 255.255.240.0 on the agencies.
- F. You should use 255.255.192.0 on the agencies.
- G. You should use 255.255.128.0 on the agencies.

Answer: D

Explanation: A subnet mask is the leftmost bits in an IP address that are used for network identification. The remaining rightmost bits of an IP address are used for identification of hosts on the network. To be able to determine the correct subnet mask for a network, you need to take into account the number of network devices on the network. Since there are between 5 - 90 users in the agencies, you should provide for between 5 - 90 IP addresses, therefore you should use the 7 bit mask 255.255.255.128

subnet mask. Under this mask, 7bits are reserves for host IDs, which allows for 126 host IDs, which would be sufficient in this scenario for any of the agencies.

Incorrect answers:

A: This 255.248.0.0 subnet mask would be excessive as it allows for over a half million host IDs.

B: This subnet mask would work for the Los Angeles office or even the Chicago office, under the 255.255.252.0 subnet mask, 10 bits are reserved for host IDs, which allows for 1,022 host IDs. This would be ideal for the Los Angeles or Chicago offices.

C: 255.255.248.0 allows for 2,046 Host IDs. This is excessive for the branch offices but insufficient for the New York office.

E: Under the 255.255.240.0 subnet mask, 12 bits are reserves for host IDs, which allows for 4,094 host IDs, which would be sufficient for the New York office.

F: 255.255.192.0 allows for over 16,000 host IDs which is way too excessive for any of the Willow Bridge, Inc. offices or agencies.

G: 255.255.128.0 allows for 32,000 host IDs which is way too excessive for any of the Willow Bridge, Inc. offices or agencies,

Reference:

Microsoft Windows Server 2003 Deployment Kit: Deploying network services - designing a TCP/IP Network.

QUESTION 17

You are designing an Active Directory implementation strategy to meet the requirements for the new envisaged Willow Bridge, Inc. Active Directory Structure.

You need to decide on the appropriate implementation strategy.

What should you do? (Each correct answer presents part of the solution. Choose TWO.)

- A. Create one site for each agency.
- B. Create one site for the New York office and the agencies that have less than 60 users.
- C. Create one site for all agencies affiliated to Willow Bridge, Inc.
- D. Create one site for the Los Angeles and Chicago offices and the agencies that has 60 + users.
- E. Create one site for each Willow Bridge, Inc. office
- F. Create one site for the entire network.

Answer: B, D

Explanation

: Sites are logical units that represent the physical network topology. Therefore you can think of a site as a portion of the network in which all the computers are well connected, or even a portion of the network that is implemented as a single LAN. On the new envisaged network, domain controllers will be located in the agencies that have 60+ users. Therefore you should implement a site for the Los Angeles and Chicago offices and the agencies that has 60 + users and another site for the New York office and the agencies that have less than 60 users.

1. Every office is equipped with its own Internet access.
2. Each office also has one or more remote dial-in and VPN servers.

3. While the large agencies are also equipped with a VPN server, a remote dial-in server and Internet connectivity.

Incorrect Answers:

A: This will not work since the agencies are either equipped with a server and domain controller or not depending on its user numbers.

C: This will not work since not all agencies will be equipped with servers and domain controllers.

E: This would be partly correct, however it would not take into account the agencies and the number of users per agency since there is a matter of servers and a domain controller that will be placed in agencies that has 60+ users.

F: If you create a single site to represent the entire network, you will have a situation where replication is not performed efficiently. Intra-site replication is optimized for speed and inter-site replication is optimized for bandwidth usage. You will find yourself in a situation where replication either fails or consumes too much bandwidth.

Reference:

Jerry Honeycutt; Introducing Microsoft Windows Server 2003, Microsoft Press, Chapter 16

Microsoft Windows Server 2003 Deployment Kit - Designing and Deploying Directory and Security Services, Designing the Site topology

QUESTION 18

You are designing an IP addressing strategy for the Willow Bridge, Inc. network.

You need to take a decision as to which subnet mask you will use in the Los Angeles office.

What should you do?

- A. You should use 255.248.0.0 on the Los Angeles office.
- B. You should use 255.255.252.0 on the Los Angeles office.
- C. You should use 255.255.248.0 on the Los Angeles office.
- D. You should use 255.255.255.128 on the Los Angeles office.
- E. You should use 255.255.240.0 on the Los Angeles office.
- F. You should use 255.255.192.0 on the Los Angeles office.
- G. You should use 255.255.128.0 on the Los Angeles office.

Answer: B

Explanation: A subnet mask is the leftmost bits in an IP address that are used for network identification. The remaining rightmost bits of an IP address are used for identification of hosts on the network. To be able to determine the correct subnet mask for a network, you need to take into account the number of network devices on the network. Since there are 700 users in the Los Angeles office, you should provide for 700 IP addresses, therefore you should use the 10 bit mask

This subnet mask would work for the Los Angeles office or even the Chicago office, under the 255.255.252.0 subnet mask, 10 bits are reserved for host IDs, which allows for 1,022 host IDs. This would be ideal for the Los Angeles or Chicago offices.

Incorrect answers:

A: This 255.248.0.0 subnet mask would be excessive as it allows for over a half million host IDs.

C: 255.255.248.0 allows for 2,046 Host IDs. This is excessive for the branch offices but insufficient for the New York office.

D: 255.255.255.128 allows for 126 host IDs because only 7 bits under this mask is reserved for host IDs which would be ideal for any of the agencies.

E: Under the 255.255.240.0 subnet mask, 12 bits are reserved for host IDs, which allows for 4,094 host IDs, which would be sufficient for the New York office, not the Los Angeles office.

F: 255.255.192.0 allows for over 16,000 host IDs which is way too excessive for any of the Willow Bridge, Inc. offices or agencies.

G: 255.255.128.0 allows for 32,000 host IDs which is way too excessive for any of the Willow Bridge, Inc. offices or agencies,

Reference:

Microsoft Windows Server 2003 Deployment Kit: Deploying network services - designing a TCP/IP Network.

Jerry Honeycutt; Introducing Microsoft Windows Server 2003, Microsoft Press, Chapter 16

QUESTION 19

You are creating the Logical design for the Network Services Infrastructure for the new Willow Bridge, Inc. network. You need to decide on a DNS strategy to implement.

What should you do?

- A. Configure a WINS referral zone on the Willow Bridge, Inc. DNS servers.
- B. Configure DHCP servers to register legacy client computers with DNS.
- C. Create WINS resource record on the Willow Bridge, Inc. DNS servers.
- D. Create WINS-R resource records on the Willow Bridge, Inc. DNS servers.

Answer: B

Explanation: You should configure the DHCP servers to register legacy client computers with DNS.

1. All Willow Bridge, Inc. computers are to be registered with DNS.
2. All Willow Bridge, Inc. servers are to be configured with static IP addresses.
3. All Willow Bridge, Inc. client computers are to be configured to receive their addresses via DHCP
4. The Research and Development Department will create a new Web Based application.

Incorrect Answers:

A: A WINS referral zone is a special DNS zone that can be implemented to provide referrals to WINS servers for name resolution purposes of hosts that are not registered with DNS.

C: WINS resource records enable DNS servers to resolve the DNS names of hosts that are not registered with DNS but are registered with DNS.

D: WINS-R resource records enable DNS servers to perform IP address to DNS name

resolution of the hosts that are registered with WINS but not registered in DNS reverse lookup zones.

Reference:

Walter Glenn, and Michael T. Simpson; MCSE 70-297 Training Kit - Designing a Windows server 2003 Active Directory and Network Infrastructure, Chapter 6, pp. 6-15.
Martin Grasdahl, Laura E. Hunter, and Michael Cross; Planning and Maintaining a Windows Server 2003 Network Infrastructure: Exam 70-293 Study Guide & DVD Training System, Syngress, Chapter 6, p. 469
Microsoft Windows Server 2003 Deployment Kit -Deploying Network Services, Deploying DNS

QUESTION 20

You are designing a strategy to upgrade the DHCP servers after the new Active Directory structure is in place.

Who can authorize the DHCP servers?

- A. Chief information officer in the New York office.
- B. IT manager in the New York office.
- C. IT staff in the Willow Bridge, Inc. offices.
- D. Network administrator in New York

Answer: B

Explanation: "Any Willow Bridge, Inc. office, whether it be a corporate office or agency, that has in excess of 60 employees has IT personnel on the staff. To this end we will only place domain controllers and servers in the offices that have IT staff on the premises. For control purposes I want the IT staff to report to me since I am ultimately the responsible person whose duty it is to manage the new network."

Reference:

Walter Glenn, and Michael T. Simpson; MCSE 70-297 Training Kit - Designing a Windows server 2003 Active Directory and Network Infrastructure, Chapter 6, pp. 6-15.
Martin Grasdahl, Laura E. Hunter, and Michael Cross; Planning and Maintaining a Windows Server 2003 Network Infrastructure: Exam 70-293 Study Guide & DVD Training System, Syngress, Chapter 6, p. 469
Microsoft Windows Server 2003 Deployment Kit -Deploying Network Services, Deploying DNS

QUESTION 21

You need to create the physical design for the Willow Bridge, Inc. Active Directory and network Infrastructure. To this end you will design the connectivity and need to make a decision as to which method should be used to provide Internet access to the users in the New York office.

What should you do?

- A. Set up a VPN server in the New York office.
- B. Implement an ISA array.

- C. Configure the firewalls to allow VPN traffic
- D. Register willowbridge.com with the Internet Authorities and configure DNS to host the willowbridge.com zone.

Answer: B

Explanation: Internet Security and Acceleration (ISA) Server can be used to provide Internet access to a private network. An array of ISA servers provides fault tolerance and load balancing.

1. Each office must continue to use their own Internet access providers.
2. Their ISPs must be separate from the one used by the New York office.

Incorrect answers:

A: VPN is used to allow secure communications over public networks. Setting up a VPN server on the New York office will enable remote users to securely access the Willow Bridge, Inc. network. The instruction is to provide Internet access to the New York office users.

C: Configuring firewalls to allow VPN traffic is all good and well if you want to allow remote users to connect to the New York office securely. However this is not providing Internet access to the New York office users.

D: Registering willowbridge.com with the Internet Authorities and configure DNS to host the willowbridge.com zone are not directly related to providing Internet access for the New York office users.

Reference:

Martin Grasdahl, Laura E. Hunter, and Michael Cross; Planning and Maintaining a Windows Server 2003 Network Infrastructure: Exam 70-293 Study Guide & DVD Training System, Syngress, Chapter 6, pp. 469

Microsoft Windows Server 2003 Deployment Kit -Deploying ISA Service, Background of ISA Server

QUESTION 22

You need to design the security for the Sales Department users who connect to the network remotely. To this end you need to take a decision as to which operating system they should use on their laptop workstations.

What should you do? (Choose all that apply.)

- A. Configure the laptop workstations with Microsoft Windows 9x.
- B. Configure the laptop workstations with Microsoft Windows NT 4.0 Workstation.
- C. Configure the laptop workstations with Microsoft Windows 2000 Professional.
- D. Configure the laptop workstations with Microsoft Windows XP Professional.

Answer: C, D

Explanation: Windows 2000 Professional and Windows XP Professional are both operating systems that will allow one to make use of smart card authentication in an Active Directory environment.

1. We want to be able to access the internal network from our home computers.

2. The Sales department members using laptop workstations must log on to Active Directory only by making use of smart cards. They will not be able to establish a remote access dial-in or VPN connection to the Willow Bridge, Inc. network if they do not use the smart card authentication.

Incorrect answer:

A: Though this operating system does support the use of smart cards and smart card readers, etc. it will not allow the user to log on to the domain in an Active Directory environment, because it does not support Group Policy.

B: Though this operating system does support the use of smart cards and smart card readers, etc. it will not allow the user to log on to the domain in an Active Directory environment, because it does not support Group Policy.

Reference:

Walter Glenn, and Michael T. Simpson; MCSE 70-297 Training Kit - Designing a Windows server 2003 Active Directory and Network Infrastructure, Chapter 6, pp. 6-15. Microsoft Windows Server 2003 Deployment Kit - Designing and Deploying Directory and Security Services, planning a smart card deployment.

QUESTION 23

You need to design the DNS service implementation for the Willow Bridge, Inc. network. To this end you must make a decision as to what action to take in order to ensure that DNS name resolution traffic in the New York follows the shortest path. What should you do? (Each correct answer forms part of the solution. Choose THREE.)

- A. Configure the DNS servers on the test network to forward queries for names of hosts on the production network to the DNS servers in the production network.
- B. Configure the DNS servers on the production and test networks to forward queries for names of hosts on the Internet to the DNS server in the peripheral network.
- C. Configure the DNS servers on the production network to forward queries for names of hosts on the test network to a DNS server on the test network.
- D. Configure a delegation to the zone on the test network on the DNS server on the peripheral network.
- E. Request the New York office ISP to configure a delegation on its DNS server to the zone on the test network.
- F. Configure a private root zone on a test network DNS server.

Answer: A, B, C

Explanation: Since you will need to implement two forests in this design you must ensure that the computers on the production network can resolve Internet names and names on the test network and those names on the production network can resolve Internet names on the production network. When a computer submits a name query to its configured DNS server, the most direct path for the subsequent name resolution traffic is to a DNS server that is authoritative for the domain where the target host belongs. This is because the authoritative server can resolve the query without communicating with other DNS servers. Therefore if you consolidate the cached data on the DNS server that can be

used by both internal networks, you minimize the need for recursion.

Incorrect answers:

D: A delegation points to a DNS server that is authoritative for a child zone. This is not what is required.

E: A name server (NS) record is a delegation that points to an authoritative DNS server to provide referrals to that server. This is not what is required in this scenario.

F: Using a private root zone on a single-domain network on which a substantial portion of queries is expected, you unnecessarily complicate name resolution traffic paths.

Reference:

Jerry Honeycutt; Introducing Microsoft Windows Server 2003, Microsoft Press, Chapter 16

Microsoft Windows Server 2003 Online Help - Understanding DNS - DNS domain names, How DNS query works.

QUESTION 24

You must design the Willow Bridge, Inc. Active Directory Infrastructure. To this end you need to apply the appropriate security configurations to WB-SR01 and WB-DB01. You now need to make a decision on which method you will use to achieve this goal.
What should you do?

A. Configure the appropriate security settings for WB-SR01 and WB-DB01 in two separate Group Policy Objects (GPOs) and link each GPO to a separate OU. Then place WB-SR01 and WB-DB01 in the appropriate OUs.

B. Specify the appropriate security settings in the local security policy of WB-SR01 and WB-DB01 respectively.

Configure two GPOs and link each GPO to the appropriate OU and then place WB-SR01 and WB-DB01 in the appropriate OUs.

C. Change the Default Domain Policy GPO to include all the required security settings for both WB-SR01 and WB-DB01.

Use permissions to filter the scope of the GPO to apply the appropriate settings to WB-SR01 and WB-DB01.

D. Create a GPO that includes all the required security settings for both WB-SR01 and WB-DB01 and link the GPO to the domain.

Filter the scope of the GPO to apply the appropriate settings to WB-SR01 and WB-DB01 by means of a WMI filter.

Answer: A

Explanation: You need to configure two GPOs, link it to separate OUs and then place WB-SR01 and WB-DB01 into the appropriate OU.

1. Group Policy is to be used to configure the Web-server named WB-SR01; and the SQL server named WB-DB01.

2. Security requirements for WB-SR01 differ from the WB-DB01 security requirements.

Incorrect answers:

B: You should first create the GPO then link it to the appropriate OU.

C: The default Domain Policy GPO is created automatically when a domain is created. Any settings to this GPO will override local security policies on any domain member computers.

D: Though it is possible to make use of WMI filters to filter the default scope of a GPO to affect the GPO to apply only to a subset of computers that would be targeted with the GPO, but you cannot combine different security settings for both WB-SR01 and WB-DB01 in the same GPO and apply only the appropriate settings to each computer respectively.

Reference:

Walter Glenn, and Michael T. Simpson; MCSE 70-297 Training Kit - Designing a Windows server 2003 Active Directory and Network Infrastructure, Chapter 4, pp. 4-27 to 4-28.

Microsoft Windows Server 2003 Deployment Kit - Designing a managed Environment: Designing Group Policy Infrastructure

QUESTION 25

You are a consultant. You have been commissioned by the Willow Bridge, Inc. CEO to design a job description to address the issues that the Chief Executive officer has brought to everyone's attention.
What should you do?

- A. Create a job for someone to execute on a Windows XP Professional workstation in the Research and development department.
- B. Create a job as a proof reader for the production development.
- C. Create a job as a proof reader for the Sales Department.
- D. Create a job for someone on the Legacy computers.

Answer: A

Explanation: In Windows XP the Accessibility Wizard configures a computer based on the user's vision, hearing, and mobility needs. Through the Accessibility Wizard, the user selects the text size that is the easiest to read. The wizard also collects input to determine whether the user has vision, hearing, or mobility challenges. The Magnifier utility creates a separate window to magnify a portion of your screen. This option is useful for users who have poor vision.

1. I have given some thought to this issue and decided that we will not discriminate against people with poor eyesight in our company.
2. We will employ someone who, according to the government qualifies for handicap status and employ that person in one of our departments."

Incorrect answers:

B: You need to be more precise in exactly what is to be proof read as this must be able to accommodate someone with poor eyesight.

C: This would not be wise as one would assume that this is the first handicapped person that Willow Bridge, Inc. would be employing and as such the situation would first have to be tested by the Research and Development department for feasibility and not the Sales department which forms part of the production network.

D: Some of the Legacy computers might not have the Accessibility features that will accommodate someone with poor eyesight.

Reference

Brian Barber, Chad Todd, Norris L. Johnson, Jr., Robert J. Shimonski, and Martin Grasdahl: Configuring and Troubleshooting Windows XP Professional, Syngress Publishers, Rockland M.A, 2001, p. 716

QUESTION 26

You need to design a DNS name resolution strategy. You must configure the DNS server on the peripheral network to meet the case study scenario.
What should you do?

- A. Configure a secondary zone for the Willow Bridge, Inc. internal network.
- B. Configure the peripheral DNS server to host the willowbridge.com zone with the A record for WB-SR01.
- C. Create a delegation to the zone on the Willow Bridge, Inc. internal network.
- D. Create a delegation to the zone on the Research and Development department test network.
- E. Specify the ISP's DNS server as a forwarder.

Answer: E

Explanation: WB-SR01 and WB-DB01 belong to the Willow Bridge, Inc. forest and, hence their names must be registered with DNS servers on the Willow Bridge, Inc. network. To enable customers to access WB-SR01, the ISP's DNS server can be configured to host the public willowbridge.com zone which include the appropriate A record for WB-SR01. The DNS server on the peripheral network should be configured to forward all queries to the ISP's DNS server and not use recursion.

1. Group Policy is to be used to configure the Web-server named WB-SR01; and the SQL server named WB-DB01.

Incorrect answers:

A: Configuring a secondary zone will result in increased resolution traffic across the external firewall.

B: You could configure the peripheral DNS server to host the willowbridge.com zone with the A record for WB-SR01, but this option does not take into account that the DNS server should not host any other zones and should not be able to resolve names on either of the Internal networks.

C: This would result in the DNS server on the peripheral network being able to resolve names on the internal network. This is therefore a security risk.

D: This will result in an unnecessary security risk because it will allow the DNS server to resolve names on the internal network.

Reference:

Microsoft Windows Server 2003 Online Help - Contents - Network Services, Concepts: Understanding DNS, Managing servers, creating Internal and External Domains.

Topic 3, IT Training Institute, Scenario

Background

IT Training Institute is a fairly new educational institution that specializes in providing information technology (IT) training to government employees and school teachers. The company has recently created a web site to provide educational material online for its registered students.

Physical Location

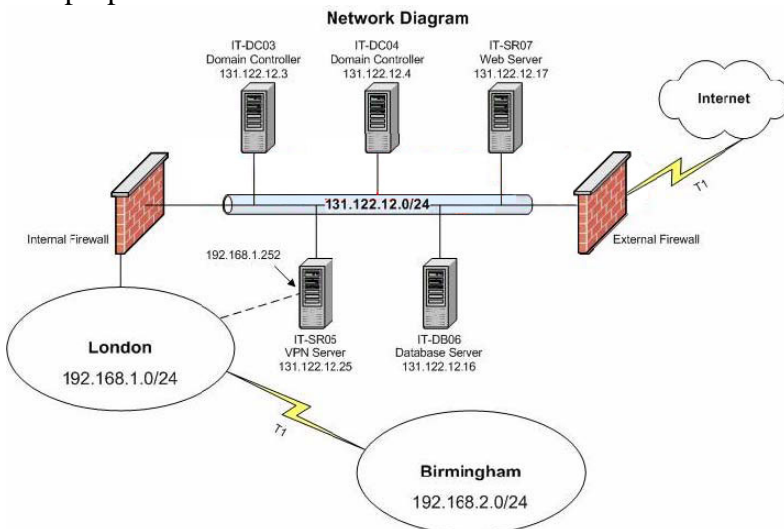
IT Training Institute has single office that supports 120 users. The office is located in London.

Planned Changes

IT Training Institute will open a branch office in Birmingham in the next two months. The Birmingham office will support 120 users when it opens. The company will also hire an additional 100 users for the London office. IT Training Institute anticipates a 60% growth in users over the next five years.

The company wants to create two distinct networks: an internal network and an external network. The two networks will be managed by two different groups of IT personnel and will be independent of each other.

The proposed network infrastructure is shown in the Network Diagram exhibit.



Business Processes

IT Training Institute students access online course material for the various courses offered by the company. The online course material has been prepared by IT consultants who have access to all online course material.

Infrastructure

Directory Services

When IT Training Institute was established, an unplanned Windows 2000 network was created. The network consists of a single Windows 2000 Active Directory native-mode domain with an internal DNS namespace of itti.com and the NetBIOS name of ITTI. When the public Web site was added, the company discovered that the domain name itti.com was already registered to a company in Florida, US

A. The company then registered the domain name ittraining.com for its Web site.

Network Infrastructure

The current IT Training Institute network contains two domain controllers named IT-DC01 and IT-DC02, and a single file server named IT-SR03. All servers on the IT Training network run Windows 2000 Server and all client computers run either Windows 2000 Professional or Windows XP Professional.

The company has a 10-Mbps Internet connection that is under utilized at present.

Problem Statements

Chief Executive Officer

"Last year we hurriedly put the network together but as the company has grown, network problems have emerged. I want the network to be completely redesigned as a Windows Server 2003 Active Directory environment. This means all our existing user accounts must be migrated from the current environment to Windows Server 2003. Network stability and scalability is crucial to the projected growth of the company. I'm prepared to make the necessary investment in network infrastructure to ensure stability and scalability."

Chief Information Officer

"We want to implement two distinct networks and we want separate IT staff to manage each network. Internal users must have access to the internal and external networks using a single set of credentials but external users must not be able to access internal resources."

"We have to keep the domain name ittraining.com for our external network. We don't want to use more domain names and we want keep our domains separate."

"We want to implement a domain based DFS system for the internal network. We will implement DFS servers in the new office as well. Users in each office should automatically be redirected to the DFS server in their current physical location. In the event of a single DFS server failure, users should be automatically redirected to an available DFS server."

External Network Administrator

"All external users who require access to resources must have a username and password and must submit requests using HTTPS."

"External users will only require access to a Web server named IT-SR07. IT-SR07 will provide a web interface to the external users and will retrieve resources from our other external servers."

"IT-SR07 will also host the interface for our public web site. Anonymous access will be provided for the public web site."

Internal Network Administrator

"Some of our employees need to access internal data while traveling. They will connect to the internal network through VPN access. A VPN server named IT-SR05 will be installed on the internal network for this purpose."

"We also need to ensure that internal users have access to resources in the existing domain during the migration process and we need to implement fault-tolerance for the internal network."

"Replication for our DFS servers must not interfere with normal business operations and should occur only after business hours."

"Over the next few months, many new users will be added to the network. We need to provide a consistent environment for these users; therefore, replication of internal user accounts between the London and Birmingham offices must occur within a maximum

time delay of one hour."

"We must also minimize the impact that name resolution of Internet based resources might have on WAN links. We need to identify a solution that will allow name resolution to occur without generating excessive and unnecessary traffic."

"One of the domain controllers at each office will be configured as a DNS server. Each office will also have a single DHCP server. All users accessing the internal network must receive their IP configurations from one of these DHCP servers."

Security Administrator

"We need to maintain the security of both the internal network and the external network. We should only allow traffic that is required by the company to pass through the internal firewall; all other traffic must be blocked."

"We also need to secure the internal and external DNS structures to prevent unauthorized systems from registering their names with DNS. DNS will be installed on a domain controller named IT-DC03 on the external network and will perform name resolution only for the namespace ittraining.com. It must not resolve any other name for external users, including names of other Internet based hosts."

Topic 3, IT Training Institute (15 Questions)

QUESTION 27

You need to identify the features that will be available immediately after you migrate the domain to Windows Server 2003.

Which feature or features will be available?

- A. Global group nesting.
- B. Domain local group nesting.
- C. Universal security groups.
- D. SID history attributes.
- E. All of the above.

Answer: E

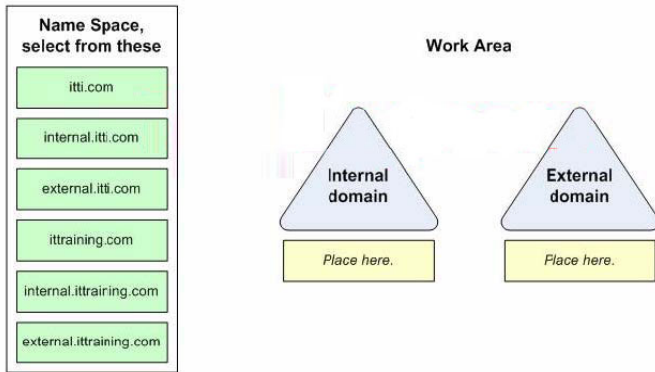
They all will be available.

QUESTION 28

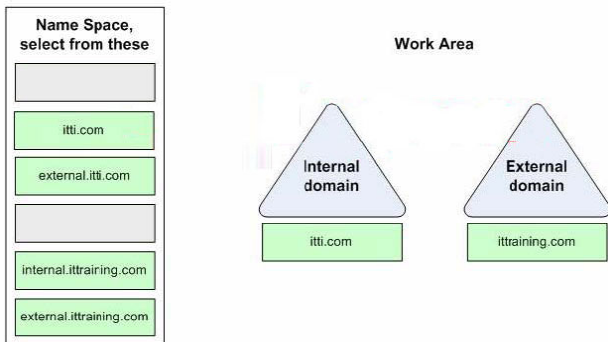
DRAG DROP

You need to design a naming strategy for the new internal and external domains. You need to identify the appropriate domain name for each domain. You need to ensure that your solution meets the business and technical requirements of IT Training Institute.

What should you do? (To answer, drag the appropriate name space to the correct location or locations in the work area.)



Answer:



Explanation: The Chief Information Officer indicates that: "We have to keep the domain name ittraining.com for our external network. We don't want to use more domain names and we want keep our domains separate."

Therefore, the domain name ittraining.com must be used for the external network as IT Training Institute will not be registering a new domain name. To keep the domain separate, a different domain name should be used for the internal network.

Reference:

http://www.microsoft.com/resources/documentation/WindowsServ/2003/all/deploy/guide/en-us/dssbc_logi_lcbx.asp

QUESTION 29

DRAG DROP

You need to design a strategy for the migration of the internal network to Windows Server 2003. Your solution must meet the business and technical requirements of IT Training Institute.

What should you do? (To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the appropriate order. Use only actions that apply.)

Steps, select from these

Create a Pristine forest.
Create a new child domain.
Change the domain functional level.
Migrate the User Accounts.
Migrate the Computer Accounts.
Establish an external trust relationship.

Steps, place here

Place first step here.
Place second step here, if any.
Place third step here, if any.
Place fourth step here, if any.
Place fifth step here, if any.
Place sixth step here, if any.

Answer:**Steps, select from these**

Create a new child domain.

Steps, place here

Create a Pristine forest.
Establish an external trust relationship.
Change the domain functional level.
Migrate the Computer Accounts.
Migrate the User Accounts.
Place sixth step here, if any.

Explanation: A migration is accomplished by creating a new pristine Active Directory on a new server. Then, you use a migration tool to copy the domain information from your old domain to your new one. Here are some of the advantages of this method:

1. Migration is gradual. You can migrate one department at a time.
2. Accounts are copied rather than moved, so you can return to the old domain if necessary.
3. You avoid the complexity of taking existing database bugs and moving them into your new Active Directory.
4. You can re-evaluate your existing domain structure and consolidate or expand your domains, as you deem necessary.

Reference:

Michael Cross, Jeffery

A. Martin, and Todd

A. Walls: MCSE: Planning, Implementing, and Maintaining a Windows Server 2003 Active Directory Infrastructure Study Guide & DVD Training System, Syngress, Chapter 7, pp. 501.

QUESTION 30

You need to design the site topology for IT Training Institute's internal domain. You need to ensure that your solution meets the company's business and technical requirements.

What should you do?

- A. Create a site for each physical location and configure the default IP site link to only allow replication between 9:00 P.M. and 3:00 A.M.
- B. Set the replication interval on the default IP site link to 60 Minutes and configure the default IP site link to only allow replication between 9:00 P.M. and 3:00 A.M.
- C. Create a site for each physical location and configure the default IP site link to only allow replication between 6:00 A.M. and 12:00 A.M.
- D. Set the replication interval on the default IP site link to 30 Minutes and configure the default IP site link to only allow replication between 6:00 A.M. and 12:00 A.M.

Answer: A

Explanation: The DFS object stores the DFS metadata for a domain-based namespace. The DFS object is created in Active Directory when you create a domain -based root, and Active Directory replicates the entire DFS object to all domain controllers in a domain.

Incorrect Answers:

B: DFS is replicated with Active Directory; therefore you cannot set the replication interval to every 60 minutes.

C: One of the goals in the case study says: "DFS replication must occur after hours." Therefore replication should not be allowed to occur up until 12:00 A.M. as this will be well into the business day.

D: DFS is replicated with Active Directory; therefore you cannot set the replication interval to every 30 minutes. Furthermore, replication should not be allowed to occur up until 12:00 A.M. as this will be well into the business day.

QUESTION 31

You need to design the DNS name resolution strategy for IT Training Institute's internal network. You need to ensure that your solution meets the business and technical requirements of IT Training Institute.

What should you do? (Each correct answer presents part of the solution. Choose two.)

- A. Configure default root hints on all DNS servers on the internal network.
- B. Disable recursion on the DNS server in Birmingham.
- C. Create a root zone on the DNS server in London.
- D. Configure the Birmingham DNS server to use the London DNS server as a forwarder.
- E. Create a root zone on the DNS server in Birmingham.

Answer: B, D

Explanation: When forwarders are configured this way in combination with disabling recursion, the local DNS server is known as a slave server because in these cases, it is completely dependent on the forwarder for queries that it cannot resolve locally.

Incorrect Answers:

A: You should disable root hints on the internal DNS servers to minimize name resolution traffic for external name resolution.

C, E: A root zone will not allow DNS to resolve names on the external network.

Reference:

J. C. Mackin, and Ian McLean: MCSA/MCSE self-paced training kit (exam 70-291): Implementing, managing, and maintaining a Microsoft Windows Server 2003 network infrastructure, Microsoft, Chapter 5, pp. 5-3 to 5-7.

QUESTION 32

You need to design a remote access strategy for IT Training Institute. You need to ensure that your solution meets the business and technical requirements of IT Training Institute.

What should you do?

- A. Allow inbound VPN traffic to pass through the external and internal firewalls.
- B. Allow inbound VPN traffic to pass through the external firewall only.
- C. Allow inbound VPN traffic to pass through the internal firewall only.
- D. Allow VPN traffic with a source IP address of 131.122.12.25 to pass through the internal firewall.
- E. Allow VPN traffic with a source IP address of 191.168.1.252 to pass through the external firewall.

Answer: B

Explanation: The case study states: "Planned VPN access will allow users access to internal data while traveling." It also states: "Users will be granted VPN access by connecting to IT-SR05." According to the planned network infrastructure exhibit, IT-SR05 is located inside the perimeter network, and outside the internal firewall. So, for the internal users to access IT-SR05 while traveling, VPN traffic has to be allowed through the external firewall only.

Incorrect Answers:

A, C: IT-SR05 is located inside the perimeter network. Traffic from the internet would need to pass through the external firewall and not the internal firewall to reach IT-SR05.

D: 131.122.12.25 is the VPN interface that is connected to the external network. This traffic should not be passed through the internal firewall.

E: 191.168.1.252 is the VPN interface that is connected to the internal network. This traffic should not be passed through the external firewall.

QUESTION 33

You need to design a domain name resolution strategy for IT Training Institute users in London. You need to ensure that your solution meets the business and technical requirements of IT Training Institute.

What should you do? (Each correct answer presents a complete solution. Choose THREE.)

- A. Create a root zone on the DNS server in London.
- B. Configure default root hints on the DNS server in London.
- C. Configure the DNS server in London to forward all request for the external namespace to IT-DC03.
- D. Configure recursion on the DNS server in London.
- E. Create a stub zone for the external namespace on the DNS server in London.

Answer: B, C, E

Explanation:

To perform recursion properly, the DNS server first needs to know where to begin searching for names in the DNS domain namespace. This information is provided in the form of root hints, a list of preliminary resource records used by the DNS service to locate servers authoritative for the root of the DNS domain namespace tree.

A common use of forwarding is to allow DNS clients and servers inside a firewall to resolve external names securely. When an internal DNS server or client communicates with external DNS servers by making iterative queries, normally the ports used for DNS communication with all external servers must be left open to the outside world through the firewall. However, by configuring a DNS server inside a firewall to forward external queries to a single DNS forwarder outside your firewall, and by then opening ports only to this one forwarder, you can resolve names without exposing your network to outside servers.

A stub zone is a copy of a zone that contains only the resource records needed to identify an authoritative DNS server. An authoritative DNS server is a server that hosts resource records for a particular DNS zone. Rather than a DNS server having to query the Internet to locate an authoritative DNS server, the DNS server can simply refer to the list of name servers (NS resource records) in the stub zone. Distributing a list of authoritative DNS servers for a zone can be implemented by using stub zones. Unlike secondary zones, which primarily are used for redundancy and load-balancing reasons, stub zones are used to improve name resolution performance.

Incorrect Answers:

A: A root zone will not allow DNS to resolve names on the external network.

D: You could enable recursion on the internal DNS server but a technical requirement is that you minimize DNS traffic.

Reference:

J. C. Mackin, and Ian McLean: MCSA/MCSE self-paced training kit (exam 70-291): Implementing, managing, and maintaining a Microsoft Windows Server 2003 network infrastructure, Microsoft, Chapter 4, pp. 4-19, and Chapter 5, pp. 5-6.

Walter Glenn, and Michael T. Simpson; MCSE 70-297 Training Kit - Designing a Windows server 2003 Active Directory and Network Infrastructure, Chapter 6, pp. 6-26.

QUESTION 34

You need to design the IP address assignment strategy for the remote users. You need to ensure that your solution meets the business and technical requirements of IT Training Institute.

What should you do?

- A. Configure IT-SR05 as a DHCP Relay Agent.
- B. Configure as static IP address pool in the range 192.168.0.0/24 on IT-SR05.
- C. Configure as static IP address pool in the range 131.122.12.0/24 on IT-SR05.
- D. Configure the internal firewall to allow DHCP broadcasts to be forwarded to the internal DNS server.

Answer: A

Explanation: DHCP Relay Agent is a routing protocol configured in Routing and Remote Access that allows DHCP clients to obtain an IP configuration from a DHCP server on a remote subnet.

Incorrect Answers:

B, C: The technical requirements state that IP addresses must be assigned by DHCP. Therefore you cannot use a static address pool to assign IP addresses.

D: DHCP broadcasts do not need to pass through the internal firewall as VPN traffic does not pass through the internal firewall.

Reference:

J. C. Mackin, and Ian McLean: MCSA/MCSE self-paced training kit (exam 70-291): Implementing, managing, and maintaining a Microsoft Windows Server 2003 network infrastructure, Microsoft, Chapter 9.

QUESTION 35

You need to ensure that users have continued access to network resources during the migration of the internal network to Windows Server 2003.

What should you do? (Choose all that apply.)

- A. Migrate the SIDHistory.
- B. Enable SID filtering.
- C. Create an external trust.
- D. Create Universal Distribution Groups.

Answer: A, C

Explanation:

You need to create an external trust in which the source domain trusts the target domain. Once user accounts are moved, you should also move the SIDHistory attributes to the target domain.

Incorrect Answers:

B: SID Filtering on external trusts is enabled by default.

D: You cannot use distribution groups to provide access to resources.

QUESTION 36

You need to design a firewall strategy for the internal network that meets the requirements of the Security Administrator.

What should you do?

- A. Allow inbound VPN traffic.
- B. Allow inbound DNS traffic.
- C. Allow inbound IPX traffic.
- D. Allow inbound HTTP and HTTPS traffic.
- E. Allow inbound traffic from the 192.168.1.0/24 network address.

Answer: D

Explanation:

Hypertext Transfer Protocol (HTTP) and Hypertext Transfer Protocol over SSL (HTTPS) are the methods by which Web pages are transferred over the network. Internal users will need to access web pages on the web server which is in the perimeter network. Therefore, inbound HTTP and HTTPS should be allowed.

Incorrect Answers:

A: The case study states: "Internal users will be granted VPN access by connecting to IT-SR05." According to the planned network infrastructure exhibit, IT-SR05 is located inside the external firewall and outside the internal firewall. So, for the internal users to access IT-SR05 while traveling, VPN traffic has to be allowed through the external firewall only.

B: The internal and external DNS structures to prevent unauthorized systems from registering their names with DNS. Also, the external DNS server should resolve names only for the external name space. Therefore inbound DNS traffic should not be allowed.

C: The network does not have Novel hosts and all client computers run either Windows 2000 Professional or Windows XP Professional. IPX is also not used on the Internet. Therefore IPX is not required.

E: The internal network address is 192.168.1.0/24. Any inbound traffic with that address would be masquerading as a legitimate host on the network.

Reference:

J. C. Mackin, and Ian McLean: MCSA/MCSE self-paced training kit (exam 70-291): Implementing, managing, and maintaining a Microsoft Windows Server 2003 network infrastructure, Microsoft, Glossary, pp. G-20.

Dan Holme, and Orin Thomas: MCSA/MCSE Self-Paced Training Kit (Exam 70-290): Managing and Maintaining a Microsoft Windows Server 2003 Environment, Microsoft, Glossary, pp. G-10.

QUESTION 37

You need to design a strategy to ensure that VPN users are able to access all internal resources. You need to ensure that your solution meets the business and technical requirements of IT Training Institute.

What should you do?

- A. Install and configure Internet Authentication Service (IAS) on IT-SR05.
- B. Create a static routing table entry on IT-SR05 that points to the London network.
- C. Create a static routing table entry on IT-SR05 that points to the Birmingham network.

D. Configure all VPN client computers with the default gateway address that points to the London network.

Answer: A

Explanation: Internet Authentication Service (IAS) is the Microsoft implementation of a Remote Authentication Dial-In User Service (RADIUS) server and proxy in Microsoft Windows Server 2003; Standard Edition, Windows Server 2003; Enterprise Edition, and Windows Server 2003; Datacenter Edition. As a RADIUS server, IAS performs centralized connection authentication, authorization, accounting, and auditing (AAA) for many types of network access, including wireless, authenticating switch, dial-up and virtual private network (VPN) remote access, and router-to-router connections. As a RADIUS proxy, IAS forwards authentication and accounting messages to other RADIUS servers. IAS supports the Internet Engineering Task Force (IETF) standards for RADIUS described in RFC 2865 and RFC 2866.

Incorrect Answers:

B, C, D: Since both London and Birmingham will be in the same domain and utilize the same DNS server there is nothing special that needs to be done to allow VPN users (once authenticated via IAS) access to all internal resources.

Reference:

<http://www.microsoft.com/resources/documentation/WindowsServ/2003/all/techref/en-us/Default.asp?url=/Reso>

QUESTION 38

You need to design a strategy to migrate user accounts to the Windows Server 2003 environment. You need to ensure that your solution meets the business and technical requirements of IT Training Institute.

What should you do? (Each correct answer presents part of the solution. Choose TWO.)

- A. Raise the domain functional level.
- B. Create an external trust relationship.
- C. Run adprep to prepare the source domain.
- D. Run adprep to prepare the target domain.

Answer: A, B

Explanation: The target domain must be running in either Windows 2000 Native or Windows Server 2003 functional level. This is required because SID History cannot be stored in a classic SAM, so all BDCs must be off the wire. In this case, we are migrating from Windows 2000 to Windows Server 2003.

The source domain must trust the target domain. This ensures that the ADMT agent has the proper security context.

Incorrect Answers:

C, D: adprep is used for in-place upgrades.

Reference:

William Boswell: Inside Windows Server 2003, Addison Wesley, Chapter 9.

QUESTION 39

You need to design a NetBIOS naming strategy for IT Training Institute's internal domain.

What should you do? (Each correct answer presents a complete solution. Choose TWO.)

- A. ad
- B. London
- C. internal
- D. external

Answer: A, C

Explanation: Internal and ad, for Active Directory, are appropriate NetBIOS domain names for an internal domain.

Incorrect Answers:

B: London would not correctly represent the internal name since it refers to a location rather than a domain.

D: The question says you are designing a NetBIOS naming strategy for the INTERNAL domain. So an internal domain name of external is very misleading.

QUESTION 40

You need to design a firewall strategy to support VPN clients. You need to ensure that your solution meets IT Training Institute's business and technical requirements.

What should you do?

- A. Allow VPN traffic destined for the 131.122.12.0/24 network to pass through the external firewall.
- B. Allow VPN traffic destined for the 192.168.1.0/24 network to pass through the internal firewall.
- C. Allow VPN traffic destined for the 131.122.12.0/24 network to pass through the internal firewall.
- D. Allow VPN traffic destined for the 192.168.1.0/24 network to pass through the external firewall.

Answer: A

Explanation: According to the planned network infrastructure exhibit, IT-SR05 is located inside the perimeter network, and outside the internal firewall. So, for the internal users to access IT-SR05 while traveling, VPN traffic has to be allowed through the external firewall only. The external IP address for IT-SR05 is 131.122.12.25 which is on the 131.122.12.0/24 network. Therefore, inbound VPN

traffic must be destined for this network and not the 192.168.1.0/24 network which is the internal network in London.

Incorrect Answers:

B, C: According to the planned network infrastructure exhibit, IT-SR05 is located inside the perimeter network, and outside the internal firewall. So, for the internal users to access IT-SR05 while traveling, VPN traffic has to be allowed through the external firewall only.

D: The external IP address for IT-SR05 is 131.122.12.25 which is on the 131.122.12.0/24 network. Therefore, inbound VPN traffic must be destined for this network and not the 192.168.1.0/24 network which is the internal network in London.

QUESTION 41

You need to design a domain name resolution strategy for the external network.

You need to ensure that your solution meets the business and technical requirements of IT Training Institute.

What should you do?

- A. Create a root zone on IT-DC03.
- B. Create a stub zone for the external namespace on IT-DC03.
- C. Configure default root hints on IT-DC03.
- D. Configure IT-DC03 to use the ISP's DNS server as a forwarder.

Answer: A

Explanation: IT-DC03 needs to resolve names only for the external name space.

Therefore you need to configure a private root zone for the external name space.

Incorrect Answers:

B: There is only one DNS server on the external network. Therefore a stub zone is not required. A stub zone is a copy of a zone that contains only the resource records needed to identify an authoritative DNS server.

C: You should disable root hints on the external DNS server as it must not provide name resolution for the internal names space or for Internet hosts.

D: You need to prevent IT-DC03 from resolving names of Internet-based hosts.

Therefore you should not allow IT-DC03 to forward requests.

Reference:

J. C. Mackin, and Ian McLean: MCSA/MCSE self-paced training kit (exam 70-291): Implementing, managing, and maintaining a Microsoft Windows Server 2003 network infrastructure, Microsoft, Chapter 4, pp. 4-19, and Chapter 5, pp. 5-6.
Walter Glenn, and Michael T. Simpson; MCSE 70-297 Training Kit - Designing a Windows server 2003 Active Directory and Network Infrastructure, Chapter 6, pp. 6-26.

Topic 4, Mondo Transport, Ltd., Scenario

Background

Mondo Transport, Ltd. provides long-distance transportation in Europe, including long-distance public transportation and long distance hauling.

Physical Locations

Mondo Transport, Ltd. has its headquarters in Moscow and branch offices in Minsk, Kiev and Volgograd.

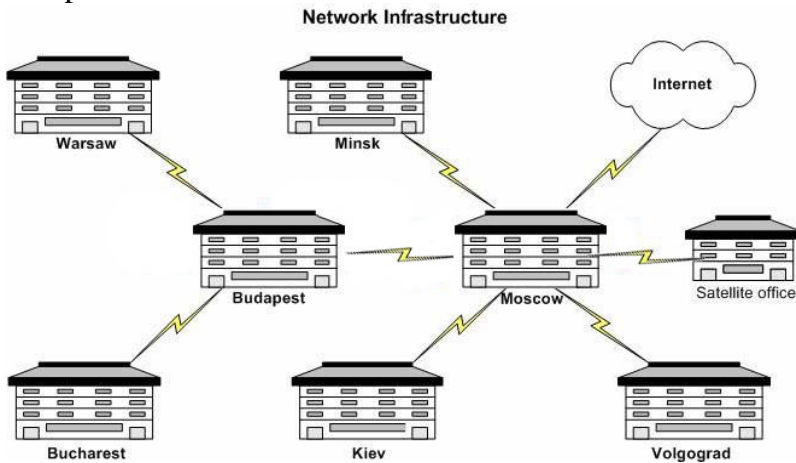
Headquarters also has a satellite office at the Moscow interchange. The satellite office is connected to headquarters by a fiber-optic link.

Planned changes

Mondo Transport, Ltd. intends opening three East European branch offices in Warsaw, Budapest and Bucharest

The Budapest branch office will serve as the regional office for Eastern Europe and a separate group of administrators will manage the new offices from Budapest.

The planned network infrastructure is shown in the Network Infrastructure exhibit.



Mondo Transport, Ltd. uses an X.500 directory-enabled application named MT_Dispatch. The current version of the MT_Dispatch application runs on a Windows NT Server 4.0 application server named MT-SR07. MT-SR07 is located in the Moscow office. Mondo Transport, Ltd. will enter into partnership with a company named Bilco, Ltd. Bilco, Ltd. will host a new version of the MT_Dispatch application on a Windows Server 2003 computer on their network.

The MT_Dispatch application will use the inetOrgPerson class when authenticating to the X.500 directory-enabled database that the application uses for authentication.

Mondo Transport, Ltd. users connect to the MT_Dispatch application by querying DNS for the application's service record. This record is stored on a UNIX DNS server running the latest version of BIND.

A VPN solution will be implemented to allow remote access to the corporate network. A Routing and Remote Access (RASS) server named MT0SR09 will be used for VPN access.

Existing Environment

Business Processes

Mondo Transport, Ltd. consists of the following primary departments:

1. Accounts
2. Human Resources (HR)
3. Information Technology (IT)
4. Dispatching
5. Administration banana

The IT department manages the entire Mondo Transport network from the Moscow

office or by traveling to the branch offices. All resources are located at the Moscow office and are accessed across the WAN links by users in the branch offices. Although the Dispatching department works closely with Administration, it is still a separate department.

The Administration department consists of three groups named Executives, Managers, and Support

Mondo Transport, Ltd. users in the Managers group have access to an application named MT_Trans. There are two versions of the MT_Trans application:

1. MT_Trans_Bus, which contains passenger information.
2. MT_Trans_Haul, which contains cargo information.

Access to the MT_Trans application is controlled through NTFS permissions.

The MT_Trans_Bus application runs on an application server named MT-SR06 in the Moscow office. Only users in the Moscow office have access to the MT_Trans_Bus application. Users in the Moscow office do not have access to the MT_Trans_Haul application.

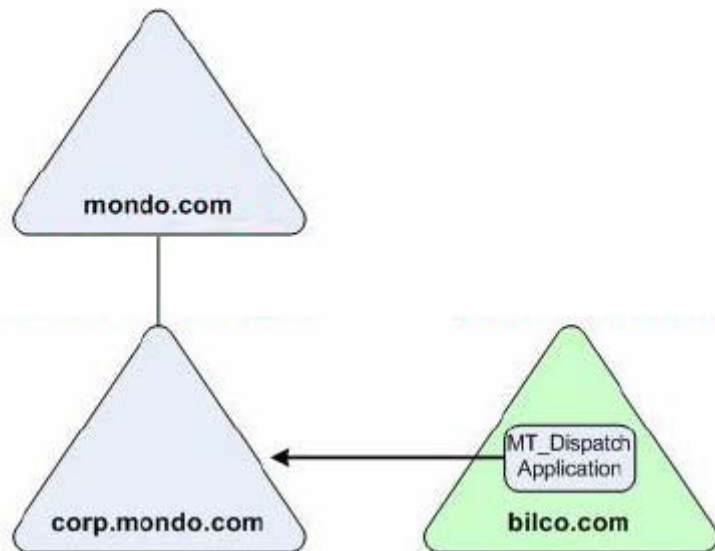
The passenger information must be current within the hour and must be available at all times to all users in the Managers group. The information contained in the MT_Trans_Bus must never become publicly available.

Users in the branch offices only have access to the MT_Trans_Haul application.

Directory Services

The existing domains and trusts are displayed in the Domain Structure exhibit.

Domain Structure



Network Infrastructure

Mondo Transport, Ltd.'s security policy requirements that network administrators use smart cards to log on to the servers. For this reason, all Mondo Transport, Ltd. servers are located at headquarters in Moscow and no servers are located at the branch offices. Each office has a 100-Mbps Ethernet network. All client computers in the branch offices are configured with static IP addresses.

Mondo Transport, Ltd. has a Microsoft Exchange Server 2000 environment that provides Outlook Web Access (OWA) to all Mondo Transport, Ltd. users. The Moscow office has

Exchange Server 2000 front-end server named MT-EX08 that is allocated for OWA. Members of the Executives group have portable client computers which they use to access OWA via the Internet.

The Moscow office has an Internet Security and Acceleration (ISA) server named MT-SR05, which is configured as a firewall and proxy server. MT-SR05 is also used for publishing OWA to executives who connect to the Mondo Transport, Ltd. network from the Internet.

Mondo Transport, Ltd. does not have a public Web site.

Mondo Transport, Ltd.'s written policy states that client computers should run either Windows 2000 Professional or Windows XP Professional but this policy is not currently enforced.

Mondo Transport, Ltd.'s existing server hardware is shown in the following table.

Computer	Processor	Hard Drive	RAM	Description
MT-DC01	Pentium II-800 MHz dual	Two 8-GB SCSI	256 MB	Domain controller for Windows 2000 root domain.
MT-DC02	Pentium II-800 MHz dual	Two 8-GB SCSI	256 MB	Domain controller for Windows 2000 corporate domain.
MT-DC03	Pentium II-800 MHz dual	Two 8-GB SCSI	256 MB	Domain controller for Windows 2000 corporate domain.
MT-DC04	Pentium II-800	Two 8-GB SCSI	256 MB	PDC for Windows NT 4.0 domain.
MT-SR05	Pentium II-800	Two 8-GB SCSI	256 MB	Firewall/Proxy server/ISA 2000 server
MT-SR06	Pentium II-750	Two 8-GB SCSI	256 MB	Windows Server NT 4.0 application server
MT-SR07	Pentium II-750	Two 8-GB SCSI	256 MB	Windows 2000 Server application server
MT-EX08	Pentium II-750	Two 8-GB SCSI	256 MB	Exchange Server 2000 front-end server

Problem Statements

Chief Executive Officer

"We have had consistent growth since we started the business in 2002, but we're reaching market saturation. We need to expand our services into Europe to continue growing."

"We have a full compliment of departments at each office with the exception of the IT department, which is only in the Moscow office. If network administrators are needed in one of the branch offices, they need to travel to that office."

"Our executives and managers also travel quite often. The managers use dial-up access to connect to the corporate network. This is proving to be quite a burden on our budget."

"A separate group of administrators will manage our European offices once they are established."

Chief Information Officer

"We want to establish a Web site named www.mondo.com. the website will include an online booking system for our customers. We have already registered the domain name [mondo.com](http://www.mondo.com). We currently use it for our e-mail addresses. This must not change."

"I am concerned that the new Web site might introduce security risks. I want daily updates of antivirus software to be installed on all desktop computers. I also want our DNS information to remain secure, and the Managers group must still remain a separate group."

"We are planning to upgrade computer hardware within the next year. All computers will have a minimum of 1 GB of RAM and the servers will have seven SCSI hard disk

drives."

"All servers must be upgraded to Windows Server 2003."

Chief Network Administrator

"We have major problems with unreliable and slow WAN links. When a WAN link fails, we can't get access to the MT_Trans application because this application still relies on the NetBIOS name of the corp.mondo.com domain to operate. MONTRANS is the NetBIOS name of the corp.mondo.com domain."

"A new network administrator will be hired to manage the MT_Trans application."

"We need to implement fault tolerance for the domains for instances when the WAN links are down or when a single server fails."

"A separate group IT department members will manage the European branch offices. They will manage the European network independently of the IT department in Moscow but they will report to me as I will be ultimately responsible for making changes to Active Directory."

"Our Exchange 2000 Server, MT-EX08 has excessively high processor utilization at peak usage in the morning. Users report that response time is very slow during the morning."

"Users also report that it takes more than five minutes for them to log on to the network in the mornings. This is probably due to their computers having to communicate with servers at headquarters during log on. You need to implement a solution that reduces communication with Moscow during log on."

"Our patch management system for the branch offices is problematic. Users do not have permissions to install software on their computers. Therefore a network administrator has to travel to the branch offices whenever service packs or new applications need to be installed."

"At present our managers must use dial-up access to connect to our corporate network from remote locations. We want to implement VPN access for them. Only the managers and the executives should be allowed to connect to the network by VPN."

Chief Security Administrator

"When our executives travel, they must be able to access data securely from any branch office and from any remote location."

"Our users have to remember too many passwords. We have one password to log on to the domain, another to access the MT_Dispatch application, and a third to access the MT_Trans application. The office users often forget their passwords"

"The browser settings on all client computers must be configured by using Group Policy objects (GPOs)."

Bilco, Ltd. Security Administrator

"Only authorized Mondo Transport, Ltd. users must be able to access to the MT_Dispatch application. We will create the required users in our domain where the application is hosted and will provide this information to Mondo Transport, Ltd. in the form of a flat file. No other connections to the Bilco, Ltd., network will be allowed."

Topic 4, Mondo Transport, Ltd. (12 Questions)

QUESTION 42

You need to design a top-level OU structure for Mondo Transport, Ltd. You need to ensure that your solution meets the business and technical requirements of the

company.

What should you do? (Choose all that apply.)

- A. Base you top-level OU structure on the departments.
- B. Base you top-level OU structure on the branch offices.
- C. Base you top-level OU structure on Moscow and Budapest.
- D. Base you top-level OU structure on Moscow, Budapest and Warsaw.
- E. Base you top-level OU structure on Moscow and the Information Technology (IT) department.

Answer: C

Explanation: The Moscow and Budapest offices will have separate administration, with Moscow serving as the headquarters for the existing environment and Budapest, the headquarters for the new branch offices.

Incorrect Answers:

A, B: Each branch office has a full compliment of departments except for the IT department, which is only located at Moscow and Budapest. Therefore your top-level OU should not be structured on the departments or the branch offices.

D: Warsaw will be a branch office under the control of Budapest. It does not warrant a top-level OU

E: The IT department for Budapest will operate independently of the IT department at Moscow.

QUESTION 43

DRAG DROP

You need to design an authentication solution for Mondo Transport, Ltd. Your solution must meet the security concerns of the Chief Network Administrator.

What should you do? (To answer, drag the appropriate steps in the pane on the left to the appropriate location in the pane on the right.)

Steps, select from these	Steps, place here
Enroll each administrative account for a smart card authentication certificates.	Place first step here.
Configure autoenrollment for computer authentication certificates.	Place second step here, if any.
Install a smart card reader on each server.	Place third step here, if any.
Install a smart card reader on each server computer	Place fourth step here, if any.
Configure each administrative account to require a smart card for interactive logon.	Place fifth step here, if any.
Configure the Default Domain Policy GPO to require smart cards for interactive login.	Place sixth step here, if any.
Install an enterprise certification authority (CA) on the network.	Place seventh step here, if any.

Answer:

Steps, select from these	Steps, place here
	Install an enterprise certification authority (CA) on the network.
Configure autoenrollment for computer authentication certificates.	Enroll each administrative account for a smart card authentication certificates.
Install a smart card reader on each server.	Install a smart card reader on each server computer.
	Configure each administrative account to require a smart card for interactive logon.
	Place fifth step here, if any.
Configure the Default Domain Policy GPO to require smart cards for interactive login.	Place sixth step here, if any.
	Place seventh step here, if any.

Explanation:

The case study states: "Mondo Transport, Ltd.'s security policy requirements that network administrators use smart cards to log on to the servers. For this reason, all Mondo Transport, Ltd. servers are located at headquarters in Moscow and no servers are located at the branch offices."

Enrollment can occur automatically, for example, when an application sends a certificate request to an enterprise CA and immediately receives a certificate in return, or manually, when a user explicitly requests a certificate from a C

A. To send enrollment

requests to an enterprise CA, you use the Certificates snap-in for Microsoft Management Console. Because smart card logons are intended only for internal users with access to Active Directory, only enterprise CAs can issue smart card certificates.

A smart card is a credit card-size device used to securely store public and private keys, passwords, and other types of personal information. To use a smart card, you need a smart card reader attached to the computer and a personal identification number for the smart card. In Microsoft Windows Server 2003, smart cards can be used to enable certificate-based authentication and single sign-on to the enterprise.

Smart card is required for interactive logon, found in the Account options section of the Account tab, disables logging on without a smart card.

Reference:

Craig Zacker, MCSE Self-Paced Training Kit (Exam 70-293): Planning and Maintaining a Microsoft Windows Server 2003 Network Infrastructure, Microsoft Press, Chapter 19, pp. 19-10 and Glossary, pp. G-51.

Deborah Littlejohn Shinder, and Dr. Thomas W. Shinder, MCSA/MCSE Exam 70-290: Managing and Maintaining a Windows Server 2003 Environment Study Guide & DVD Training System, Syngress, Chapter 4, pp. 283.

QUESTION 44

You need to design a secure remote access solution for Mondo Transport, Ltd. Your solution must meet the business and technical requirements of the company.

What should you do?

- A. Configure MT-SR09 as a DHCP Relay Agent.
- B. Configure the firewall on MT-SR05 to block all VPN traffic.
- C. Configure MT-SR09 to support L2TP/IPSec.
- D. Configure MT-SR09 to assign IP Addresses from DHCP.

Answer: C

Explanation: Windows 2000 Professional and Windows XP Professional VPN uses L2TP and PPTP as a tunneling protocol. L2TP uses IPSec for security.

Incorrect Answers:

A, D: Implementing IP Addressing from remote clients through DHCP does not improve remote access security.

B: If MT-SR09 is located behind the firewall, then you need to allow VPN traffic to pass through the firewall.

QUESTION 45

You need to design a domain naming strategy for the new Mondo Transport, Ltd. environment. You need to ensure that your solution meets the business and technical requirements of the company.

What should you do? (Each correct answer presents part of the solution. Choose TWO.)

- A. Register mondotransport.com as a new domain name for the company.
- B. Register dispatch.mondo.com as a new domain name for the company.
- C. Use the existing mondo.com registered domain name for the company.
- D. Use the UPN suffix of mondotransport.com for all new users.
- E. Use the UPN suffix of mondo.com for all new users.

Answer: C, E

Explanation: In the case study, the Chief Information Officer states: "mondo.com is already registered to the company and is used for e-mail addresses. This must not change." It also states that the NetBIOS name of the corp. mondo.com domain is MONTRANS and that some applications still rely on this NetBIOS name to operate. Users logging on using Windows 2000 or later platforms may log on the same way, or they may log on using the more efficient UPN. The UPN takes the format <UserName>@<UPN Suffix>, where the UPN suffix is, by default, the DNS domain name in which the user object resides.

You should plan names that fit both DNS and NetBIOS name requirements.

Reference:

Walter Glenn, and Michael T. Simpson; MCSE 70-297 Training Kit - Designing a Windows server 2003 Active Directory and Network Infrastructure, Chapter 3, pp 3-27.

QUESTION 46

You need to design a site topology for the new Active Directory environment. You need to ensure that your solution meets Mondo Transport Ltd.'s business and

technical requirements.
What should you do?

- A. Create single site for all the offices.
- B. Create two sites: one site for all the branch offices and one site for the Moscow office.
- C. Create three sites: one site for the Eurasian branch offices, one site for the European offices, and one site for the Moscow office.
- D. Create four sites: one for the Minsk, Kiev and Volgograd branch offices, one site for the Warsaw, Budapest and Bucharest branch offices, one site for the Moscow main office, and one site for the Moscow satellite office.
- E. Create seven sites; one site for the Minsk branch office, one site for the Kiev branch office, one site for the Volgograd branch office, one site for the Budapest branch office, one site for the Warsaw branch office, one site for the Bucharest branch office, and one site for the Moscow main office.

Answer: E

Explanation: You need to improve logon time and reduce logon communication with the Moscow office. This means that you need to deploy a separate Domain controller with Global Catalog (GC) at each office. You need a separate site at each office to control site affinity. This will force client computers in the site to communicate with the local GC for logon purposes.

Incorrect Answers:

- A: A single site will not change the current structure.
- B, C, D: If you only create a site topology with more than one office, then you will continue to have logon problems because site affinity will find any of the remote GC's to authenticate.

QUESTION 47

You need to design a strategy to enable the MT_Dispatch application to successfully resolve computer names. You need to ensure that your solution meets Mondo Transport, Ltd.'s business and technical requirements.
What should you do?

- A. Implement DNS for name resolution.
- B. Implement WINS for name resolution.
- C. Implement HOSTS files on all computers.
- D. Implement LMHOSTS files on all computers.

Answer: A

Explanation: The case study states: "The MT_Dispatch application is an X.500 directory-enabled application that runs on Windows NT Server 4.0 computers in the Moscow office. The company plans to use a new version of the MT_Dispatch application that will run on a Windows Server 2003 computer hosted by Bilco, Ltd. Only Users connect to this application by querying DNS for the application's service

record. This record is stored on a UNIX DNS server running the latest version of BIND."

Berkeley Internet Name Domain (BIND) is an implementation of the Domain Name System (DNS) written and ported to most available versions of the UNIX operating system.

Incorrect Answers:

B, C, D: The case study states that users connect to the MT_Dispatch application by querying DNS.

Reference:

Walter Glenn, and Michael T. Simpson, MCSE 70-297 Training Kit - Designing a Windows server 2003 Active Directory and Network Infrastructure, Glossary, pp. G-2.

QUESTION 48

You need to design a DNS implementation strategy for Mondo Transport, Ltd. You need to ensure that your solution meets the business and technical requirements of the company.

What should you do?

- A. Configure a secondary zone of the bilco.com domain on a domain controller in each office.
- B. Configure the DNS Server service on a domain controller in each office and configure an Active Directory-integrated zone to replicate to all DNS servers in the domain.
- C. Configure an Active Directory-integrated zone on a domain controller in the Moscow office and configure this zone to replicate to the domain controllers in the branch offices.
- D. Configure a primary zone for mondo.com on a domain controller in the Moscow office. Configure a secondary zone on separate DNS server in the Moscow office.

Answer: B

Explanation: When you are running the DNS server service on a computer that is an Active Directory domain controller and you select the Store The Zone In Active Directory (Available Only If DNS Server Is A Domain Controller) check box while creating a zone in the New Zone Wizard, the server does not create a zone database file. Instead, the server stores the DNS resource records for the zone in the Active Directory database. Storing the DNS database in Active Directory provides a number of advantages, including ease of administration, conservation of network bandwidth, and increased security. In Active Directory-integrated zones, the zone database is replicated automatically, along with all other Active Directory data. Active Directory uses a multiple master replication system so that copies of the database are updated on all domain controllers in the domain. You don't have to create secondary zones or manually configure zone transfers, because Active Directory performs the database replication automatically.

This solution satisfies the requirements of the case study, which states: "Our DNS information must remain secure." As well as "Faster name resolution is required when connecting to internal servers and external Web sites".

Furthermore, it also states: "Redundancy for any service must be provided if a single

service fails."

Providing redundancy:-For a network that relies heavily on DNS name resolution, having a single DNS server means having a single point of failure. You should deploy a sufficient number of DNS servers so that at least two copies of every zone are always online.

Reference:

Craig Zacker; MCSE Self-Paced Training Kit (Exam 70-293): Planning and Maintaining a Microsoft Windows Server 2003 Network Infrastructure, Microsoft Press, Chapter 4, pp. 4-28 to 4-37.

QUESTION 49

You need to design the Active Directory logical structure for Mondo Transport, Ltd. Your solution must meet the business and technical requirements of the company.

What logical structure should you implement?

- A. Implement a single forest with one domain.
- B. Implement a single forest with two domains.
- C. Implement two forests with one domain each.
- D. Implement two forests with two domains each.

Answer: B

Explanation: In this scenario there are two IT department teams; one managing the Eurasian offices and the other managing the European offices. Both IT department teams must report to the Chief Network Administrator who will implement Active Directory changes and services and data does not need to be isolated. Therefore you need a single forest with two domains.

Incorrect Answers:

A: The IT department in Budapest is responsible for managing the users and computers in the European offices while the IT department in Moscow is responsible for managing the users and computers in the Eurasian offices. Therefore you need to create two domains.

C, D: In this scenario there are two IT department teams; one manages the Eurasian offices and the other manages the European offices. You do not need to ensure data and service isolation between the two and

QUESTION 50

You need to design a strategy that meets the security requirements for the MT_Trans application. You need to ensure that your solution meets Mondo Transport, Ltd.'s business and technical requirements.

What should you do?

- A. Allow users to access the application via MT-SR09.
- B. Allow users to access the application by dial-up access to MT-SR09.
- C. Install a VPN server in each branch office. Allow users to access the application via

their VPN server.

D. Install a dial-up server in each branch office. Allow users to access the application via their dial-up server.

Answer: A

Explanation:

Virtual private networking (VPN) provides a way of making a secured, private connection from the client to the server over a public network such as the Internet. Unlike dial-up networking, in which a connection is made directly between client and server, a VPN connection is logical and tunneled through another type of connection. Typically, a remote user would connect to an Internet service provider (ISP) using a form of dial-up networking (particularly good for users with high-speed connections). The Routing And Remote Access server would also be connected to the Internet (probably via a persistent, or permanent, connection) and would be configured to accept VPN connections. Once the client is connected to the Internet, it then establishes a VPN connection over that dial-up connection to the Routing And Remote Access server.

The reason for configuring it in the Moscow office is that the MT_Trans runs on a server in the Moscow office, and the information contained in it must never become publicly available.

Currently, an on-site user must send the information to flight officers via an e-mail message, so VPN would make it easier for the flight officers to access it.

Reference:

Walter Glenn, and Michael T. Simpson; MCSE 70-297 Training Kit - Designing a Windows server 2003 Active Directory and Network Infrastructure, Chapter 1, pp. 1-43.

QUESTION 51

You need to design the placement of the PDC emulator operations master role. You need to ensure that your solution meets Mondo Transport, Ltd.'s business and technical requirements.

What should you do? (Choose all that apply.)

- A. Configure the PDC emulator operations master role on a domain controller in the Moscow office.
- B. Configure the PDC emulator operations master role on a domain controller in the Minsk branch office.
- C. Configure the PDC emulator operations master role on a domain controller in the Kiev branch office.
- D. Configure the PDC emulator operations master role on a domain controller in the Volgograd branch office.
- E. Configure the PDC emulator operations master role on a domain controller in the Budapest branch office.
- F. Configure the PDC emulator operations master role on a domain controller in the Bucharest branch office.
- G. Configure the PDC emulator operations master role on a domain controller in the

Warsaw branch office.

Answer: A, E

Explanation: In a native mode Windows Server 2003 environment, the PDC Emulator receives preference in the replication of user account passwords.

The reason for it being placed in Moscow is, "The IT department manages the entire network from the Moscow office or by traveling to the branch offices. All resources are located at the Moscow office and are accessed across the WAN links by users in the branch offices." However, the "Budapest branch office will serve as the regional office for Eastern Europe and a separate group of administrators will manage the new offices from Budapest." Therefore you need a PDC Emulator in Budapest as well.

Reference:

Robert Williams, and Mark Walla, The Ultimate Windows Server 2003 System Administrator's Guide, Addison-Wesley, Chapter 5.

QUESTION 52

You need to design a strategy to improve the performance and reliability of the domain controllers. You need to ensure that your solution meets Mondo Transport, Ltd.'s business and technical requirements.

What should you do? (Each correct answer presents part of the solution. Choose TWO.)

- A. Create a single RAID-5 volume on each domain controller.
- B. Create two RAID-5 volumes on each domain controller.
- C. Create two mirrored volumes on each domain controller.
- D. Create a single mirrored volume on each domain controller.

Answer: A, D

Explanation: A mirrored volume

provides good performance along with excellent fault tolerance. Two disks participate in a mirrored volume, and all data is written to both volumes. As with all RAID configurations, use separate controllers (by adding a controller, you create a configuration called "duplexing") for maximum performance.

A RAID-5 volume uses three or more physical disks to provide fault tolerance and excellent read performance while reducing the cost of fault tolerance in terms of disk capacity. Data is written to all but one disk in a RAID-5. That volume receives a chunk of data, called parity, which acts as a checksum and provides fault tolerance for the stripe. The calculation of parity during a write operation means that RAID-5 is quite intensive on the server's processor for a volume that is not read-only. RAID-5 provides improved read performance, however, as data is retrieved from multiple spindles simultaneously.

Reference:

Dan Holme, and Orin Thomas, MCSA/MCSE Self-Paced Training Kit (Exam 70-290):

Managing and Maintaining a Microsoft Windows Server 2003 Environment, Microsoft Press, Chapter 11, 11-35 to 11-37.

QUESTION 53

DRAG DROP

You need to design an IP address management strategy for Mondo Transport, Ltd. You need to ensure that your solution allows for the anticipated growth of the company. Your solution must also meet the business and technical requirements of the company.

What should you do? (To answer, drag the appropriate steps in the pane on the left to the appropriate location in the pane on the right.)

Steps, select from these	Steps, place here
Install a DHCP server in each office other than the satellite office.	Place first step here.
Install two DHCP servers in each office other than the satellite office.	Place second step here, if any.
Configure the scopes to assign all of the available IP addresses to each office.	Place third step here, if any.
Configure the scopes to assign half the available IP addresses to each office.	Place fourth step here, if any.
Create duplicate scopes that contain the necessary scope options on each server.	Place fifth step here, if any.

Answer:

Steps, select from these	Steps, place here
Install a DHCP server in each office other than the satellite office.	Install two DHCP servers in each office other than the satellite office.
	Create duplicate scopes that contain the necessary scope options on each server.
Configure the scopes to assign all of the available IP addresses to each office.	Configure the scopes to assign half the available IP addresses to each office.
	Place fourth step here, if any.
	Place fifth step here, if any.

Explanation:

You should install two DHCP servers in each office, create duplicate scopes on each DHCP server in the office, and configure each DHCP server in the office to assign a different half the addresses. This will provide fault tolerance.

Topic 5, TestLabs, Inc., Scenario

Background

TestLabs, Inc. is national company that specialized in the development and testing of pharmaceutical medicines. The company has its own research facility in Chicago.

Physical Locations

TestLabs, Inc. has its headquarters in Chicago and branch offices in the following locations:

1. Philadelphia
2. Atlanta
3. New Orleans.

TestLabs, Inc. has expanded into the West Coast by acquiring a pharmaceutical company named Bilco Medical, Ltd. Bilco Medical, Ltd. is located in Berkeley and has a strong background in medical research. Bilco Medical, Ltd. now serves as the Berkeley branch office of TestLabs, Inc.

Business Processes

TestLabs, Inc. consists of the six primary departments listed below:

1. Accounting
2. Administration
3. Distribution
4. Human Resources (HR)
5. Information Technology (IT)
6. Research

Each office maintains its resources separately and each office has its own IT department.

Information is not shared between the three offices, although they all make use of the same database, named TL_Research.

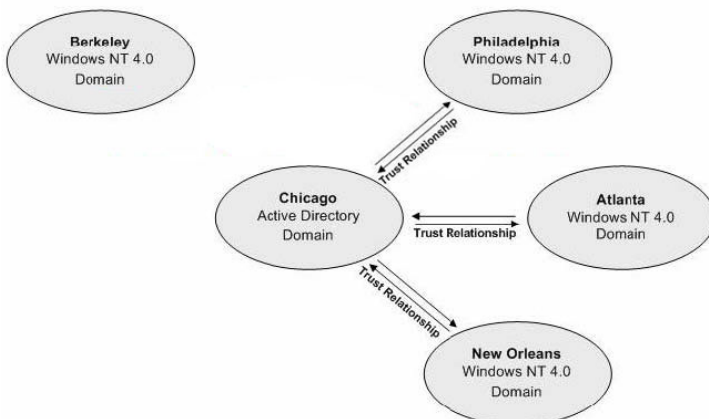
Each office uses a separate instance of an application named TL_ResUpdate that tracks the testing and development of new pharmaceutical drugs. The TL_ResUpdate application updates the TL_Research database.

Infrastructure

Directory Services

Each TestLabs, Inc. branch office has Windows NT 4.0 domain while the Chicago office has a Windows 2000 Active Directory domain named ad.testlabs.com. Trust relationships have been established between the branch offices and headquarters as shown in the Domain Structure exhibit.

Domain Structure



The domain for the Chicago office consists of a single Active Directory site and contains four top-level organizational units (OUs) named Accounting, Distribution, Human Resources, and Research.

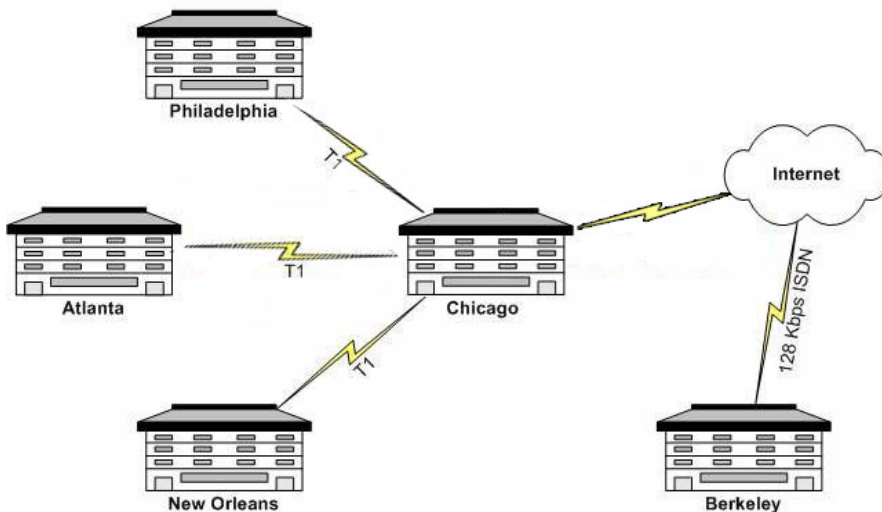
Bilco Medical, Ltd. has a Windows NT 4.0 domain in its Berkeley office. There is not

trust established between the Berkeley office and any of the other locations.

Network Infrastructure:

The Philadelphia, Atlanta and New Orleans branch offices are connected to headquarters by dedicated T1 line as shown in the Network Infrastructure exhibit. The Berkeley branch office is connected to headquarters by a VPN connection.

Network Infrastructure



All client computers in TestLabs, Inc.'s Accounting, IT, and Administration departments run either Windows 2000 Professional or Windows XP Professional.

All client computers in the Distribution department run Windows 98 Second Edition (SE).

All client computers at Bilco Medical, Ltd. run either Windows 98 SE or Windows NT Workstation 4.0.

Both TestLabs, Inc. and Bilco Medical, Ltd. have public Web sites which provides users with information about the company. The TestLabs, Inc. Website is named www.testlabs.com and is hosted by an ISP in Chicago. The Bilco Medical, Ltd. Web site is named www.bilco.com and is hosted by an ISP in Berkeley. The ISP in Berkeley uses a UNIX-based DNS server.

Problem Statements

Chief Executive Office

"Now that we've acquired Bilco Medical, Ltd. we need to integrate more closely into our network. We should also enable headquarters to work more effectively with the branch offices."

"I feel that the acquisition of Bilco Medical, Ltd. is a positive addition to our company. However, Bilco Medical, Ltd. will remain a separate division within TestLabs, Inc. and will maintain its own line of business. For this reason, I would like to track the contributions that Bilco Medical, Ltd. makes to our overall business."

"We want to modernize all our domains, including the Bilco Medical, Ltd. domain but we will want keep the identity and domain namespace of Bilco Medical, Ltd. and TestLabs, Inc. separate."

Chief Information Officer

"The TL_Research database is critical to the success of our company yet it is not used effectively. We must reduce the duplication of effort between TestLabs, Inc. branch

offices in maintaining the TL_Research database by centralizing the database in Chicago."

"The IT department in Chicago will be primarily responsible for the administration of the TL_Research database and will create additional groups for the TL_Research database, as needed."

"We haven't experienced any problems with our WAN links, but I still want to ensure that database access for the TL_Research databases is maintained even in the event of WAN link failure."

Chief Network Administrator

"We want to upgrade our Windows 2000 domain in the Chicago office as well as our Windows NT 4.0 domains in the Philadelphia, Atlanta and New Orleans to Windows Server 2003. The upgrade of these domains must be optimized to reduce the need for network administrators to travel between offices as the administration of Active Directory will be the responsibility of the IT department in the Chicago office."

"We also want to add the Bilco Medical, Ltd. domain to the forest, but the Bilco Medical, Ltd. domain will retain its current namespace. The upgraded Bilco Medical, Ltd. domain will be named ad.bilco.com. We want to ensure that the minimum number of domains is created."

"We will install a single DHCP server in each office. We need to ensure that client computers are still able to obtain an IP address in the event of a DHCP server failure."

"Research department users need greater freedom of movement within the office and in the field. For this reason we will be issuing them with personal digital assistants (PDAs)."

"We want to upgrade all Bilco Medical, Ltd. client computers to Windows XP Professional. To ease the transition, we have decided to migrate the user settings from the existing Bilco Medical, Ltd. client computers but we will recreate the user and group accounts for Bilco Medical, Ltd."

"We foresee substantial expenditure in hiring new IT staff and upgrading client computers in the Bilco Medical, Ltd. division. We also need to provide sufficient access to Bilco Medical, Ltd., but expenditure must be kept to a minimum."

"I want to make sure that we monitor the activities of the new IT staff to be hired in the Bilco Medical, Ltd. division."

"We also want an improved user experience when accessing network resources in the Chicago office."

Chief Security Officer

"We need to ensure that the appropriate permissions to the TL_ResUpdate application, the TL_Research database, and other resources are established for users based on the department that the user belongs to."

"For security reasons, we audit all administrative activity in all domains, particularly in the Bilco Medical, Ltd. domain. This includes interactive logons; shutdowns and restarts of domain controllers; changes to security logging; and changes to user and group accounts."

"Although wireless network will be implemented in each office to support wireless PDAs and VPNs will be implemented in each location to support remote access for the PDAs, I want remote access policies to be centralized."

Bilco Medical, Ltd. Manager

"Now that we've become part of a larger organization, we should be more stable financially but we are not sure if the restrictions imposed by our new parent company will benefit the business of Bilco Medical, Ltd."

"One area where the relationship with TestLabs, Inc. will be most beneficial is the migration from our current spreadsheet system to a database system. The data in our spreadsheets will be imported into a database named BM_Data that will be created, administered and maintained by TestLabs, Inc. in the Chicago office. The database will be replicated from our office to the Chicago office but it is anticipated that database replication will exceed the available bandwidth provided by our Internet connection."

Topic 5, TestLabs, Inc. (11 Questions)

QUESTION 54

You need to design a DNS zone strategy to support the Active Directory domain for Bilco Medical, Ltd. You need to ensure that your solution meets TestLabs, Inc.'s technical and business requirements.

What should you do? (Each Correct answer presents part of the solution. Choose TWO).

- A. Create a standard primary DNS Zone for ad.bilco.com.
- B. Create an Active Directory Integrated DNS Zone for ad.bilco.com.
- C. Enable only authorized client computers to update DNS.
- D. Configure a zone transfer between the DNS servers at Bilco Medical, Ltd. and DNS server at Bilco Medical, Ltd.'s ISP.

Answer: B, C

Explanation:

The case study specifically states that all Domain Controllers are DNS servers and that zones must be secured.

When you are running the DNS server service on a computer that is an Active Directory domain controller and you select the Store The Zone In Active Directory (Available Only If DNS Server Is A Domain Controller) check box while creating a zone in the New Zone Wizard, the server does not create a zone database file. Instead, the server stores the DNS resource records for the zone in the Active Directory database. Storing the DNS database in Active Directory provides a number of advantages, including ease of administration, conservation of network bandwidth, and increased security.

Note: Although the question speaks about designing a zone and not updates, D does not make any sense.

Incorrect Answers:

A: This type of zone can be modified, which is not secure.

D: This option does not make any sense.

Reference:

Walter Glenn, and Michael T. Simpson, MCSE 70297 Training Kit Designing a Windows server 2003 Active Directory and Network Infrastructure, Chapter 1, p. 124.

Craig Zacker, MCSE Self Paced Training Kit (Exam 70293): Planning and Maintaining a Microsoft Windows Server 2003 Network Infrastructure, Chapter 4, p. 436.

QUESTION 55

You need to design a DNS strategy to allow the Bilco Medical, Ltd. domain to resolve names in the TestLabs, Inc. domain. You need to ensure that your solution meets TestLabs, Inc.'s technical and business requirements.

What should you do?

- A. Create a stub zone for ad.bilco.com on a DNS server in Chicago.
- B. Create a secondary zone for ad.bilco.com on a DNS server in Chicago.
- C. Create a secondary zone for ad.testlabs.com on a DNS server in Berkeley.
- D. Configure the DNS server in Berkeley to forward queries to the DNS server in Chicago.

Answer: D

Explanation:

You need to configure the DNS server in Bilco Medical, Ltd. to forward queries for the bilco.com namespace to the DNS server in the bilco.com root domain.

Incorrect Answers:

A: A stub zone is a copy of a zone that contains only the resource records needed to identify an authoritative DNS server. An authoritative DNS server is a server that hosts resource records for a particular DNS zone. Rather than a DNS server having to query the Internet to locate an authoritative DNS server, the DNS server can simply refer to the list of name servers (NS resource records) in the stub zone. Distributing a list of authoritative DNS servers for a zone can be implemented by using stub zones. Unlike secondary zones, which primarily are used for redundancy and load-balancing reasons, stub zones are used to improve name resolution performance.

B, C: Secondary zones are primarily are used for redundancy and load-balancing reasons. It does not improve name resolution performance.

Reference:

J. C. Mackin, and Ian McLean: MCSA/MCSE self-paced training kit (exam 70-291): Implementing, managing, and maintaining a Microsoft Windows Server 2003 network infrastructure, Microsoft, Chapter 4, pp. 4-19, and Chapter 5, pp. 5-6.

Walter Glenn, and Michael T. Simpson; MCSE 70-297 Training Kit - Designing a Windows server 2003 Active Directory and Network Infrastructure, Chapter 6, pp. 6-26.

QUESTION 56

You need to design a strategy for adding the additional hardware necessary to support Bilco Medical, Ltd. You need to ensure that your solution meets TestLabs, Inc.'s technical and business requirements.

What should you do?

- A. Add a dedicated T1 WAN Link between Berkeley and Chicago.
- B. Add a dedicated E3 WAN Link between Berkeley and New Orleans.

- C. Add an ISDN connection between Berkeley and Chicago.
- D. Add an ISDN connection between Berkeley and New Orleans.

Answer: A

Explanation: You need to allow for database replication between Chicago and Berkeley but the Bilco Medical, Ltd. Manager say: "it is anticipated that database replication will exceed the available bandwidth provided by our Internet connection". Therefore you should create a WAN link between Berkeley and Chicago.

Incorrect Answers:

B: E1 and E3 WAN links are used in Europe. Also, you do not need a link between Berkeley and New Orleans as Bilco Medical, Ltd.'s database and the TestLabs, Inc. domain is managed from Chicago and not New Orleans.

C: An ISDN solution is already in place to Bilco Medical, Ltd.'s ISP but it is not sufficient.

D: You do not need a link between Berkeley and New Orleans as Bilco Medical, Ltd.'s database and the TestLabs, Inc. domain is managed from Chicago and not New Orleans.

QUESTION 57

You need to design a client computer upgrade strategy for Bilco Medical, Ltd. You need to ensure that your solution meets TestLabs, Inc.'s technical and business requirements.

What should you do? (Choose all that apply.)

- A. Use the `ldifde` command to migrate user settings.
- B. Use the User State Migration Tool (USMT) to Migrate user settings.
- C. Use the Active Directory Migration Tool (ADMT) to migrate user settings.
- D. Create trust relationships between the `ad.testlabs.com` domain and the Bilco Medical, Ltd. domain.
- E. Create trust relationships between the forest root domain and the Bilco Medical, Ltd. domain.

Answer: B

Explanation: The User State Migration Tool (USMT) tool is used to collect a user's documents and settings before an operating system is upgraded from an earlier version of Windows to Windows XP Professional. After the upgrade, a user's documents and settings can be restored.

Incorrect Answers:

A: The `ldifde` command line tool facilitates the importing and exporting of larger numbers of security principals, including groups. It does not migrate user settings.

C: Active Directory Migration Tool (ADMT) 2.0, which allows migration of users and passwords from Windows NT 4.0 and Windows 2000 domains to Windows 2003 domains. It does not migrate user settings.

D, E: Trust relationships between the root domain or forest root are not required for the

migration of user settings.

Reference:

William Gruber, Sandra Faucett, Greg Gille, Jim Bevan, Deborah R. Jay, and Chris McKitterick, Microsoft Windows Server 2003 Deployment Kit Automating and Customizing Installations, A Resource Kit Publication, Chapter 5, p. 321.

QUESTION 58

You need to design a DNS Name resolution strategy for the client computer in the Distribution department. You need to ensure that your solution meets TestLabs, Inc.'s technical and business requirements.

What should you do? (Each Correct answer presents a complete solution. Choose TWO.)

- A. Create a reverse lookup zone in DNS for each new domain.
- B. Create a WINS lookup record in the DNS forward lookup zone.
- C. Create a WINS reverse record in the DNS reverse lookup zone.
- D. On each DHCP server, enable Dynamic updates for DownLevel client computers.

Answer: B, D

Explanation: The WINS resource record instructs the DNS service to use WINS to look up and forward queries for host names not found in the zone database.

"...the Dynamically update DNS A and PTR records for DHCP clients that do not request updates (for example, clients running Windows NT 4.0) check box must also be selected before DHCP will update the A and PTR records for these clients automatically. The check box is not checked by default."

Incorrect Answers:

A: The reverse lookup zone will handle those few queries where the client knows the IP address and wants a host name. You can get by without creating reverse lookup zones

C: A WINS reverse lookup zone is of no use.

Reference:

Walter Glenn, and Michael T. Simpson, MCSE 70297 Training Kit Designing a Windows server 2003 Active Directory and Network Infrastructure, Chapter 6, p. 614.
Deborah Littlejohn Shinder, and Dr. Thomas W. Shinder, Exam 70291: MCSA/MCSE Implementing, Managing, and Maintaining a Windows Server 2003 Network Infrastructure Guide & DVD Training System, Syngress, Chapter 3, p. 17.
William Boswell, Inside Windows Server 2003, Addison Wesley, Chapter 5.

QUESTION 59

You need to design an upgrade strategy for the client computers in the Bilco Medical, Ltd. division. You need to ensure that your solution meets TestLabs, Inc.'s technical and business requirements.

What should you do?

- A. Upgrade the client computers to Windows XP Professional.
- B. Use the User State Migration Tool (USMT) to Migrate user settings.

- C. Create trust relationships between the Bilco Medical, Ltd. domain and the forest root domain. Then use the Active Directory Migration Tool (ADMT) to migrate user settings.
- D. Create trust relationships between the forest root domain and the Bilco Medical, Ltd. domain. Then use the Active Directory Migration Tool (ADMT) to migrate user settings.

Answer: B

Explanation: The User State Migration Tool (USMT) tool is used to collect a user's documents and settings before an operating system is upgraded from an earlier version of Windows to Windows XP Professional. After the upgrade, a user's documents and settings can be restored.

Incorrect Answers:

A: You need to migrate user settings before you upgrade the client computers in accordance with the requirements of the Network Administrator.

C, D: Active Directory Migration Tool (ADMT) 2.0, which allows migration of users and passwords from Windows NT 4.0 and Windows 2000 domains to Windows 2003 domains. It does not migrate user settings.

Reference:

William Gruber, Sandra Faucett, Greg Gille, Jim Bevan, Deborah R. Jay, and Chris McKitterick, Microsoft Windows Server 2003 Deployment Kit Automating and Customizing Installations, A Resource Kit Publication, Chapter 5, p. 321.

QUESTION 60

You need to design a remote access strategy for the Research department. You need to ensure that your solution meets TestLabs, Inc.'s technical and business requirements.

What should you do?

- A. Configure all servers that run Routing and Remote Access (RRAS) as RADIUS Clients.
- B. Configure an identical Remote Access policy on all servers that run Routing and Remote Access (RRAS) and configure the Access method as VPN access.
- C. Configure an identical Remote Access policy on all servers that run Routing and Remote Access (RRAS) and configure the Access method as dialup access.
- D. Configure an identical Remote Access policy on all servers that run Routing and Remote Access (RRAS) and configure the Access method as wireless access.

Answer: A.

Explanation: IAS is the Microsoft implementation of a RADIUS server and proxy. The basic purpose of a RADIUS server is to centralize remote access authentication, authorization, and logging. RADIUS is useful, for example, in large organizations such as ISPs that need to manage many remote access connections to separate remote access servers.

For basic RADIUS scenarios in which no RADIUS proxy is implemented, deploying IAS as a RADIUS server requires configuration both at the client running Routing And

Remote Access and at the server running IAS.

Incorrect Answers:

B, C, D: The case study specifies that Remote Access policies must be centralized.

Reference:

J. C. Mackin, and Ian McLean, MCSA/MCSE self paced training kit (exam 70291): implementing, managing, and maintaining a Microsoft Windows Server 2003 network infrastructure, Chapter 10, pp. 1069 - 1074.

QUESTION 61

You need to design a DNS implementing strategy for TestLabs, Inc. You need to ensure that your solution meets the business and technical requirement of the company.

What should you do?

- A. Create Sub Zones for TestLabs, Inc.
- B. Create Standard Primary Zones TestLabs, Inc.
- C. Create Secondary Zones TestLabs, Inc.
- D. Create Active Directory Integrated Zones TestLabs, Inc.

Answer: D

Explanation: The case study specifically states that all Domain Controllers are DNS servers and that zones must be secured.

When you are running the DNS server service on a computer that is an Active Directory domain controller and you select the Store The Zone In Active Directory (Available Only If DNS Server Is A Domain Controller) check box while creating a zone in the New Zone Wizard, the server does not create a zone database file. Instead, the server stores the DNS resource records for the zone in the Active Directory database. Storing the DNS database in Active Directory provides a number of advantages, including ease of administration, conservation of network bandwidth, and increased security.

Incorrect Answers:

A: Stub zones are most frequently used to keep track of the name servers authoritative for delegated zones.

B: For standard primary zones, only a single server can host and load the master copy of the zone. If you create a zone and keep it as a standard primary zone, no additional primary servers for the zone are permitted.

C: Secondary zones can increase fault tolerance and availability, but zone transfer traffic can consume unacceptable amounts of bandwidth in some circumstances.

Reference:

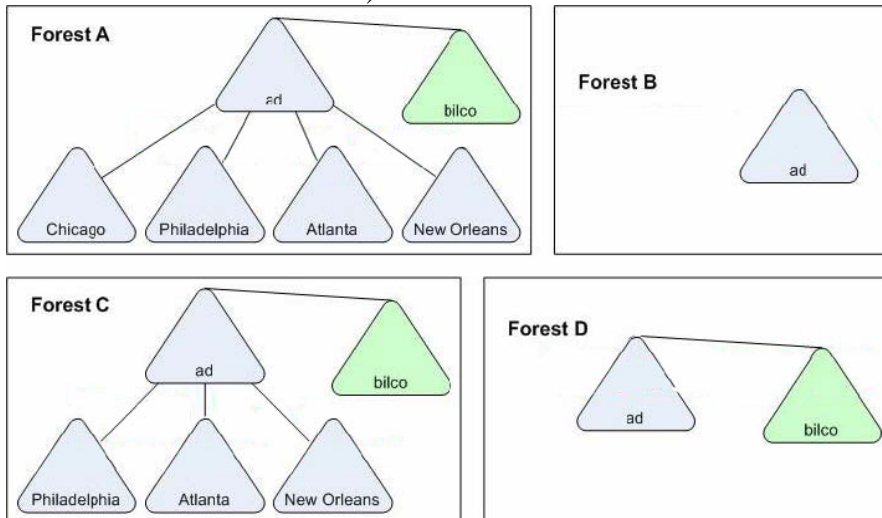
J. C. Mackin, and Ian McLean, MCSA/MCSE self paced training kit (exam 70291): implementing, managing, and maintaining a Microsoft Windows Server 2003 network infrastructure, Chapter 4, pp. 430, 566.

Craig Zacker, MCSE Self Paced Training Kit (Exam 70293): Planning and Maintaining a Microsoft Windows Server 2003 Network Infrastructure, Chapter 4, p. 436.

QUESTION 62

You need to design a Active Directory Infrastructure for the new forest. You need to ensure that your solution meets TestLabs, Inc.'s technical and business requirements.

What should you do? (To answer, select the appropriate Active Directory Infrastructure in the exhibit.)



- A. Forest A.
- B. Forest B.
- C. Forest C.
- D. Forest D.

Answer: C

Explanation: According to the CEO and CIO, Bilco Medical, Ltd., will be added to the forest, but will retain a separate namespace. This means that the Bilco Medical, Ltd. domain is a domain tree along side TestLabs, Ltd.'s domain in the single Active Directory forest.

You must also use the minimum number of domains. Therefore you should place headquarters in the root domain and the other three offices in their own subdomains.

Incorrect Answers:

A: You need to use the minimum number of domains. You do not need a subdomain for the Chicago office as the Active Directory domain is managed from Chicago.

B: Bilco Medical, Ltd. should have a separate root domain as it must retain its current namespace.

D: The IT department at headquarters must be responsible to Active Directory administration and not the IT departments at the branch offices. Therefore a division is required between headquarters and the branch offices.

Reference:

Walter Glenn, and Michael T. Simpson, MCSE 70297 Training Kit Designing a Windows server 2003 Active Directory and Network Infrastructure, Chapter 3, p. 38.

QUESTION 63

You need to design the upgrade path for all TestLabs, Inc.'s domains. You need to ensure that your solution meets the technical and business requirements of the company.

What should you do?

- A. Upgrade the Chicago domain and then upgrade the Philadelphia, Atlanta, New Orleans and Berkley domains.
- B. Create a forest root domain and then upgrade the Chicago, Philadelphia, Atlanta, New Orleans and Berkley domains.
- C. Create a forest root domain. Upgrade the Chicago domain and then upgrade the Philadelphia, Atlanta, New Orleans and Berkley domains.
- D. Create a forest root domain. Upgrade the Philadelphia, Atlanta, New Orleans and Berkley domains and then upgrade the Chicago domain.

Answer: A

Explanation: You must first upgrade the root domain at Chicago by running the adprep /forestprep command on the Schema master. Then you must run the adprep /domainprep command on the infrastructure master. After that you can upgrade the Windows NT 4.0 domains.

Incorrect Answers:

B: You should first upgrade the Windows 2000 forest root in Chicago to take advantage of the advanced features of Windows Server 2003 forests. If you upgrade the Windows NT 4.0 domains before you upgrade the Windows 2000 forest root, you will not be able to use the advanced Windows Server 2003 features.

C, D: You should not create a new forest root as a Windows 2000 forest root already exists in Chicago. You should upgrade the forest root domain.

QUESTION 64

You need to design a strategy to perform an in place upgrade of domain controllers in Philadelphia, Atlanta and New Orleans. You need to ensure that your solution meets TestLabs, Inc.'s technical and business requirements.

What should you do? Which method should you use?

- A. Run the adprep command.
- B. Uses sysprep.
- C. Use and Answer File.
- D. Use Remote Installation Services (RIS).

Answer: C.

Explanation: An in place domain upgrade is useful in the following circumstances:

1. The current domain structure translates well to Windows Server 2003.
2. You are limited in the amount of design and deployment time you are given.
3. You want to minimize changes to the current administrative structure or flow of

information on the network.

4. You want to minimize the effect that users and administrators experience during the migration.

Incorrect: answer:

A: The adprep command prepares Windows 2000 domains and forests for an upgrade to Windows Server 2003. We have Windows NT 4.0 domains, not Windows 2000 domains.

B: Sysprep is used for clean installations not upgrades.

D: RIS cannot perform domain controller upgrades.

Reference:

Walter Glenn, and Michael T. Simpson, MCSE 70297 Training Kit Designing a Microsoft Windows Server 2003 Active Directory and Network Infrastructure, Chapter 5, p. 534.

Topic 6, International Retailers, Scenario

Background

International Retailers is a shipping company that specializes in distributing equipment all over the world.

Physical Locations

The company's head quarters is located in New York and has 250 users. The company has three branch offices in the following locations:

1. Calais which has 150 users
2. Perth which has 50 users
3. Durban which has 70 users

Planned Changes

To reduce costs and streamline business processes, the company wants to implement a Windows Server 2003 Active Directory environment. The transition to the new network must be performed with the least amount of administrative effort and minimal disruption of services to users.

The company plans to open two additional branch offices within the next three months. These offices will be located in Sao Paulo and Rio de Janeiro. Sao Paulo will have 40 users and Rio de Janeiro will have between 10 and 15 users.

International Retailers	Location	Number of users
Head Quarters	New York	250
Branch Office	Calais	150
Branch Office	Perth	50
Branch Office	Durban	70
Future Branch Office	Sao Paulo	40
Future Branch Office	Rio de Janeiro	10-15

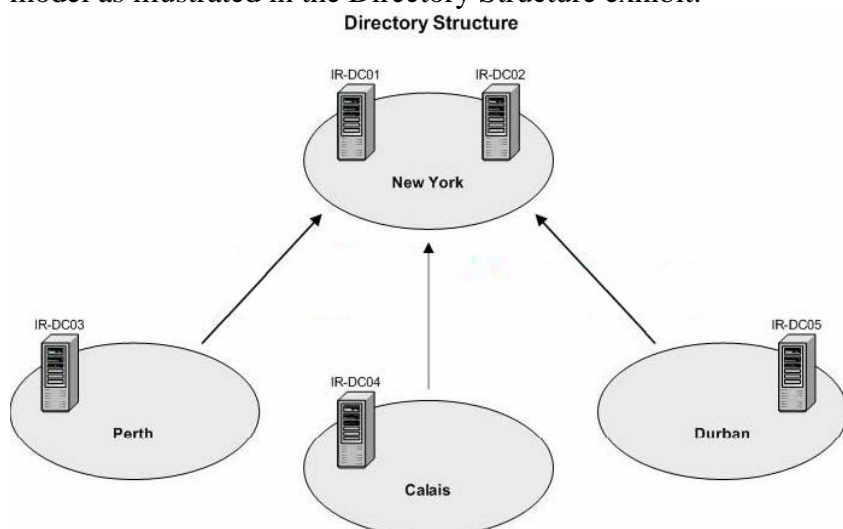
The International Retailers Web presence is in the form of a public Web site named international.com on a Web server. This Web server is not joined to the domain. The international.com domain name is registered with Internet Authorities as a public Web site as well as an Internet e-mail.

A Windows NT Server 4.0 computer named IR-SR01 in the New York office hosts a mission-critical, line of business application. This application is accessed by users from

all departments and offices in the company. The application vendor currently does not support running the application on any operating system other than Windows NT Server 4.0.

Existing Directory Services

The company has four Windows NT 4.0 domains configured in a single master domain model as illustrated in the Directory Structure exhibit.



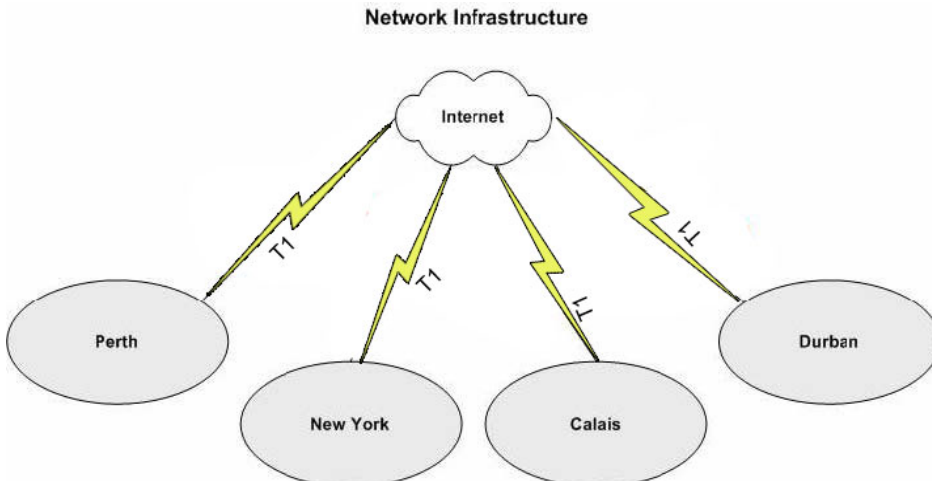
All user accounts reside in and are maintained in the master user domain (MUD) in New York. Client computer accounts are managed locally in each regional / resource domain which is located in Perth, Calais and Durban. Network administration is carried out by the New York IT personnel. Day-to-day maintenance of local computers is handled by local IT teams at the branch offices. IT responsibilities for the company are shown in the following table.

Job Title	Office	Responsibility
CIO	New York	Oversees all IT operations for all offices
IT Manager	New York	Manages all aspects of the network for all offices.
IT Team	New York	Manages user and computer accounts at the local branch. Day-to-day maintenance of local computers.
IT Team	Perth	Manages user and computer accounts at the local branch. Day-to-day maintenance of local computers.
IT Team	Calais	Manages user and computer accounts at the local branch. Day-to-day maintenance of local computers.
IT Team	Durban	Manages user and computer accounts at the local branch. Day-to-day maintenance of local computers.

Existing Network Infrastructure

Each branch office network is connected to the Internet via a local Internet Service Provider (ISP). In each branch office there is a Windows 2000 RRAS server that is configured as VPN servers to make provision for VPN connections to all the other offices. At present each office utilizes between 10 and 20 percent of its available WAN bandwidth.

The existing network infrastructure is shown in the Network Infrastructure exhibit.



The existing domain controller hardware is illustrated in the following table.

Name	Operating system	CPU	Location	Role
DC01	Windows NT Server 4.0	Pentium III 1 GHz	New York	PDC
DC02	Windows NT Server 4.0	Pentium III 866 MHz	New York	BDC
DC03	Windows NT Server 4.0	RISC 300 MHz	Perth	PDC
DC04	Windows NT Server 4.0	AMD 850 MHz	Calais	PDC
DC05	Windows NT Server 4.0	RISC 250 MHz	Durban	PDC

Client Computers and Users

Currently the network system client computers run Microsoft Windows NT 4.0 Workstation with the latest service pack, Microsoft Windows 2000 Professional, or Microsoft Windows XP Professional. The following table illustrated the distribution of these computers on the International Retailers network:

Operating system	New York	Perth	Calais	Durban	Total
Windows NT 4.0 Workstation			50		50
Windows 2000 Professional	100	90		50	240
Windows XP Professional	150	60		20	230
Total client computers	250	150	50	70	520

Problem Statements

The following business problems must be considered:

1. Because of security limitations of Windows NT Server 4.0, all IT staff has been added to the Administrators group of the international domain. IT staff should be allowed administrative rights only to their specific areas of responsibility.
2. Lack of control over IT procedures and processes have made the current environment costly to maintain.

Chief Executive Officer

The current IT infrastructure at International Retailers is negatively affecting business operations. IT operations need to be streamlined to accommodate the anticipated growth. We are planning to open two new branch offices; one in Rio de Janeiro and one in Sao Paulo. A budget for these offices has already been approved with regard to the purchase of the necessary hardware. No new server hardware is to be purchased for the existing offices. New server hardware has been budgeted for the new offices.

The budget approval will cover the hardware for the following:

1. Sao Paulo - 40 users and local IT team
2. Rio de Janeiro - 15 users, NO servers, NO IT personnel.

The Rio de Janeiro computers should authenticate primarily to domain controllers that will be in the Sao Paulo office.

The Sao Paulo IT team will be responsible for the necessary technical support that might be required by the Rio de Janeiro users.

Chief Information Officer

The current IT environment needs to be reorganized. Corporate standards need to be implemented. Users currently install unauthorized and unlicensed software. These standards need to be implemented. Administrative roles have been clearly defined, but now need to be enforced.

We should keep the structure of the network as simple as possible because there are not many IT personnel. We should pay most of our attention to striving to provide our users with the technical support they require. We will continue to manage the network from the New York office. And the local IT teams in the offices have limited authority since they can only provide the necessary technical support to the users in their respective branches, reset their domain user account passwords, and perform routine maintenance tasks on their local computers.

The process of upgrading the International Retailers computers is already in progress. Eventually all servers will run Microsoft Windows Server 2003, and all client computers will run Microsoft Windows XP Professional. However, since not all computers meet the system requirements for these operating systems, and given the fact that there are monetary restraints, we should focus on servers first and the client computers will have to run their current operating systems in the foreseeable future until at least the next financial budget allocation.

Our line of business application developers informed us that the application we are currently using, that is installed on IR-SR01, is designed to run on Microsoft Windows NT Server 4.0 and that there will NOT be an upgrade for the application in the next year. Also we want to provide all users VPN access to the network.

Chief Security Officer

There is a need to provide standardized settings for all users and computers. The current IT administration practices need to be reevaluated, and new practices that are more effective need to be enforced.

Users will have limited access to their computers. They will be allowed to modify only certain desktop settings, and they will not be allowed to install unauthorized applications. Some users currently have blank passwords. Password security standards must be implemented. Therefore all users must have strong passwords that must be changed at least every three months.

Security auditing must be implemented to track all unauthorized logon attempts to the domain. Auditing must not be enabled on any client computers.

The DNS infrastructure must be fault tolerant and secure. Therefore only secure dynamic updates will be allowed.

Office Worker

The current environment is difficult to use. Information is scattered on the network, making it difficult to find. There does not seem to be any clear definition as to who is responsible for responding to network and computer problems. Because of this confusion, most users manage their own computers.

Also, we want to be able to connect to the network when working remotely.

Organizational Goals

The following organizational requirements must be considered:

1. Branch offices in Rio de Janeiro and Sao Paulo will be implemented in the next year. The Sao Paulo branch office is expected to have 40 users and client computers. The Rio de Janeiro branch office will have no more than 15 users and client computers.
2. Because of the small size of the Rio de Janeiro branch office, it will have no IT staff and no servers. The Sao Paulo IT staff will manage users and computers for both the Rio de Janeiro and Sao Paulo branch offices.
3. Two servers have been purchased for the Sao Paulo branch office. One will be designated as a domain controller. The other server will be a VPN server and will also provide NAT services.

Technical Requirements

The following requirements must be considered:

1. The DNS namespace used for the externally hosted e-mail infrastructure is international.com.
2. This namespace must be contiguous and intuitive and must not cause confusion for the internal users when they access the Internet.
3. Apart from the international.com domain, NO other names will be registered on the Internet.
1. The new WAN infrastructure must provide fault tolerance for inter-site communications in the event of a single domain controller failure.
1. The new WAN infrastructure should also allow inter-site traffic to be directed along specific routes between sites.
2. Name resolution must occur within the sites since we should strive to minimize name resolution traffic across the WAN links.
3. All computers on the network should be able to resolve each other's names.
4. To improve network support, Windows Server 2003 will become the corporate standard for all server computers wherever possible. Client computers will be standardized over the next two years to run Windows XP Professional.
5. The amount of public IP addresses on the International Retailers network must be kept to a minimum.
6. Therefore only private addresses must be used on the internal network.

Active Directory

The following Active Directory requirements must be considered:

1. Centralized control over Active Directory must be maintained by the network administrator in the New York office. Limited access to Active Directory will be given to the IT teams in the branch offices.
2. Although bandwidth is not currently an issue, incremental increase in bandwidth usage is anticipated. To accommodate this projected growth, all designs should minimize WAN traffic.
3. Departments within International Retailers have their own unique needs, which include, but are not limited to, specialized departmental applications.

Network Infrastructure

The following infrastructure requirements must be considered:

1. Remote access security and restrictions for all offices must be implemented and managed centrally by the network administrator in the New York office. Only one set of

remote access policies must exist for the company.

2. A domain-naming strategy must be identified that reduces administrative complexity and is intuitive to the users.

3. One domain controller in each of the current offices will have the DNS service installed. DNS name resolution traffic must be minimized over all WAN links.

Topic 6, International Retailers (14 Questions)

QUESTION 65

You need to evaluate whether to upgrade all domains to Windows Server 2003.

Based on current configurations, which server or servers prevent you from achieving this goal? (Choose TWO.)

- A. IR-SR01
- B. IR-DC01
- C. IR-DC02
- D. IR-DC03
- E. IR-DC04
- F. IR-DC05
- G. IR-DC06

Answer: D, F

Explanation: The question asks what is preventing you from upgrading the DOMAINS to Windows Server 2003. The correct answer is D and F. Both these servers are PDC in their domain. The problem is that they are RISC servers. There is no RISC version of Windows 2003 so the domain cannot be upgraded.

1. A Windows NT Server 4.0 computer named IR-SR01 in the New York office hosts a mission-critical, line of business application.

2. The application vendor currently does not support running the application on any operating system other than Windows NT Server 4.0.

Incorrect Answers:

A: The case study says that IR-SR01 is currently hosting a mission critical application, and that the application vendor does not support running this application on any operating system other than Windows NT Server 4.0.

B, C, E, G: These BDCs are running Pentium processors which do support Windows Server 2003. Furthermore, BDCs can be upgraded from Windows NT Server 4.0 domains to Windows Server 2003 domains.

Reference:

Jerry Honeycutt; Introducing Microsoft Windows Server 2003, Microsoft Press, Redmond, Washington, Chapter 16.

QUESTION 66

You are designing the Windows Server 2003 Active Directory forest structure to meet the stated requirements.

Which forest structure should you use?

- A. One Active Directory forest with one domain.
- B. One Active Directory forest with three domains.
- C. One Active Directory forest with four domains.
- D. Four Active Directory forests with one domain in each forest.

Answer: A

Explanation: In the security section of the case study it states: "Regional network administrators must have only limited control over the Active Directory Service. They will be responsible for managing user and computer accounts for their regions. Therefore, the locations will become OUs and we will delegate control."

Incorrect answers:

B, C, D: The network administrator in the New York office will manage all domain controllers, configure sites and perform other high-level administrative tasks. This would then be the Root of the forest. There was no reason in the case study given that would state the requirement of a multi domain model such as different passwords or schema. It is for this reason that B, C, D are incorrect.

Reference:

Windows Server 2003 Deployment Kit - Designing and deploying Directory and Security Services, Creating a Domain Design.

QUESTION 67

You need to decide which Active Directory domains should be created to meet the stated requirements.

What should you do?

- A. Create a international.com domain
- B. Create a corp.international.com domain
- C. Create a calais.international.com domain
- D. Create a perth.international.com domain
- E. Create a Durban.international.com domain

Answer: B

Explanation: Since the name international.com domain is the namespace already in use and registered for the International Retailers public Web site and the requirements state that:

1. Centralized control over Active Directory must be maintained by the network administrator in the New York office.
2. The DNS namespace used for the externally hosted e-mail infrastructure is international.com.
 1. This namespace must be contiguous and intuitive and must not cause confusion for the internal users when they access the Internet.
 2. Apart from the international.com domain, NO other names will be registered on the Internet.

You should not use the name international.com domain on the internal network and therefore corp.international.com domain would be more appropriate.

Incorrect answers:

A: You cannot use the international.com domain name for the internal network since it will cause confusion.

C, D, E: Any of these label names will be appropriate as the names of child domains if you were to have designed separate child domains for the branch offices. But this is not what is required.

Reference:

Windows Server 2003 Deployment Kit - Designing and deploying Directory and Security Services, Creating a Domain Design.

QUESTION 68

Your need to design the top-level organizational level (OU) for International Retailers. You need to ensure that your design meets the stated requirements and accommodates the anticipated growth of the company.

What should you do?

- A. Use Calais OU, Perth OU, New York OU, Durban OU, Rio de Janeiro-Sao Paulo OU
- B. Use IT Administration OU, All International Departments OU, All International Offices OU
- C. Use Sales OU, Purchasing OU, Marketing OU, Accounting OU, Distribution OU, Human Resources OU
- D. Use International Users OU, International Computers OU, International Servers OU, International Applications OU

Answer: A

Explanation: Although you should not create separate OUs based on geographic locations just because it's an obvious dividing point for structure, there are times when it is an appropriate decision. When the network is dispersed over a wide area, you can make it easier to design site boundaries by creating a separate OU for each location and then creating nested OUs that delegate administrative control.

Sites in Active Directory provide a way to abstract the logical organization of the directory structure (the forest, domain, and organizational unit [OU] structure) from the physical layout of the network. Sites take the responsibility for representing the physical layout within Active Directory. Because sites are independent of the domain structure, a single domain can include multiple sites or a single site can include multiple domains.

1. Centralized control over Active Directory must be maintained by the network administrator in the New York office. Limited access to Active Directory will be given to the IT teams in the branch offices.
2. Because of the small size of the Rio de Janeiro branch office, it will have no IT staff and no servers. The Sao Paulo IT staff will manage users and computers for both the Rio de Janeiro and Sao Paulo branch offices.

Incorrect answers:

B: This is not functional since there will not be IT staff in all the sites.

C, D: This OU structure will not be practical under the circumstances. Departments within International Retailers have their own unique needs, which include, but are not limited to, specialized departmental applications.

Reference:

Walter Glenn, and Michael T. Simpson; MCSE 70-297 Training Kit - Designing a Windows server 2003 Active Directory and Network Infrastructure, Chapter 4, pp. 4-4, and Chapter 5, pp. 5-3 to 5-4.

QUESTION 69

You are creating the logical design for the Active Directory infrastructure. You need to design a strategy for group policy implementation regarding password policies.

What should you do? (Each correct answer is a complete solution. Choose TWO.)

A. Create a new GPO named Passwords and configure the appropriate password policies in it.

Link Passwords to each site. Then delegate the local IT team the right to reset passwords in their respective sites.

B. Create a new GPO named Passwords and configure the appropriate password policies in it.

Link Passwords to each office-specific OU. Then delegate all IT teams the right to reset passwords in the domain.

C. Configure the appropriate password policies in the Default Domain Policy GPO.

D. Configure the appropriate password policies in the Default Domain Controllers Policy GPO.

E. Create an OU for each office and place the accounts of all users in that office in the corresponding OU.

Then delegate the right to reset user passwords in the OU to the local IT team.

F. Delegate the IT teams the right to reset passwords in the Domain Controllers OU.

Answer: C, E

Explanation: You need to implement password policies and enable the IT teams in the respective offices to reset passwords for the local users. Password policies that apply to domain user accounts can be configured only in domain-level Group Policy Objects (GPOs) therefore you can either configure the appropriate password policies in the Default Domain Policy GPO. The Default Domain GPO is created by default, or you could configure the password policies in another GPO and link it to the domain. You need to take into account:

1. There is a need to provide standardized settings for all users and computers. The current IT administration practices need to be reevaluated, and new practices that are more effective need to be enforced.
2. Some users currently have blank passwords. Password security standards must be implemented. Therefore all users must have strong passwords that must be changed at least every three months.
3. And the local IT teams in the offices have limited authority since they can only

provide the necessary technical support to the users in their respective branches, reset their domain user account passwords, and perform routine maintenance tasks on their local computers.

Therefore for each office - create an OU and place the accounts of all users in that office in the corresponding OU. Then for each OU, delegate the right to reset user passwords in the OU to the local IT team.

Incorrect answers:

A: User account policies that are configured in GPOs linked to sites or OUs will apply only to local user accounts on the computers in those sites or OUs, they do not apply to domain user accounts.

B: If you delegate the IT teams the right to reset passwords in the domain, then all IT personnel will be able to reset passwords on any user account. This goes against the requirement that states that IT teams should only be able to reset passwords only for the users in their respective branch offices.

D: The Default Domain Controllers Policy is automatically creates and is linked to the Domain Controllers OU. Password policies in this GPO will not apply to domain user accounts.

F: There should not be user accounts in a Domain Controllers OU. Therefore you should not delegate rights to reset passwords in this OU.

Reference:

Dan Holme, and Orin Thomas; MCSA/MCSE Self-Paced Training Kit (Exam 70-290): Managing and Maintaining a Microsoft Windows Server 2003 Environment, Chapter 3, pp. 3-39, and 3-42 to 3-43.

Windows Server Deployment Kit, Group Policy, Group Policy Design.

QUESTION 70

You are designing the Active Directory and network structure physical design. You need to decide on the placement of the PDC emulator role to meet the business and technical requirements.

What should you do?

- A. Place the PDC emulator role in the New York office.
- B. Place the PDC emulator role in the Calais office.
- C. Place the PDC emulator role in the Perth office.
- D. Place the PDC emulator role in the Durban office.
- E. Place the PDC emulator role in the Rio de Janeiro office.
- F. Place the PDC emulator role in the Sao Paulo office.

Answer: B

Explanation

: A PDC emulator is the domain controller in an Active Directory domain that appears as a Windows NT 4.0 PDC for domain member computers that run legacy operating systems. Only one domain controller in a domain can be the PDC emulator. By default the first domain controller is the PD emulator. When more domain controllers are added to the domain, you can configure another domain controller as the PDC emulator.

In this case study, only one Active Directory domain is required, hence only one PDC

emulator will exist on the network. Domain member computers that run Microsoft Windows 2000, or later, can use any available domain controller for directory writes e.g. password changes. But since Calais will be the only office that has client computers running Microsoft Windows NT 4.0 as the operating systems it would make sense to place the PDC emulator there.

1. Our line of business application developers informed us that the application we are currently using, that is installed on IR-SR01, is designed to run on Microsoft Windows NT Server 4.0 and that there will NOT be an upgrade for the application in the next year.
2. A Windows NT Server 4.0 computer named IR-SR01 in the New York office hosts a mission-critical, line of business application. This application is accessed by users from all departments and offices in the company. The application vendor currently does not support running the application on any operating system other than Windows NT Server 4.0.
3. Calais is the only office that runs client computers on Microsoft Windows NT 4.0. To minimize WAN traffic between the PDC emulator and the legacy computers option B makes the most sense.

Incorrect answers:

A: New York has the most NT 4.0 users, so placing it there would minimize traffic over the WAN lines. However, there is a legacy operating system in operation at Calais and this has to be taken into consideration. Normally, if the location of legacy client computers is not a consideration, then the PDC emulator would need to be placed in the site with the largest number of users.

C, D, E, F are incorrect. Since this would not be required and will not minimize WAN traffic.

Reference:

Jerry Honeycutt; Introducing Microsoft Windows Server 2003, Microsoft Press, Redmond, Washington, Chapter 16.

QUESTION 71

You need to design the service site topology and therefore need to implement the appropriate Active Directory sites to meet the requirements of the new International Retailers network.

What should you do? (Each correct answer presents part of the solution. Choose all that apply.)

- A. Implement a New York site.
- B. Implement a Calais site.
- C. Implement a Perth site.
- D. Implement a Rio de Janeiro site.
- E. Implement a Sao Paulo site.
- F. Implement a Durban site.

Answer: A, B, C, E, F

Explanation: Each office except for the Rio de Janeiro office must be configured as a separate site. The Rio de Janeiro site will not have any servers and must make use of the

Sao Paulo office domain controllers.

Incorrect answer:

D: The Rio de Janeiro office does not have any servers which mean that you cannot implement it as a site.

Reference:

Jill Spealman, Kurt Hudson, and Melissa Craft; MCSE Self-Paced Training Kit (Exam 70-294); Planning, Implementing, and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Chapter 12, pp. 12-14.

William Boswell; Inside Windows Server 2003, Addison Wesley, Chapter 8
Microsoft Windows Server 2003 Deployment Kit: Designing the site-topology

QUESTION 72

You are designing the DNS service implementation to meet the business and technical requirements.

What should you do?

- A. Configure a forest root zone named international.com on a DNS server in New York.
- B. Configure a private root zone on a DNS server in New York.
- C. Configure a DNS server in each branch office to forward queries for names of all non-local hosts to a DNS server in New York.
- D. Configure DNS servers in each branch office to forward queries for the names of hosts in other offices to the DNS servers in their respective offices.

Answer: A

Explanation: The new network must consist of a single Active Directory domain, therefore only one zone is required to support that domain. You need to configure a forest root zone. In this type of zone, the DNS database is stored within Active Directory. All DNS servers in an Active Directory-integrated zone are considered primary servers because the DNS information actually becomes part of the Active Directory database; any DNS server can be updated and any of them can resolve client requests. Active Directory is responsible for replicating zone information between DNS servers, often making replication quicker and making it a part of Active Directory management instead of a separate management practice

1. Centralized control over Active Directory must be maintained by the network administrator in the New York office. Limited access to Active Directory will be given to the IT teams in the branch offices.
2. The DNS infrastructure must be fault tolerant and secure.
3. A domain-naming strategy must be identified that reduces administrative complexity and is intuitive to other users.

Incorrect answers:

B: A private root zone is most appropriate in a case where there are many domains in a multi-layered hierarchy. In this scenario there is no need to create a private root zone since all internal DNS servers will host the same zone and, consequently will have the ability to resolve names of any hosts in the internal network.

C: To resolve names of non-local hosts / Internet names, the internal DNS servers can

either query the root DNS servers or forward queries to external DNS servers, such as those of the ISP.

D: It is not necessary to configure the internal DNS servers to forward queries for names of internal non-local hosts to each other because all internal DNS servers will host the same zone and will therefore be able to resolve the name of any host on the internal network.

Reference:

Walter Glenn, and Michael T. Simpson; MCSE 70-297 Training Kit - Designing a Windows server 2003 Active Directory and Network Infrastructure, Chapter 1, pp. 1-24.

QUESTION 73

You need to design a plan for maintaining the WINS infrastructure on the new Windows Server 2003 Active Directory environment. There are therefore a few factors that you need to keep in mind that requires that International Retailers maintain the WINS infrastructure.

What are these factors? (Choose TWO.)

- A. The current client operating systems.
- B. The current server operating systems.
- C. PPTP is used as VPN client access method.
- D. The installation of Active Directory client software.

Answer: A, B

Explanation: IR-SR01 will not be upgraded due to the mission critical application. Until the upgrade of the client computers to Windows XP Pro takes place, there are still several that are running pre-Windows 2000 operating systems.

As long as there are computers running versions of Windows older than Windows 2000, there will be a need for WINS.

1. A Windows NT Server 4.0 computer named IR-SR01 in the New York office hosts a mission-critical, line of business application. This application is accessed by users from all departments and offices in the company. The application vendor currently does not support running the application on any operating system other than Windows NT Server 4.0.

2. The Calais office runs the Microsoft Windows NT 4.0 Workstation operating system.

Incorrect Answers:

C: Point-to-Point Tunneling Protocol (PPTP) is a data-link layer protocol used to provide secured communications for virtual private network (VPN) connections.

D: In environments that include any combination of Windows 95, Windows 98, Windows Me, and Windows NT 4.0, the Active Directory client software will need to be installed on these systems in order to participate in an Active Directory domain.

Reference:

Walter Glenn, and Michael T. Simpson; MCSE 70-297 Training Kit - Designing a Windows server 2003 Active Directory and Network Infrastructure, Chapter 7, pp. 7-2.
Dan Holme, and Orin Thomas; MCSA/MCSE Self-Paced Training Kit: Upgrading Your Certification to Microsoft Windows Server 2003: Managing, Maintaining, Planning, and

Implementing a Microsoft Windows Server 2003 environment: Exams 70-292 and 70-296, Chapter 4, pp. 4-53.

QUESTION 74

You need to create the physical design for the Active Directory and Network infrastructure. This means that you need to set up the internal network for name resolution purposes. You are designing a DNS implementation strategy for the Calais office.

What should you do?

- A. Create an Active Directory-integrated zone named international.com. Configure all computers in Calais to use DC4 as their DNS server.
- B. Create an Active Directory-integrated zone named calais.international.com. Configure all computers in Calais to use DC4 as their DNS server.
- C. Create a standard primary zone named calais.international.com. Configure all computers in Calais to use DC3 as their DNS server.
- D. Create a standard primary zone named calais.international.com. Configure all computers in Calais to use DC4 as their DNS server.

Answer: A

Explanation: In the Network Infrastructure Section it states: "One domain controller in each of the current offices will have the DNS service installed. DNS name resolution traffic must be minimized over all WAN links".

The local server for Calais is DC4, which is also a domain controller. Also, seeing as how DC4 is a local server, it would minimize traffic over its WAN link.

Incorrect Answers:

- B: calais.international.com is not a valid domain name.
- C: DC3 is located in Perth, so this option would increase traffic on the WAN lines.
- D: The master copy of the DNS database resides in a standard ASCII text file, in this zone. Only this primary zone can be directly modified.

Reference:

Walter Glenn, and Michael T. Simpson; MCSE 70-297 Training Kit - Designing a Windows server 2003 Active Directory and Network Infrastructure, Chapter 1, pp. 1-24.
The Microsoft Windows Server 2003 Deployment kit: Deploying DNS - integrating with other Windows Server 2003 services.

QUESTION 75

You must identify network topology and performance levels for the International Retailers network. You need to implement the appropriate strategy to meet the business and technical requirements.

What should you do?

- A. An Internet Authentication Service (IAS) Server must be installed in each office.
- B. Configure the VPN servers on the network to be IAS servers.
- C. Redundant site links should be created.

- D. A cost of 1 should be assigned to all site links.
- E. A cost of 100 should be assigned to all site links.

Answer: C

Explanation: The communication between computers in different sites/offices will occur via VPN. These VPN connections are established over the Internet and form a full mesh of virtual WAN links. Site links are logical objects that represent physical connectivity between sites. Active Directory replication and communication rely on site link topology. By default a single site link is created that includes all existing sites. But this default configuration does not allow preferable routes for Active Directory-related traffic to be specified. Therefore you need to create redundant site links.

1. The new WAN infrastructure must provide fault tolerance for inter-site communications in the event of a single domain controller failure.

1. The new WAN infrastructure should also allow inter-site traffic to be directed along specific routes between sites.

2. Name resolution must occur within the sites since we should strive to minimize name resolution traffic across the WAN links.

Incorrect answers:

A: Internet Authentication Service (IAS) Server is Microsoft's industry standard for the implementation of Remote Authentication Dial-In User Service (RADIUS). A RADIUS server is a server that authenticates, authorizes, and performs accounting functions when a connection attempt is made from a remote access client. It is also a network access server (NAS) that is running IAS. A RADIUS client can be a dial-up server, VPN server, or a wireless access point (AP). However, there is no need for an IAS server in each office.

B: All VPN servers have to be IAS clients not servers.

D, E: Site-link costs are numeric values representing the relative preference among site links. Assign a cost of what ever value will prevent you from implementing preferable routes for inter-site traffic, besides there is only one default-created site link.

Reference:

Walter Glenn, and Michael T. Simpson; MCSE 70-297 Training Kit - Designing a Windows server 2003 Active Directory and Network Infrastructure, Chapter 10, pp. 10-38.

Microsoft Windows Server 2003 Deployment Kit: Designing and Deploying Directory and Security Services: Designing a Site Topology

QUESTION 76

You are designing a DNS infrastructure to meet the Internet name resolution requirements.

What should you do?

- A. Create a standard primary zone on all DNS servers.
- B. Create an Active Directory-integrated zone on a DNS server on New York.
- C. Configure all DNS servers to use forwarders. Specify the IP address of the DNS server at the local ISP.

D. Recursion on all DNS servers must be disabled.

Answer: C

Explanation: Since all clients will use their local DNS servers for name resolution, they will need to have Forwarders enabled on the DNS servers for Internet Host Name resolution.

If your organization is connected to the Internet by means of a slow wide area link, you can optimize name resolution performance by channeling all DNS queries through a forwarder.

Incorrect answers:

A: There will be no requirement to create a standard primary root zone on the DNS servers.

B: The zone should include the entire network and not just the New York office.

D: You should not disable recursion on the DNS servers; rather you should configure them to use forwarders.

Reference:

J. C. Mackin, and Ian McLean; MCSA/MCSE self-paced training kit (exam 70-291): Implementing, managing, and maintaining a Microsoft Windows Server 2003 network infrastructure, Chapter 5, pp. 5-3 to 5-7.

QUESTION 77

You need to create the physical design for the Active Directory and Network infrastructure and therefore have to design the IP addressing scheme for the new Sao Paulo office.

Which network address or addresses are valid for the Sao Paulo office? (Choose all that apply)

- A. 10.10.10.0/24
- B. 172.16.10.0/27
- C. 131.15.0.0/24
- D. 169.254.10.0/25
- E. 192.168.10.0/28
- F. 200.200.200.0/24

Answer: A, B, E

Explanation: Private addresses are confined to specific ranges that can be used by any private network but that cannot be seen on the public Internet. For example, a user connecting computers in a home TCP/IP network does not need to assign a public IP address to each host. The user instead can take advantage of the address ranges shown in the table to provide addresses for hosts on the network.

Incorrect Answers:

C, D: The case study says that the IT staff in the Rio de Janeiro office will manage users in the Sao Paulo office because Sao Paulo will not have any servers installed. It also says that a VPN server will provide NAT services, which enables a local-area network (LAN)

to use one set of Internet Protocol (IP) addresses for internal traffic and a second set of addresses for external traffic.

F: You may not make use of public IP addresses. And you also cannot use APIPA addresses for the Sao Paulo branch office because it will not be routable.

Reference:

J. C. Mackin, and Ian McLean; MCSA/MCSE self-paced training kit (exam 70-291): implementing, managing, and maintaining a Microsoft Windows Server 2003 network infrastructure, Chapter 2, pp. 2-7 to 2-8.

Dan Holme, and Orin Thomas; MCSA/MCSE Self-Paced Training Kit (Exam 70-290): Managing and Maintaining a Microsoft Windows Server 2003 Environment, Glossary, pp. G-14.

Microsoft Windows Server 2003 Deployment Kit: Deploying network services - Designing a TCP/IP Network.

QUESTION 78

You are designing the migration path to Active Directory to meet the business and technical requirements.

What should you do?

- A. All existing Windows NT 4.0 domains should be upgraded.
- B. Upgrade only the New York domain and restructure all other Windows NT 4.0 domains.
- C. Create a new forest and migrate all existing domains into the new forest.
- D. Create a new forest and migrate the New York domain into the new forest. Then restructure all other Windows NT 4.0 domains.

Answer: B

Explanation: An Active Directory can support millions of objects in a single domain. The WAN bandwidth in this case study that can be used for Active Directory-related traffic should be able to support up to 100,000 users in a single domain. The local IT team's responsibility of resetting passwords, and performing routine maintenance. There is no indication in the scenario that data or service isolation or domain-level autonomy are required at the branch offices. The case study does not call for multiple Active Directory domains or forests. And there are less than 550 user accounts which all reside in the New York MUD. Therefore a single domain forest will be the solution.

1. All user accounts reside in and are maintained in the master user domain (MUD) in New York.

Incorrect answers:

A: This will not be possible since Calais will still be reliant on the legacy software due to their operating system being Microsoft Windows NT 4.0 Workstation. The Windows NT 4.0 domain controllers cannot be upgraded. It should rather be decommissioned.

C: Creating a new forest and then migrating all existing domains into the new forest

D: Creating a new forest would be valid, but this solution would require more effort than the in place upgrade of the New York domain.

Reference:

Microsoft Windows Server 2003 Deployment Kit - upgrading Windows NT 4.0 Domains to Windows Server 2003 Active Directory.

Topic 7, Certkiller .com, Scenario

Certkiller .com Background

Certkiller .com is the world leading producer and manufacturer of genuine quality approved hiking, skydiving and scuba diving equipment. Certkiller .com has 10 retail outlets throughout United States.

Certkiller .com Physical Location

Certkiller .com has its headquarters located in Miami. Certkiller .com has additionally opened five branch offices to meet the supply demands of the customers. The branch offices are located in the locations below:

1. Los Angeles
2. Washington
3. New York
4. New Orleans
5. Denver

Certkiller .com has each Branch office managing at least 2 retail outlets.

Certkiller .com Planned Changes

Certkiller .com has plans for the future which requires upgrading the network to make provision for future expansion of the outdoor product line. Certkiller .com has planned for the first upgrade to be performed in two years.

Certkiller .com Business Processes

Certkiller .com's head office in Miami is responsible for managing the five branch offices. Certkiller .com additionally has the branch offices managing their own respective retail outlets. Certkiller .com considers it imperative that the larger outlets have managers who are responsible for daily reporting. Certkiller .com has provided the larger retail outlet managers a desktop computer for creating the reports.

Certkiller .com has a group of network administrators in the Miami main office responsible for controlling all network resources and access to the resources.

Certkiller .com has recently retained two network employees per branch office to assist the administrative group by performing tasks from the branch office whenever necessary.

Certkiller .com makes use of a point-of-sale (POS) application that the retail outlet employees use for selling the merchandise to the public. Certkiller .com has the application running on servers that run Windows NT 4.0 Terminal Server Edition.

Certkiller .com has not given the network retail employees access to any other applications.

Certkiller .com has the network employees in the Miami main office and branch offices working decent shifts between the hours of 8:00 A.M and 5:00 P.M, Monday through Friday. Certkiller .com has also recently requested that the network administrators are required to work on weekends to support the retail outlets. Certkiller .com are also giving the network retail workers shifts, the two shifts the retail employees are working are between the hours of 6:00 A.M and 11.00 P.M.

Certkiller .com Infrastructure

Certkiller .com Directory Services

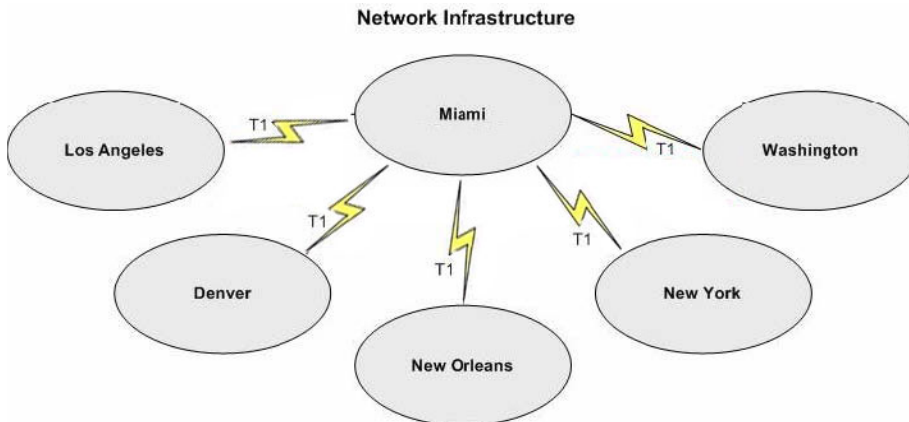
The Certkiller .com network consists of a single Windows NT 4.0 Domain named Certkiller . Certkiller .com has recently placed one PDC and Three BDC's in the Miami main office.

Certkiller .com has additionally deployed a BDC to each branch office. Certkiller .com has ensured that the Domain Controllers are not used for any other network service.

Certkiller .com has named each of the groups according the function of the Group.

Certkiller .com Network Infrastructure

The Certkiller .com network connections between Miami office and the branch offices are shown in the Network Infrastructure exhibit below:



The Certkiller .com Miami main office and branch offices all have 100-Mbps Ethernet network equipment. Certkiller .com has given the retail outlets associated with the branch offices a fractional T1 line with a committed rate of 256 kbps or greater.

Certkiller .com's WAN links are always reliable. Certkiller .com has reached an agreement with the telecommunications provider to have any WAN failure resolved within one hour. Certkiller .com currently has enough bandwidth and seems to be sufficient during business hours.

Certkiller .com's Miami main office and branch offices all have servers running Windows NT Server 4.0, Terminal Server Edition. Certkiller .com has the number of servers per office based on the number of retail outlets connecting to the Miami main office or branch offices. The number of terminals at the retail outlets is also a factor in the number of servers. The server distribution is shown in the following table:

Office	Users	Outlets	Terminal Servers	Terminals	File Servers
Miami	300	90	7	172	3
Los Angeles	100	80	6	150	1
Washington	100	60	4	115	1
New York	100	60	4	115	1
New Orleans	180	75	5	144	1
Denver	150	75	5	144	1

Certkiller .com makes use of only one of the terminal servers in Miami, running Windows NT Server 4.0, as the dedicated terminal server to the finance department.

Certkiller .com has the remaining five terminal servers available for use by the retail outlets. Certkiller .com makes use of no additional servers or operating systems. The Certkiller .com network has successfully tested all the company software on computers that run Windows Server 2003 and Windows XP Professional.

The Certkiller .com network existing hardware is shown below:

Computer	Processor	RAM	Hard Drive
Domain Controller	Pentium 133 MHz	64 MB	1.6 GB
Terminal Server	Pentium 133 MHz	96 MB	2 x 2.0 GB
Client computer	Pentium 100 MHz	32 MB	1.0 GB

Certkiller .com Problem Statements

Certkiller .com wants to have the following business problems considered:

1. Certkiller .com has recently noticed that the employees in the branch offices often log on to install software using local computer accounts rather than domain accounts. The Certkiller .com network retail employees have also recently started reporting that network performance is slow.
2. Certkiller .com also realized that the IP addresses are configured manually. Certkiller .com has resolved that this particular problem leads to incorrectly configured or duplicate addresses on the network.
3. The Certkiller .com network employees have also expressed concerns about losing their installed application, data and profiles during the changeover.

Certkiller .com Executives

Certkiller .com Chief Executive Officer

Certkiller .com has planned the expansion to occur as a phased process over the next two years. Certkiller .com will make use of the acquired profits to achieve this.

Certkiller .com also has planned for a new company policy to be enforced to ensure that all company employees have access to similar network services when they are at work.

Certkiller .com also recently conducted a market survey that shows Certkiller .com requires establishing a web presence to remain competitive.

Certkiller .com Chief Information Officer

Certkiller .com's original network was implemented about three years ago. The only change Certkiller .com has made was acquiring the upgraded WAN links last year. The upgrade Certkiller .com acquired did not solve the performance problems experienced by the retail outlets. Certkiller .com has since then established that the performance related problems might be caused by hardware.

Certkiller .com is expecting lots of growth with the customers with the introduction of the new product line. Certkiller .com has decided that this would be reason enough to ensure that terminals are upgraded to provide for the increased connection to our servers from the retail outlets. Certkiller .com has no plans for adding a vast number of terminals.

Certkiller .com has made substantial profit which is available for use for this project.

Certkiller .com envisages a plan where the network will not have to be upgraded for a further six years without major changes.

Certkiller .com Network Administrator

The network administrators at Certkiller .com have noticed in System Monitor most of the servers are running high processor and memory utilization. The network administrators of Certkiller .com currently instruct the retail outlets on which terminal server to connect to, for achieving manual load balancing.

The network administrators at Certkiller .com configured the individual users in the retail outlets to have access to personal data in the new environment. Certkiller .com network currently has no DNS servers or Internet access available.

The newest member of the Certkiller .com network administrators has noticed that the current management of our groups is incorrect. The current Certkiller .com network is only using local groups for the assignment of permissions. This particular process is done

by using groups that contain all the users located in the branch offices. Certkiller .com knows that they could be more specific and focus on the function of the group within the office. The Certkiller .com network administrators know that the users can be managed very easily, because the users make use of the passwords "password". Certkiller .com additionally noticed that only certain users change their password and this has caused a need for more complex passwords to be implemented.

The network administrators also stated that certain network users at the retail outlets leave the terminal connected to the application for weeks without disconnecting. The result of the actions is that the backup of the application data fails. The network users of the Certkiller .com branch offices additionally leave their computers on for long periods of time.

Certkiller .com is in the process of planning implementation of a naming strategy used to identify users by first name, followed by the first character of their surname.

Certkiller .com wants to have the Group names indicate the department, as well as "GG" for global groups or "UG" for universal groups. Certkiller .com network administrators want the Domain local groups to be identified by the type of access they receive.

Certkiller .com Retail Manager

The Certkiller .com network retail manager has recently expressed his concern about the network gradually becoming slower. The Certkiller .com network retail manager also noted that the retail outlets do not have access to e-mail and the Internet.

The entire network retail employees users make use of the same username and password to connect to the terminal server. The network Retail Manager knows that this will result in the network not having any privacy. The Certkiller .com network additionally cannot have a respective desktop background. The Certkiller .com network employees in the branch offices have the latest games and hacking software on their computers that we are not able to access.

Certkiller .com Business Requirements

Certkiller .com Business Drivers

The Certkiller .com network wants to have the following business requirements considered:

1. The Certkiller .com network decided that they need to establish a Web site, named [www.Certkiller .com.com](http://www.Certkiller.com.com), to enable customers to search for the retail outlet nearest to them.
2. Certkiller .com also plans to make use of an online ordering system that must be established, allowing customers to order company merchandise online.

Certkiller .com Organizational Goals

The Certkiller .com network wants to have the following organizational requirements considered:

1. Certkiller .com plans to have the retail outlets expanded over the next two years to provide seating and allow for increased business. Certkiller .com has additional plans for the future expansion which include providing customers with Internet access while they are having fun in the store.
2. Certkiller .com wants to have a manager appointed in each retail outlet who will be responsible for improving customer service. The new customer services manager's desktop computer will be used by other staff members to access the Internet and their e-mail. The users will be required to have their own passwords on the computer.

Certkiller .com Security

The Certkiller .com network wants to have the following security requirements considered:

1. The Certkiller .com network wants all security settings to be equal to or more restrictive than the default Windows Server 2003 settings.
2. Certkiller .com additionally wants all the users to be forced to change their passwords at least once a month as a part of the requirements.
3. The Certkiller .com network users with desktop computers should no longer be allowed to log on to the local computer as an administrator.
4. Certkiller .com wants to have the duration of logon hours must be strictly enforced.
5. The Certkiller .com network management has decided that the users should not be allowed to shutdown the terminal servers.

Certkiller .com Technical Requirements

Certkiller .com Active Directory

The Certkiller .com network wants to have the following active directory requirements considered:

1. Certkiller .com requires having the Active Directory design specify how the management of user and group permissions will be established and maintained.
2. The Certkiller .com management wants to have the new design overcome the existing performance issues and provide all employees with e-mail and Internet access.
3. Certkiller .com additionally wants to have the employees in the retail outlets allowed to use these services only while on their lunch or coffee breaks. The Certkiller .com network employees will be able to use only their own user accounts for network access.
4. Certkiller .com network wants to have the new Active Directory design to facilitate the use of Group Policy to control all user accounts within a branch office.
5. Certkiller .com additionally wants the Group Policy settings for users in the branch offices to be different from the Group Policy settings for users in the retail outlets.
6. The Certkiller .com network user accounts for users in the finance department should be managed separately.

Certkiller .com Network Infrastructure

The Certkiller .com network wants to have the following network infrastructure requirements considered:

1. Certkiller .com is planning to establish a new T1 WAN link from the Miami office to the ISP will be installed.
2. Certkiller .com network wants to have all the server computers to have Windows Server 2003 installed. The Certkiller .com network also wants to have all desktop computers have Windows XP professional installed. You are required to achieve this as quickly as possible.
3. Certkiller .com network wants to have all terminal servers in a single office to be configured to use Network Load Balancing.
4. The Certkiller .com network has decided to have all the network users should use roaming profiles to ensure consistent desktop appearance and access to applications.
5. The Certkiller .com network terminal server user profiles should be stored on a network shared folder. Certkiller .com considers it imperative that Redundancy be configured for all other servers. The Certkiller .com network additionally requires that the DNS infrastructure be secured by assigning permissions for the zone data.

Topic 7, Certkiller .com (12 Questions)

QUESTION 79

You work as the network administrator at Certkiller .com. You are in the process of creating and designing a DNS service implementation. You have recently received instruction to start designing and creating the Logical Design for a Network Services Infrastructure. The solution you are busy with will be used for configuring a newly installed Windows Server 2003 computer to meet the Active Directory DNS requirements of Certkiller .com. You are required to select which way to configure the server computer.

What should you do?

- A. You should configure the server with a stub zone for the Certkiller .com.com DNS zone hosted by the ISP.
- B. You should configure the server as a secondary DNS server for the Certkiller .com DNS zone hosted by the ISP.
- C. You should configure the server as a caching-only DNS server.
- D. You should configure the server as the primary DNS server for the Certkiller .com.com DNS zone.

Answer: D

Explanation: You should remember that the primary DNS servers store original source data for zones in the scenario. You are capable of implementing the primary zones two ways using Windows Server 2003:

1. You are able to create either standard primary zones which stores the zone data in a text file
2. You could additionally implement the DNS zone as an Active Directory-integrated zone which makes use of the Active Directory database to store the zone data.
3. Certkiller .com is in the process of planning implementation of a naming strategy used to identify users by first name, followed by the first character of their surname. Certkiller .com wants to have the Group names indicate the department, as well as "GG" for global groups or "UG" for universal groups. Certkiller .com network administrators want the Domain local groups to be identified by the type of access they receive.

Incorrect Answers:

- A: You should not consider configuring a stub zone on the DNS server because a stub zone is a copy of a zone containing only the resource records required to identify an authoritative DNS server.
- B: In the scenario you should not make use of a secondary DNS server because the secondary server is authoritative backup server for the primary DNS server.
- C: In the scenario you should not make use of a caching-only server because the purpose of this particular server is to cache queries so that future requests for the same resource record are done instantly.

Reference:

Dan Holme, and Orin Thomas, MCSA/MCSE Self-Paced Training Kit: Upgrading Your

Certification to Microsoft Windows Server 2003: Managing, Maintaining, Planning, and Implementing a Microsoft Windows Server 2003 environment: Exams 70-292 and 70-296, Microsoft, Chapter 8, pp. 8-25.

Walter Glenn, and Michael T. Simpson, MCSE 70-297 Training Kit - Designing a Windows server 2003 Active Directory and Network Infrastructure, Chapter 6, pp. 6-26 and 6-31.

QUESTION 80

You work as the network administrator at Certkiller .com. You are in the process of creating and designing the Conceptual Design by gathering and analyzing the Technical and Business requirements. You have recently received instruction to start designing the Active Directory infrastructure of Certkiller .com. The solution you are busy designing should meet the business and technical requirements of Certkiller .com. You are required to select which structure should be suitable for use. What should you do?

- A. You should make use of a single forest structure with two trees each containing a single domain
- B. You should make use of a two forests structure each containing two trees, with a single domain in each tree
- C. You should make use of a single forest structure with one tree and two domains
- D. You should make use of a two forests structure each containing a single tree and a single domain
- E. You should make use of a single forest structure containing one tree, and one domain.

Answer: E

Explanation: In the scenario you should configure the new structure as a single-domain model. You should remember that in the single domain model all objects are located within the same security boundaries. This means you are not required to plan trust relationships with other domains or implementing cross-domain authentication and permissions.

1. Certkiller .com has plans for the future which requires upgrading the network to make provision for future expansion of the outdoor product line. Certkiller .com has planned for the first upgrade to be performed in two years
2. The Certkiller .com network wants all security settings to be equal to or more restrictive than the default Windows Server 2003 settings
3. Certkiller .com additionally wants all the users to be forced to change their passwords at least once a month as a part of the requirements

Incorrect Answers:

A, B, D: In the scenario you are not required to implement multiple forests because this should be done only when linking two separate existing organizations. You should remember that all security settings should be equal to or more restrictive than the default Windows Server 2003 settings.

C: In the scenario you are not required to implement different domain-level security policies as the network users are required to have all security settings equal to or more

restrictive than the default Windows Server 2003 settings

Reference:

Walter Glenn, and Michael T. Simpson, MCSE 70-297 Training Kit - Designing a Windows server 2003 Active Directory and Network Infrastructure, Chapter 3, pp. 3-2 to 3-12.

QUESTION 81

You work as the network administrator at Certkiller .com. You are in the process of creating the Logical Design for an Active Directory Infrastructure. You have recently received instruction to start designing a group management strategy for users in the finance department. In the solution you are busy designing you are required to identify the appropriate changes needed for the current group management strategy. You are required to additionally accomplish this goal using the minimum number of groups.

What should you do?

- A. The finance users should be added to the financeGG group. The financeGG group should then additionally be added to the financeData group which has the necessary permissions assigned.
- B. The finance users should be added to the financeGG group. Add the financeGG group should then additionally be added to the financeUG group and the financeData group which has the necessary permissions assigned.
- C. The finance users should be added to the financeData group which has the necessary permissions assigned.
- D. The finance users should be added to the financeGG group which has the necessary permissions assigned.

Answer: D

Explanation: You should consider making use of this option in the scenario since you are required to accomplish the task using the minimum number of groups. By adding the finance users to the financeGG group you are adhering to the scenario requirements.

1. Certkiller .com is in the process of planning implementation of a naming strategy used to identify users by first name, followed by the first character of their surname. Certkiller .com wants to have the Group names indicate the department, as well as "GG" for global groups or "UG" for universal groups. Certkiller .com network administrators want the Domain local groups to be identified by the type of access they receive

Incorrect Answers:

A, B, C: In the scenario you should not consider using these answers because these options do not make use of the minimum number of groups as required in the particular objective. The options can be used on the network but would require additional groups increasing the administrative overhead.

QUESTION 82

You work as the network administrator at Certkiller .com. You have recently

received instruction to start designing the network security policy solution of Certkiller .com. You are in the process of creating and designing the network security policy solution which must adhere to the Certkiller .com network corporate security policy. You are additionally required to select which actions should be performed? (Choose all that apply.)

- A. A policy should be enabled which forces users to log off when their logon hours expire
- B. The retail outlets network users should be allowed to log on between the hours of 6:00 A.M and 11:00 P.M., daily.
- C. A password policy should be configured that requires strong passwords
- D. The branch offices network users should be allowed to log on between the hours of 8:00 A.M and 5:00 P.M., Monday through Friday
- E. A password policy should be configured which requires all users to change their passwords once a month.

Answer: A B, C, D, E

Explanation: In the scenario you should consider taking all the actions mentioned because the actions all adhere to the Certkiller .com network security policy. By taking the actions in the answer you ensure that your design enforces the corporate security policy of Certkiller .com.

1. The Certkiller .com network administrators know that the users can be managed very easily, because the users make use of the passwords "password". Certkiller .com additionally noticed that only certain users change their password and this has caused a need for more complex passwords to be implemented
2. The network administrators also stated that certain network users at the retail outlets leave the terminal connected to the application for weeks without disconnecting. The result of the actions is that the backup of the application data fails. The network users of the Certkiller .com branch offices additionally leave their computers on for long periods of time
3. Certkiller .com wants to have the duration of logon hours must be strictly enforced
4. Certkiller .com additionally wants all the users to be forced to change their passwords at least once a month as a part of the requirements
5. Certkiller .com has the network employees in the Miami main office and branch offices working decent shifts between the hours of 8:00 A.M and 5:00 P.M, Monday through Friday. Certkiller .com has also recently requested that the network administrators are required to work on weekends to support the retail outlets. Certkiller .com are also giving the network retail workers shifts, the two shifts the retail employees are working are between the hours of 6:00 A.M and 11.00 P.M.

QUESTION 83

You work as the network administrator at Certkiller .com. You are in the process of creating the conceptual design by gathering and analyzing the technical and business requirements. You have recently received instruction to start analyzing the impact of Active Directory on the existing technical environment when migrating.

The migration solution you are designing should meet the business and technical requirements of Certkiller .com
What should you do?

- A. A new Windows NT 4.0 BDC should be installed and configured. The BDC should be promoted to a PDC. The PDC should then be upgraded to Windows Server 2003.
- B. A new Windows 2000 Server Active Directory domain should be created. A two-way trust relationship should be established with the Certkiller domain. The Active Directory Migration Tool (ADMT) should be used to migrate all user and computer accounts.
- C. The Certkiller BDC should be upgraded to Windows Server 2003. The PDC should then be upgraded to Windows Server 2003.
- D. An existing domain controller should be upgraded to Windows Server 2003. A two-way trust relationship should be established with the Certkiller .com domain.

Answer: A

Explanation: In the scenario you are required to design a strategy which will allow the migration to take place without problems. By taking the actions in the scenario you ensure that the network users will not lose their applications and data profiles.

1. The Certkiller .com network employees have also expressed concerns about losing their installed application, data and profiles during the changeover

Incorrect Answers:

B: This option should not be used in the scenario because the Certkiller .com network requires running a single Active Directory domain. This particular option does not meet the scenario objective.

C: In the scenario you should not consider using this option because you should always first upgrade the PDC and then you can remove or upgrade all the BDC in the domain.

D: This option should not be considered for use in the scenario because not all of the network servers meet the minimum requirements for installing Windows Server 2003.

Reference:

William Boswell: Inside Windows Server 2003, Addison Wesley, Chapter 9.

QUESTION 84

You work as the network administrator at Certkiller .com. You are in the process of creating the Logical Design for an Active Directory Infrastructure. You have recently received instruction to start designing a strategy for Group Policy Implementation. The solution you are designing for implementing Group Policy objects (GPOs) should meet the business and technical requirements of Certkiller .com
What should you do?

- A. New GPOs should be created to match the number of organizational units (OUs). These GPOs should be configured to enforce software restriction policies. This GPO should be linked to its respective OU.
- B. One new GPO should be created to enforce software restriction policies. This GPO should be linked to all organizational units (OUs).

- C. One new GPO should be created to enforce software restriction policies. This GPO should be linked to the appropriate organizational unit (OU).
- D. One new GPO should be created to enforce software restriction policies. This GPO should be linked to the domain.

Answer: D

Explanation: In the scenario it is stated that the network retail employees install the latest games and hacking tools. To prevent the network users from installing unauthorized applications you should make use of this option.

1. The entire network retail employees users make use of the same username and password to connect to the terminal server. The network Retail Manager knows that this will result in the network not having any privacy. The Certkiller .com network additionally cannot have a respective desktop background. The Certkiller .com network employees in the branch offices have the latest games and hacking software on their computers that we are not able to access
2. Certkiller .com network wants to have the new Active Directory design to facilitate the use of Group Policy to control all user accounts within a branch office
3. Certkiller .com additionally wants the Group Policy settings for users in the branch offices to be different from the Group Policy settings for users in the retail outlets

Incorrect Answers:

A: In the scenario you should not consider making use of this option because the software restriction policies should be applied to the entire domain to ensure no unauthorized applications are installed. This particular option will only complicate the management of the policies by adding new GPOs.

B, C: In the scenario you should not consider making use of this option because the software restriction policies should be applied to the entire domain to ensure no unauthorized applications are installed.

Reference:

William Boswell: Inside Windows Server 2003, Addison Wesley, Chapter 12.

QUESTION 85

You work as the network administrator at Certkiller .com. You are in the process of creating the Logical Design for a Network Services Infrastructure. You have received additional instruction to start designing a DNS name resolution strategy for Certkiller .com. The DNS name resolution strategy you are designing should allow all users access to internal and external web sites.

What should you do?

- A. The DNS server should be configured to forward all unanswered queries to a DNS server located at the ISP.
- B. The DNS server located at the ISP should be added to the list of name servers for the Certkiller .com DNS zone.
- C. Zone transfers should be allowed to any DNS server
- D. A new stub zone should be created for the DNS zone on the DNS server

Answer: A

Explanation: In the scenario you are required to provide Internet Access to the network users of Certkiller .com. You should remember when a DNS server receives a query; it will first check to see whether it can answer the query authoritatively if not the query will be forwarded. This ensures that the network users are able to connect to the Internet.

1. The Certkiller .com management wants to have the new design overcome the existing performance issues and provide all employees with e-mail and Internet access

Incorrect Answers:

B: This option should not be used in the scenario because this will have the internal Certkiller .com name space exposed to Internet users.

C: In the scenario the network consists of a single Windows NT 4.0 domain which uses one DNS zone so there is no need to have zone transfers configured.

D: You should not consider configuring a stub zone on the DNS server because a stub zone is a copy of a zone containing only the resource records required to identify an authoritative DNS server.

Reference:

J. C. Mackin, and Ian McLean, MCSA/MCSE self-paced training kit (exam 70-291): implementing, managing, and maintaining a Microsoft Windows Server 2003 network infrastructure, Microsoft, Chapter 4, pp. 4-19 to 4-16.

QUESTION 86

You work as the network administrator at Certkiller .com. You are in the process of creating the conceptual designing by gathering and analyzing the technical and business requirements. You received additional instruction to start designing the network services infrastructure to meet the requirements of Certkiller .com. You are required to select which of the following actions to perform.

What should you do? (Each correct answer presents part of the solution. Choose TWO.)

A. Two DHCP servers should be installed and configured in Miami and two DHCP servers in each branch office.

B. On each DHCP server you should create one scope. One DHCP server should be specified to always update DNS records. The scope should then be configured to assign half of the IP addresses available to each office.

C. One DHCP server should be installed and configured in Miami and one DHCP server in each branch office.

D. Two scopes should be created on each DHCP server. One DHCP server should be specified to update DNS records only for client computers that request it. A second DHCP server should be specified to never update DNS records.

Answer: A, D

Explanation: In the scenario it is mentioned that IP addresses are entered manually causing various conflicts. The Dynamic Host Configuration Protocol (DHCP) is an

industry standard protocol that is used to allow a server automatically assign IP addresses to clients.

1. Certkiller .com also realized that the IP addresses are configured manually. Certkiller .com has resolved that this particular problem leads to incorrectly configured or duplicate addresses on the network
2. The Certkiller .com network terminal server user profiles should be stored on a network shared folder. Certkiller .com considers it imperative that Redundancy be configured for all other servers. The Certkiller .com network additionally requires that the DNS infrastructure be secured by assigning permissions for the zone data.

Incorrect Answers:

B: You should not consider making use of this option in the scenario because this will not ensure that the legacy clients are registered in DNS.

C: You should not consider making use of only one DHCP server because one of your scenario requirements states that Certkiller .com considers it imperative that Redundancy be configured for all other servers.

Reference:

Walter Glenn, and Michael T. Simpson, MCSE 70-297 Training Kit - Designing a Windows server 2003 Active Directory and Network Infrastructure, Chapter 1, pp. 1-39, 6-13.

QUESTION 87

You work as the network administrator at Certkiller .com. You are in the process of creating the Logical Design for a Network Services Infrastructure. You have recently received additional instruction to start designing a DNS name resolution strategy for the retail outlets. The solution you are designing for Certkiller .com should ensure that the existing bandwidth is used efficiently. You are required to select which actions to perform? (Choose all that apply.)

- A. On the terminal servers you should configure the DNS server service as caching-only servers.
- B. An application partition should be created to be used for DNS.
- C. A new DNS zone should be created and configure zone transfers to name servers only.
- D. You should create secondary zones for all other sites on the DNS server in each branch office.
- E. The scope of replication should be specified to be used for DNS.

Answer: B, C, E

Explanation: You should always remember in Windows Server 2003 that an incremental zone transfer (IXFR), servers keep track of, and transfer only, changes made to resource records in a particular zone. This is very useful because this particular method uses less traffic sent over the network.

1. The Certkiller .com network retail manager has recently expressed his concern about the network gradually becoming slower. The Certkiller .com network retail manager also noted that the retail outlets do not have access to e-mail and the Internet.
2. Certkiller .com has recently noticed that the employees in the branch offices often log

on to install software using local computer accounts rather than domain accounts. The Certkiller .com network retail employees have also recently started reporting that network performance is slow.

Incorrect Answers:

A: In the scenario you should not make use of a caching-only server because the purpose of this particular server is to cache queries so that future requests for the same resource record are done instantly

B: In the scenario the network is configured as a single-domain forest. Because the network uses a single domain you require maintaining only one DNS domain and a single zone for the entire network.

Reference:

Jill Spealman, Kurt Hudson, and Melissa Craft, MCSE Self-Paced Training Kit (Exam 70-294): Planning, Implementing, and Maintaining a Microsoft Windows Server 2003 Active Directory Infrastructure, Chapter 5, pp. 5-4.

QUESTION 88

You work as the network administrator at Certkiller .com. You are in the process of creating the conceptual design by gathering and analyzing the technical and business requirements. You have recently received additional instruction to start designing a strategy for installing Windows server 2003 on the new domain controllers. You are required to select which method to use?

- A. You should consider using a software installation group policy to deploy the .msi package to the required computers.
- B. You should consider configuring a domain controller and duplicate the disk image and install on the other domain controllers.
- C. You should consider using Remote Installation Services (RIS).
- D. You should consider using an unattended installation.

Answer: D

Explanation: In the scenario you should consider making use of an appropriate answer file and uniqueness database file. By making use of the answer file you ensure that you always adhere to the technical and business requirements of Certkiller .com.

1. Certkiller .com network wants to have all the server computers to have Windows Server 2003 installed. The Certkiller .com network also wants to have all desktop computers have Windows XP professional installed. You are required to achieve this as quickly as possible

Incorrect Answers:

A: In the scenario you should remember that it is impossible to deploy .msi packages to computers without operating systems to use.

B: You should not consider making use of Sysprep in the scenario because Sysprep requires an existing Active Directory infrastructure and the scenario uses Windows NT 4.0.

C: You should not consider making use of RIS in the scenario because RIS requires an existing Active Directory infrastructure and the scenario uses Windows NT 4.0.

QUESTION 89

You work as the network administrator at Certkiller .com. You are in the process of creating the physical design for an Active Directory and Network Infrastructure. You have recently received instruction to start designing an Internet connectivity strategy for Certkiller .com. The solution you are designing should ensure that all employees have Internet access. You are required to select the actions to perform at each branch office.

What should you do?

- A. An Internet Security and Acceleration (ISA) Server Computer should be installed and configured.
- B. A server running Routing and Remote Access should be installed and configured to function as a VPN server.
- C. A DNS server should be configured to function as caching-only servers.
- D. Internet Connection sharing should be configured on the terminal servers.

Answer: A

Explanation: In the scenario you should remember that the ISA server functions like a Proxy server used by the client computers to access Internet resources. The ISA server will then be responsible for performing name resolution on behalf of the ISA clients.

1. Certkiller .com plans to have the retail outlets expanded over the next two years to provide seating and allow for increased business. Certkiller .com has additional plans for the future expansion which include providing customers with Internet access while they are having fun in the store
2. Certkiller .com wants to have a manager appointed in each retail outlet who will be responsible for improving customer service. The new customer services manager's desktop computer will be used by other staff members to access the Internet and their e-mail. The users will be required to have their own passwords on the computer
3. The Certkiller .com management wants to have the new design overcome the existing performance issues and provide all employees with e-mail and Internet access

Incorrect Answers:

B: In the scenario the network users and employees do not work remotely so there is no reason to have a VPN server installed and configured.

C: In the scenario you should not make use of a caching-only server because the purpose of this particular server is to cache queries so that future requests for the same resource record are done instantly.

D: You should not configure Internet Connection Sharing (ICS) on the terminal server in the network because the ISA server provides centralized administration.

Reference:

J. C. Mackin, Ian McLean, MCSA/MCSE self-paced training kit (exam 70-291):

implementing, managing, and maintaining a Microsoft Windows Server 2003 network infrastructure, Microsoft, Glossary, p. G-26.

QUESTION 90

You work as the network administrator at Certkiller .com. You are in the process of creating and designing a DNS service implementation. You have recently received instruction to start designing and creating the Logical Design for a Network Services Infrastructure. The solution you are busy with will be used for configuring the Active Directory DNS requirements of Certkiller .com. You are required to select which actions to take to support this specific DNS infrastructure. What should you do?

- A. On the DNS server in each branch office you should configure the root hints to point to the DNS server in the main office.
- B. A delegation should be created for each branch office on the main office DNS server.
- C. You should create secondary zones for all other sites on the DNS server in each branch office.
- D. You should configure site links between the main office and branch offices.

Answer: D

Explanation:

In the scenario you are required to secure the DNS data by using permissions. You should consider implementing the DNS zone as an Active Directory-integrated zone which makes use of the Active Directory database to store the zone data.

1. The Certkiller .com network terminal server user profiles should be stored on a network shared folder. Certkiller .com considers it imperative that Redundancy be configured for all other servers. The Certkiller .com network additionally requires that the DNS infrastructure be secured by assigning permissions for the zone data

Incorrect Answers:

A, B, C: In the scenario the network is configured as a single-domain forest. Because the network uses a single domain you require maintaining only one DNS domain and a single zone for the entire network. The options used here do not comply with the network infrastructure.

Topic 8, Courseware Publishers, Scenario

Courseware Publishers Background

Courseware Publishers offers books about technical networking issues and more. Courseware Publishers operates on a Monday-through-Friday schedule.

Courseware Publishers Physical Locations

Courseware Publishers has its headquarters in Phoenix. Courseware Publishers additionally has three library branch offices in the following locations:

1. Philadelphia
2. Miami
3. Boston

Courseware Publishers recently added an additional two library satellite offices: Phoenix North and Phoenix South. Courseware Publishers has no IT staff in the satellite offices.

Courseware Publishers Planned Changes

Courseware Publishers has over the years evolved into a single business unit from four separate technical libraries in each of the cities where the Courseware Publishers offices are currently located.

Courseware Publishers has recently recognized that the use of a cohesive administrative structure will better serve the Courseware Publishers employees and better secure Courseware Publishers critical resources.

Courseware Publishers has recently received stock of new books which is on offer from Philadelphia that is available online via the Internet. Courseware Publishers has plans for the future to start offering online content from all offices, not just from Philadelphia.

Courseware Publishers Business Process

Courseware Publishers currently operated as four independent business units: Phoenix, Philadelphia, Miami, and Boston.

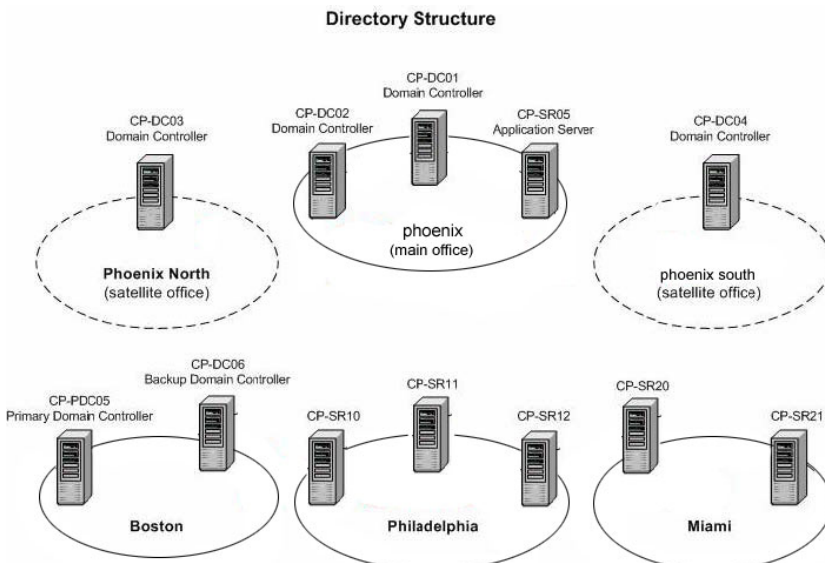
Courseware Publishers has each library branch office functioning independently with its own IT staff. Courseware Publishers has made access to the resources primarily localized to each office. The book records and courseware hosted on the servers in Phoenix are not made primarily localized.

The Courseware Publishers book records database contains the critical data. Courseware Publishers makes use of e-mail to send the critical data to the Atlanta office for entry into the book records database. The Courseware Publishers admissions department is responsible for entering the critical data. The Courseware Publishers registrar's department ensures that the critical data is accurate. Courseware Publishers are unable to update the books records database from any other location.

Courseware Publishers has already developed the online course content and is in use.

Courseware Publishers Directory Services

The Courseware Publishers servers are configured as shown in the Directory Structure exhibit:

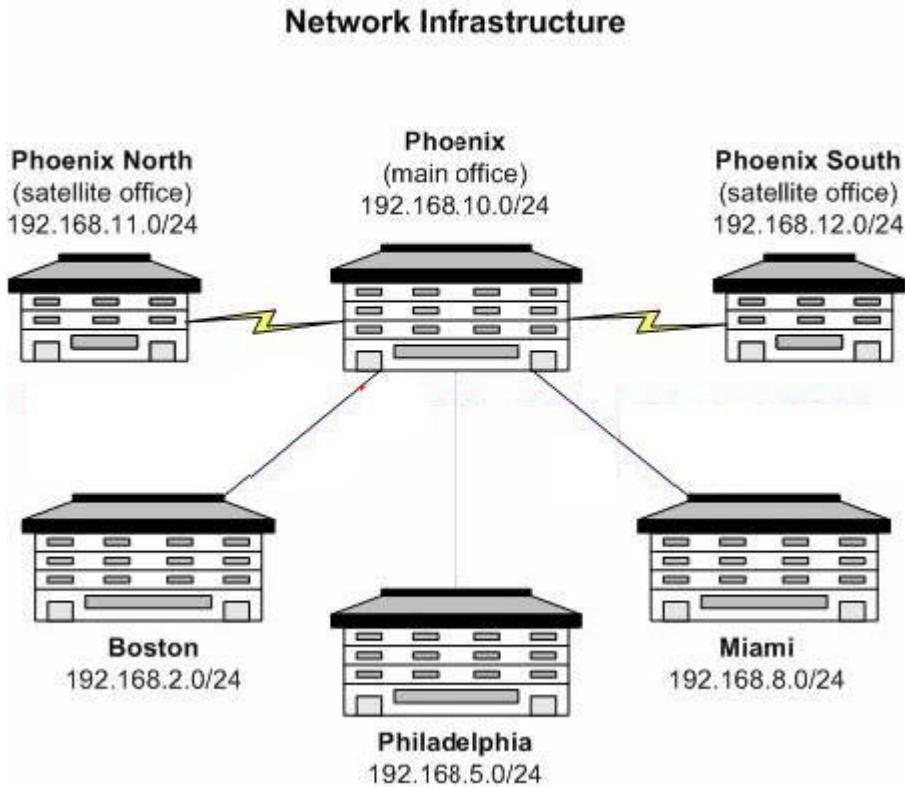


The Courseware Publishers Phoenix office currently operates a Windows 2000 Active Directory domain. The Courseware Publishers library branch offices in Philadelphia and

Miami both operate in a workgroup configuration. Courseware Publishers requires that each library branch office manage its own users and groups.

Courseware Publishers Network Infrastructure

The Courseware Publishers existing network is shown in the Network Infrastructure exhibit.



Courseware Publishers has recently discovered that WAN connections between the Phoenix main office and the library branch office Phoenix South can be unreliable. Courseware Publishers has the following configuration in the Phoenix main office and library branch offices:

1. Courseware Publishers maintains DHCP servers in Phoenix main office and the branch offices.
2. All the servers of Courseware Publishers are Pentium III 550-MHz or greater processors with at least 512 MB of memory. Courseware Publishers additionally knows that all of the offices run different client operating systems which include Windows NT Workstation 4.0, UNIX, Windows 2000 Professional, Windows 98 and Windows XP Professional
3. The Courseware Publishers librarians are running either Windows 2000 Professional or Windows XP Professional on their desktop computers. Courseware Publishers librarians who work from home make use of a UNIX client computer to access the network.

Courseware Publishers Problem Statements

Courseware Publishers requires to have the following business problems considered:

1. Courseware Publishers has recently discovered that the biggest security vulnerability is the methodology used to update the library records database in Phoenix.
2. Courseware Publishers additionally has trouble in the past, with librarians gaining

access to and altering the Library records.

3. Courseware Publishers has reason to believe that the network has been compromised because of weak passwords on Liberians computers.

The Courseware Publishers Chief Executive Officer

The Courseware Publishers network CEO has recently said that he is pleased with the performance of the staff of Courseware Publishers. The Courseware Publishers network CEO is concerned about protecting the intellectual property.

Courseware Publishers requires to have both their online curriculum and the library records databases protected. Courseware Publishers wants the focus configured so that no one outside of the organization can view or modify the information.

The Courseware Publishers Chief Information Officer

The aim of Courseware Publishers is to provide an adequate security structure for the network environment. Courseware Publishers considers the creation of a centralized network operation as important. The Courseware Publishers network CIO additionally states that he is confident in the ability of the IT staff in Phoenix to be the lead administrative role in the envisioned environment.

The network CIO of Courseware Publishers requires to have the practice of sending library information through e-mail should stop. Courseware Publishers additionally thinks that the strategy of a single, centralized student records database is valid.

The network CIO of Courseware Publishers requires to have the database be made directory-aware. This should enable the Courseware Publishers network users responsible for updating the library records will require only a single set of credentials. The Courseware Publishers network CIO also mentioned that the librarians are not receiving updated schedule information on a timely basis. Courseware Publishers wants to have this problem addressed by having the new scheduling program installed on all librarians' computers and remote computers.

Courseware Publishers Registrar, Phoenix Office

The main concern of the Courseware Publishers is about the network changes.

Courseware Publishers considers that using only one logon name to be good news. The Courseware Publishers Registrar Phoenix office additionally heard that the password used should not be a word.

The Courseware Publishers Registrar Phoenix office requires knowing how they are going to remember a password that is not a word. The Courseware Publishers Registrar Phoenix office already has a hard time remembering network passwords used. The Courseware Publishers Registrar Phoenix office was recently informed that the librarians in each location should be able to enter information in the database. The Courseware Publishers Registrar Phoenix office considers this to be their job exclusively.

Courseware Publishers Business Drivers

Courseware Publishers requires to have the following business requirements considered:

1. Courseware Publishers currently makes use of the registered domain name courseware.com. Courseware Publishers are going to focus more on the online books available in the future.

Courseware Publishers Organizational Goals

Courseware Publishers wants to have the following organizational requirements considered:

1. Courseware Publishers requires to have the library records database available to all

offices from Phoenix.

2. Courseware Publishers wants the database available during the hours of 9:00 A.M. to 8:00 P.M. Eastern Time, Monday through Friday.

3. Courseware Publishers wants to have their online books and courseware available 24 hours a day, seven days a week.

Courseware Publishers Security

Courseware Publishers wants to have the following security requirements considered:

1. Courseware Publishers wants to have their library records database server secured at all times to allow only authorized users to modify or add data.

2. Courseware Publishers wants to have the Librarians and staff in each library branch office to be the authorized personnel.

3. Courseware Publishers additionally knows that the Librarians require the necessary permissions to modify the content for the online courseware.

4. Courseware Publishers wants the Librarians to be required to make changes to the library records database of the online courseware from the LAN only.

5. Courseware Publishers wants to have their network DNS infrastructure as secure as possible. Courseware Publishers additionally requires that only the authorized network computers are capable of changing the DNS data.

6. Courseware Publishers does not want the internal namespace visible on the Internet.

Courseware Publishers Customer Requirements

Courseware Publishers requires the following customer requirements to be considered:

1. Courseware Publishers wants to ensure that remote access will be required for all Librarians accessing the business offices from home.

2. Courseware Publishers currently has certain Librarians who use UNIX client computers for remote access.

3. The Courseware Publishers Librarians will require a new scheduling application to be installed on both the office and home computers who are members of the domain.

Courseware Publishers wants the application to be used even if you are making use of a dial-up connection.

4. The Courseware Publishers network Sales representatives currently make use of Windows 98 as the operating system on their computers.

5. Courseware Publishers does not want these Windows 98 Sales computers to be upgraded in the near future. Courseware Publishers requires that you install the Active Directory client on those computers. The Courseware Publishers network has several sales representatives in all the company's offices.

6. The Courseware Publishers requires having web access to the online curriculum by the customers enrolled in the online curriculum.

7. Courseware Publishers wants to have the online web access limited to enroll Librarians only.

Courseware Publishers Active Directory

Courseware Publishers wants to have the following Active Directory requirements considered:

1. Courseware Publishers wants to have the new Active Directory structure to be used to provide a centralized method of service administration for supporting the administrative staff.

2. The new Active Directory structure will be used to provide secure access to Library.

records.

3. Courseware Publishers wants the Phoenix office to be responsible for administration of the Active Directory services.

4. Courseware Publishers requires to have the resource administration to occur in Phoenix and the branch offices.

5. The Courseware Publishers customers should not have any permission to any resource other than the online courses and books.

Courseware Publishers Network Infrastructure

Courseware Publishers wants to have the following infrastructure requirements considered:

1. Courseware Publishers currently has a limited budget therefore Courseware Publishers requires to continue working with the existing physical network. Courseware Publishers additionally wants to ensure that traffic across the WAN links are minimized

2. Courseware Publishers wants to have authorized computers in the registrar's office to require smart card support for updating the Library records database. Courseware Publishers considers it imperative that the remote access policies for Phoenix, Philadelphia, Miami and Boston be centralized.

3. Courseware Publishers requires the Phoenix, Philadelphia, Miami and Boston offices to each host DNS subdomains supporting the online courseware. Courseware Publishers additionally requires to have the UNIX Librarians to support pointer (PTR) records for several applications used from the remote computers

4. Courseware Publishers requires to have unauthorized updates of DNS records to be prevented. Courseware Publishers additionally wants to have the amount of DNS zone transfer or replication to be minimized

5. Courseware Publishers wants all the remote and client computers to have host (A) resource records in DNS.

Topic 8, Courseware Publishers (10 Questions)

QUESTION 91

You work as the network administrator at courseware.com. You are in the process of creating the Logical Design for a Network Services Infrastructure. You have recently received instruction to start designing a DNS name resolution strategy. The DNS strategy you are designing requires that you meet the business and technical requirements of Courseware Publishers.

What should you do? (Each correct answer presents part of the solution. Choose TWO.)

- A. Create Standard primary zones should be created.
- B. A dynamic reverse lookup zone should be created for each subnet.
- C. The BIND secondaries option should be enabled for each DNS server fices.
- D. A dynamic forward lookup should be created for each domain.

Answer: B, D

Explanation: In the scenario you should remember that a reverse lookup zone is a

database that is used to store a mapping of an IP address to friendly DNS domain names. You should also keep in mind that a forward lookup zone is a name-to-address database helping computers translate DNS names into IP addresses.

1. Courseware Publishers requires to have both their online curriculum and the library records databases protected. Courseware Publishers wants the focus configured so that no one outside of the organization can view or modify the information.
2. Courseware Publishers requires the Phoenix, Philadelphia, Miami and Boston offices to each host DNS subdomains supporting the online courseware. Courseware Publishers additionally requires to have the UNIX Librarians to support pointer (PTR) records for several applications used from the remote computers

Incorrect Answers:

A: In the scenario you are required to prevent the unauthorized network users from making changes to DNS data, therefore you should not use a standard primary zone.

C: In the scenario you should not consider using the BIND secondaries option as this could cause the zone to fail to load.

Reference:

James Chellis, Paul Robichaux, and Matthew Sheltz; MCSA/MCSE: Windows Server 2003 Network Infrastructure Implementation, Management, and Maintenance Study Guide, Sybex, Glossary, pp. 470 and 477,

J. C. Mackin, and Ian McLean; MCSA/MCSE self-paced training kit (exam 70-291): Implementing, managing, and maintaining a Microsoft Windows Server 2003 network infrastructure, Chapter 4, pp. 4-31.

Martin Grasdal, Laura E. Hunter, and Michael Cross; MCSE Planning and Maintaining a Windows Server 2003 Network Infrastructure: Exam 70-293 Study Guide & DVD Training System, Chapter 6, pp. 396.

QUESTION 92

You work as the network administrator at courseware.com. You have recently received instruction to configure the desktop environment for the authorized network users. You are required to ensure only authorized personnel are able to enter information into the database.

What should you consider using? (Choose all that apply.)

- A. Windows XP Professional
- B. Windows 98 second edition with Active Directory client installed
- C. Windows 98 with Active Directory client installed
- D. Windows NT Workstation 4.0 with the latest service pack and Active Directory client installed
- E. Windows 95 with USB support, and install the Active Directory client
- F. Windows 2000 Professional

Answer: A, F

Explanation: In the scenario you are required to provide centralized authentication which is achieved by making use of group policies. The operating systems which

support group policies are Windows 2000 Professional and Windows XP Professional.

1. Courseware Publishers wants to have authorized computers in the registrar's office to require smart card support for updating the Library records database. Courseware Publishers considers it imperative that the remote access policies for Phoenix, Philadelphia, Miami and Boston be centralized

Incorrect Answers:

B, C, D, E:

These desktop environments mentioned in these options should not be considered for use in the scenario because the desktop environments used do not support group policies.

Reference:

Walter Glenn, and Michael T. Simpson; MCSE 70-297 Training Kit - Designing a Windows server 2003 Active Directory and Network Infrastructure, Chapter 4, pp. 4-38 to 4-39.

QUESTION 93

You work as the network administrator at courseware.com. You are in the process of creating the Logical Design for a Network Services Infrastructure. You have recently received instruction to start designing the NetBIOS name resolution strategy for Courseware Publishers. The solution you are designing should ensure the sales representatives of Courseware Publishers are provided with adequate NetBIOS name resolution.

What should you do?

- A. WINS lookup should be enabled on the DNS server in Phoenix.
- B. WINS should be enabled on one domain controller in each office.
- C. WINS should be installed on the PDC emulator.
- D. WINS should be installed on servers in Phoenix and Boston.

Answer: B

Explanation: In the scenario it is stated that the sales representatives make use of Windows 98. The Windows 98 client computers will require NetBIOS which is provided by WINS. The scenario additionally states that there are sales representatives in all the offices.

1. All the servers of Courseware Publishers are Pentium III 550-MHz or greater processors with at least 512 MB of memory. Courseware Publishers additionally knows that all of the offices run different client operating systems which include Windows NT Workstation 4.0, UNIX, Windows 2000 Professional, Windows 98 and Windows XP Professional

2. The Courseware Publishers network Sales representatives currently make use of Windows 98 as the operating system on their computers

Reference:

J. C. Mackin, and Ian McLean; MCSA/MCSE self-paced training kit (exam 70-291): Implementing, managing, and maintaining a Microsoft Windows Server 2003 network infrastructure, Chapter 4, pp. 4-7 to 4-6.

Elias N. Khnaser, Susan Snedak, Chris Peiris, and Rob Amini; MCSE Designing Security for a Windows Server 2003 Network Exam 70-298 Study Guide, Chapter 2.

QUESTION 94

You work as the network administrator at courseware.com. You are in the process of creating the Logical Design a strategy for Group Policy implementation. You have recently received instruction to start designing a strategy to install the new scheduling application.

What should you do? (Each correct answer presents part of the solution. Choose TWO.)

- A. The scheduling application should be prevented from installing across slow WAN links.
- B. You should ensure the scheduling application can install across slow WAN links.
- C. The scheduling application package should be published to the Librarian OU.
- D. The scheduling application package should be assigned to the Librarian OU.

Answer: B, D

Explanation: You should remember that in the scenario the Librarians do not receive updated schedule information. By assigning the application to this OU you ensure that the Librarians can install the application across slow WAN links.

1. The Courseware Publishers network CIO also mentioned that the librarians are not receiving updated schedule information on a timely basis. Courseware Publishers wants to have this problem addressed by having the new scheduling program installed on all librarians' computers and remote computers.

Incorrect Answers:

- A: You should not consider using this option in the scenario because the network bandwidth might be consumed by the users when they receive the assigned application.
- C: This option should not be used in the scenario because you can not simply publish the files as this will not ensure that the application will be installed.

QUESTION 95

You work as the network administrator at courseware.com. You are in the process of creating the Logical Design for a Network Services Infrastructure. You have recently received instruction to start designing a VPN remote access authentication strategy. The solution you are designing should meet the business and technical requirements of Courseware Publishers.

What should you do?

- A. The Connection Manager Administration Kit (CMAK) on the PDC should be configured.
- B. Network address translation (NAT) should be configured on all VPN servers.
- C. The RADIUS service should be implemented in each branch office.
- D. The RADIUS service should be implemented in Phoenix.

Answer: D

Explanation: You should always remember that the Remote Authentication Dial-In User Service (RADIUS) is a widely used protocol which is used enables centralized accounting, authentication, and authorization for remote network access. You should also keep in mind that RADIUS can be used to manage network access for VPN, dial-up, and wireless networks.

1. Courseware Publishers wants to have authorized computers in the registrar's office to require smart card support for updating the Library records database. Courseware Publishers considers it imperative that the remote access policies for Phoenix, Philadelphia, Miami and Boston be centralized
2. Courseware Publishers wants to ensure that remote access will be required for all Librarians accessing the business offices from home

Incorrect Answers:

A: This option should not be considered for use in the scenario because the Connection Manager Administration Kit (CMAK) is used to automate VPN client installation.

B: Network Address Translation should not be used in the scenario because the technology is used to use one set of Internet Protocol (IP) addresses for internal traffic and a second set of addresses for external traffic.

C: There is no need to implement the RADIUS service in each branch office because the content has already been developed and is in use in Phoenix.

Reference:

Elias N. Khnaser, Susan Snedak, Chris Peiris, and Rob Amini; MCSE Designing Security for a Windows Server 2003 Network Exam 70-298 Study Guide, Chapter 10

Roberta Bragg; MCSE Self-Paced Training Kit (Exam 70-298): Designing Security for a Microsoft Windows Server 2003 Network, Chapter 7, pp. 7-62.

QUESTION 96

You work as the network administrator at courseware.com. You are in the process of creating the Physical Design for an Active Directory and Network Infrastructure. You have recently received instruction to start designing a network and routing topology for the new Active Directory environment. You are required to choose which of the groups have the required rights to authorize DHCP servers? (Each correct answer presents part of the solution. Choose TWO.)

- A. The DHCP administrators in Phoenix only
- B. The DHCP administrators in all offices
- C. The IT staff in Phoenix
- D. The Members of the Enterprise Admins group
- E. The IT staff in Boston

Answer: C, D

Explanation: In the scenario you are required to choose which of the groups are able to authorize DHCP servers. You should remember that only Enterprise Admins have the ability to authorize DHCP servers. In the scenario it states that the

IT staff in Phoenix will be responsible for administering Active Directory.

1. The aim of Courseware Publishers is to provide an adequate security structure for the network environment. Courseware Publishers considers the creation of a centralized network operation as important. The Courseware Publishers network CIO additionally states that he is confident in the ability of the IT staff in Phoenix to be the lead administrative role in the envisioned environment.

Incorrect Answers:

A, B: You should always remember that the DHCP Administrators group is a built-in group in Active Directory which does not have the ability to authorize DHCP servers.

E: In the scenario it is stated that the IT staff in Phoenix will be responsible for administering Active Directory so this option is incorrect.

Reference:

Deborah Littlejohn Shinder, Dr. Thomas W. Shinder; Exam 70-290: MCSA/MCSE, Implementing, Managing, and Maintaining a Windows Server 2003 Network Infrastructure Guide & DVD Training System, Syngress Publishing, Inc., Chapter 3, pp. 257.

QUESTION 97

You work as the network administrator at courseware.com. You are in the process of creating the Logical Design for a Network Services Infrastructure. You have recently received instruction to designing the placement of operations master roles in the new environment for Courseware Publishers. You are required to choose in which location or locations the PDC emulator should be designated?

- A. Miami
- B. Boston
- C. Philadelphia
- D. Phoenix

Answer: D

Explanation: In the scenario it is stated that the Phoenix office is responsible for the administration of Active Directory. In the scenario you should consider placing the Forrest Root domain here and the PDC Emulator should be designated to Phoenix.

1. The aim of Courseware Publishers is to provide an adequate security structure for the network environment. Courseware Publishers considers the creation of a centralized network operation as important. The Courseware Publishers network CIO additionally states that he is confident in the ability of the IT staff in Phoenix to be the lead administrative role in the envisioned environment.

Incorrect Answers:

A, B, C: In the scenario you should keep in mind that the Primary Domain Controller (PDC) is the first domain controller created in the domain. This means that all the other domain controllers are considered backup domain controllers (BDCs).

Reference:

Deborah Littlejohn Shinder, Dr. Thomas W. Shinder; Exam 70-290: MCSA/MCSE, Implementing, Managing, and Maintaining a Windows Server 2003 Network

Infrastructure Guide & DVD Training System, Syngress Publishing, Inc, Chapter 1, pp. 19.

QUESTION 98

You work as the network administrator at courseware.com. You are in the process of creating the Physical Design for an Active Directory and Network Infrastructure. You have recently received instruction to start designing DNS and DHCP network and routing topology. The solution you are designing should support the new environment.

What should you do?

- A. The DHCP server should be configured to update DNS for DHCP clients that do not support dynamic updates.
- B. A DNS domain name should be configured on the DHCP server.
- C. A WINS resource record should be created in the Active Directory DNS zone.
- D. A WINS referral zone should be created in the DNS zone that supports Active Directory.

Answer: A

Explanation: You should remember in the scenario that one of the dynamic update settings that you can configure on the DNS tab of the DHCP server properties is used to determine if the DHCP server should provide dynamic DNS update service of DHCP clients not capable of performing dynamic updates.

1. Courseware Publishers requires the Phoenix, Philadelphia, Miami and Boston offices to each host DNS subdomains supporting the online courseware. Courseware Publishers additionally requires to have the UNIX Librarians to support pointer (PTR) records for several applications used from the remote computers.
2. Courseware Publishers requires to have unauthorized updates of DNS records to be prevented. Courseware Publishers additionally wants to have the amount of DNS zone transfer or replication to be minimized.
3. Courseware Publishers wants all the remote and client computers to have host (A) resource records in DNS

Incorrect Answers:

B: You should not consider using this option in the scenario because the option specifies the domain name that DHCP clients should use when resolving unqualified names during DNS domain name resolution.

C: You should not consider using a WINS resource record in the scenario because the resource record instructs the DNS services to use WINS to look up and forward queries for host names which are not in the zone database.

D: You should only consider configuring a WINS referral zone to provide a means of organizing and distinguishing between WINS and DNS records.

Reference:

J. C. Mackin, and Ian McLean; MCSA/MCSE self-paced training kit (exam 70-291): Implementing, managing, and maintaining a Microsoft Windows Server 2003 network infrastructure, Chapter 7, pp. 7-13 and 7-41.

Walter Glenn, and Michael T. Simpson; MCSE 70-297 Training Kit - Designing a Windows server 2003 Active Directory and Network Infrastructure, Chapter 6, pp. 6-14.
Martin Grasdahl, Laura E. Hunter, and Michael Cross; MCSE Planning and Maintaining a Windows Server 2003 Network Infrastructure: Exam 70-293 Study Guide & DVD Training System, Chapter 6, pp. 403.

QUESTION 99

You work as the network administrator at courseware.com. You are in the process of creating the Logical Design for an Active Directory and Network Infrastructure. You have recently received instruction to start designing security for remote access users. You are required to select which of the following operating systems should be used on the remote computers? (Choose all that apply.)

- A. Windows 98
- B. Windows 95
- C. Windows 2000 Professional
- D. Windows NT Workstation 4.0
- E. Windows XP Professional

Answer: C, E

Explanation: In the scenario you must remember that support for smart cards is configured through Group Policy. The Answers used in the scenario both support Group Policy meaning they are able to support smart cards.

1. Courseware Publishers wants to have authorized computers in the registrar's office to require smart card support for updating the Library records database. Courseware Publishers considers it imperative that the remote access policies for Phoenix, Philadelphia, Miami and Boston be centralized

Incorrect Answers:

A, B, D: These desktop environments mentioned in these options should not be considered for use in the scenario because the desktop environments used do not support group policies. You should remember that support for smart cards is configured through Group Policy.

QUESTION 100

You work as the network administrator at courseware.com. You are in the process of creating the Logical Design for a Network Services Infrastructure. You have recently received instruction to start designing a VPN remote access authentication strategy. The solution you are designing should meet the business and technical requirements of Courseware Publishers.

What should you do?

- A. Configure Internet Authentication Service (IAS) for accounting.
- B. Network address translation (NAT) should be configured on all VPN servers.
- C. The server running Routing and Remote Access should be configured to restrict dial-in traffic.

D. The Connection Manager Administration Kit (CMAK) on the PDC should be configured.

Answer: A

Explanation: Internet Authentication Service (IAS) is the Microsoft implementation of Remote Authentication Dial-In User Service (RADIUS), an authentication and accounting system used by many Internet Service Providers (ISPs). When a user connects to an ISP using a username and password, the information is passed to a RADIUS server, which checks that the information is correct, and then authorizes access to the ISP system.

1. Courseware Publishers wants to have authorized computers in the registrar's office to require smart card support for updating the Library records database. Courseware Publishers considers it imperative that the remote access policies for Phoenix, Philadelphia, Miami and Boston be centralized

2. Courseware Publishers wants to ensure that remote access will be required for all Librarians accessing the business offices from home

Incorrect Answers:

B: Network Address Translation should not be used in the scenario because the technology is used to use one set of Internet Protocol (IP) addresses for internal traffic and a second set of addresses for external traffic.

C: In the scenario the customers should be able to view the library books and courseware available by using their remote computers.

D: This option should not be considered for use in the scenario because the Connection Manager Administration Kit (CMAK) is used to automate VPN client installation.

Reference:

Dan Holme, and Orin Thomas: MCSA/MCSE Self-Paced Training Kit (Exam 70-290): Managing and Maintaining a Microsoft Windows Server 2003 Environment, Microsoft, Glossary, pp. G-11.

Topic 9, Race Technologies, Scenario

Background

Race Technologies is one of the worlds leading manufacturers of custom performance racing parts for Formula 1 spec cars. Race Technologies owns several large wind tunnels across the United States used for testing and developing new prototype parts.

The designers and mechanics of Race Technologies hours of operation are 8:00 A.M. to 5:00 P.M., Monday through Friday.

Physical Locations

Race Technologies has their headquarters located in St. Louis. Race Technologies owns an additional five branch offices located in the regions below:

1. Miami
2. Washington
3. Chicago
4. Phoenix
5. Detroit

Race Technologies has provided the current number of users in each office is shown below:

Office	Current users
St. Louis	225
Miami	150
Detroit	105
Washington	15
Phoenix	15

Planned Changes

Race Technologies are considering implementing a Windows Server 2003 Active Directory environment which will meet the new security and customer requirements.

Existing Environment

Business Processes

Race Technologies consists of the departments below:

1. Human Resources (HR)
2. Finance
3. Information Technology (IT)
4. Designers
5. Mechanics
6. Shipping

Race Technologies IT department network users will be responsible for all network management.

The network users of Race Technologies frequently work on multiple projects at the same time. As a result of this action a strong administrative structure based on each user's office location and department is used.

Infrastructure

Directory Services

The existing domains and trust relationships configured for Race Technologies is shown in the Domain model.

Race Technologies makes use of a single Windows 2000 domain located in the St. Louis office. Race Technologies has configured the name of the domain as racetech.com. The Race Technologies current domain functional level is set at Windows 2000 mixed-mode. The Race Technologies domain contains Windows 2000 Servers configured as domain controllers, Windows NT Server 4.0 computers configured as BDCs, and Windows 2000 Server computers configured as member servers.

This is currently the only Active Directory domain which has three top-level OUs. The following three top-level OUs are part of the domain:

1. Designers
2. Mechanics
3. Shipping

Race Technologies has implemented the default site configuration in the existing Active Directory environment.

Problem statements

Race Technologies wants to have the following business problems considered:

1. We want to have the users change their passwords frequently and be configured with logon hours. The reason for this is because the current network does not enforcement

frequent password changes and logon hours.

2. We have recently received a call from the ISP. The ISP has stated that they are only able to supply a single subnet, consisting of 32 IP addresses, for the Internet link.
3. We should consider having the administrative tasks require less manual overhead since it difficult to manage users and groups and their necessary permissions. Race Technologies has recently discovered that NetBIOS name resolution is saturating the WAN links.
4. The finance and HR departments of Race Technologies still are unable to agree on a mutual security policy to implement.

Chief Execute Officer

"Race Technologies has recently lost a good number of projects. The contracts were lost because the deadline for the new prototype was not met. We should consider decreasing the amount of time spent on administering the network and customers are my primary reason for requesting the upgrade of the entire network."

"Race Technologies has made a large fund available which should be used to purchase the critical hardware requirements because Race Technologies do not want any downtime experienced for network users. Race Technologies wants to have strict business hours enforced ensuring that the network employees are not able to work at the office or work from home outside normal business hours."

Chief Information Officer

"The Race Technologies network is currently having problems which are caused as a result of all the merges and acquisitions. Race Technologies should have all their servers installed with Windows Server 2003 to resolve these problems. Race Technologies should also consider upgrading the network client computers to Windows XP Professional over the next year."

"The Race Technologies IT response level is far too high resulting to loads of lost production hours. Race Technologies wants to have each office continue managing its own users and computers, with the exception of the finance and HR departments. The finance and HR departments have their own respective requirements. Race Technologies wants to ensure no production time is lost due to interruption in the network connectivity."

Chief Network Administrator

"Race Technologies has a policy which states that we are expected to resolve issues within 24 hours. Race Technologies do not always resolve all the network issues in time. The Race Technologies network administrators work after hours on weekends since most high-level administrative should only be done when users are not in the office."

"The Race Technologies Domain administrators are responsible for managing the private IP addresses of every computer belonging to their respective domains."

"Race Technologies has ensured that there is Help desk staff in each branch office to assist users with software-related problems and basic network problems. Race Technologies has configured each domain with its own help desk staff with personnel located in each office. Race Technologies wants the Help Desk staff to be responsible for resetting passwords if users forget them in the future."

Office Worker

"Race Technologies should really start treating all network employees equally because only selected users have Internet access. Because the lack of Internet access prevents us

from remaining competitive we cannot perform the necessary research about new technologies or prototypes available."

Business Requirements

Business Drivers

Race Technologies wants to have the following business requirements considered:

1. Race Technologies wants to have the administrative effort minimized by using a single internal namespace. Race Technologies makes use of a Web site located outside the firewall for providing the company contact information.

Organizational Goals

Race Technologies wants to have the following organizational requirements considered:

1. Race Technologies wants the new design to accommodate the finance and HR departments. Race Technologies does not currently meet the requirements addressed by the company's planned password policy.
2. Race Technologies wants to have all the network computers with the latest service packs and hot fixes installed. Race Technologies also wants to have the network computers in the Shipping department updated with the latest versions of graphics and audio drivers installed.

Security

Race Technologies wants to have the following security requirements considered:

1. Race Technologies wants to have specific security groups set up to address the security requirements.
2. Race Technologies wants to have security based on departments and groups of individuals within the respective departments.
3. The Race Technologies' Finance department users require need access to the income and expenses information on a server named RT-SR01 located in the HR department.

Customer Requirements

Race Technologies wants to have the following customer requirements considered:

1. Race Technologies is planning on using a new service-level agreement which requires a response from the IT department to users within one hour to go into effect. Race Technologies wants to have the employees personal information to remain secure
2. Race Technologies wants to have all the network computers capable of accessing all client computers, regardless of office location.

Technical Requirements

Active Directory

Race Technologies wants to have the following Active Directory requirements considered:

1. Race Technologies wants the new Active Directory environment to enable the security requirements of various departments which should be met. Race Technologies wants to accomplish this by installing Windows Server 2003 on all domain controllers.
2. Race Technologies are planning on using a completely decentralized administrative approach where each group of administrators is responsible for its own departmental environment.
3. Race Technologies wants to ensure that only one operations master role will be allowed per domain controller to provide fault tolerance.
4. Race Technologies additionally wants to have DNS replication of the forest root domain limited to forest domain controllers only.

Network Infrastructure

Race Technologies wants to have the following infrastructure requirements considered:

1. Race Technologies wants to have a new Routing and Remote Access solution installed:
2. Race Technologies requires a DHCP solution that is fault tolerant within each office implemented
3. Race Technologies want the networks WAN links to be fault tolerant
4. Race Technologies wants to have name resolution localized on the local network. Race Technologies additionally requires the users to be able to access internal and external Websites

Topic 9, Race Technologies (12 Questions)

QUESTION 101

You work as the network administrator at racetech.com. You are in the process of creating the Logical Design for an Active Directory Infrastructure. You have recently received additional instruction to start designing a strategy for Group Policy implementation. The solution you are designing should address the requirements of the shipping department. What should you do?

- A. The Default Domain Policy should be configured to have the No Override option.
- B. To prevent the GPO from applying to members of the Shipping department you should use block inheritance.
- C. A GPO should be created and linked to the Chicago site.
- D. A GPO should be created and linked to the racetech.com domain.
- E. A GPO should be created and linked to the Shipping OU.

Answer: E

Explanation: You should keep in mind that you are able to make use of Group Policy to define user settings such as password restrictions or computer settings. You should consider using a Group Policy plan which applies GPOs efficiently and links GPOs to OUs.

1. Race Technologies are planning on using a completely decentralized administrative approach where each group of administrators is responsible for its own departmental environment
2. Race Technologies wants to have all the network computers with the latest service packs and hot fixes installed. Race Technologies also wants to have the network computers in the Shipping department updated with the latest versions of graphics and audio drivers installed

Incorrect Answers:

- A: You should not make use of this option in the scenario because you are required to configure a department and the option applies at eh domain level.
- B: This option should not be considered for use in the scenario because this will prevent the configured GPOs from being applied to the domain members.

C: This option should not be used in the scenario because the option would apply the GPO to the Chicago site and the question wants the Shipping department configured.

D: This option should not be used in the scenario because the option would apply the GPO to the entire racetech.com domain and the question wants the Shipping department configured.

Reference:

Walter Glenn, and Michael T. Simpson, MCSE 70-297 Training Kit - Designing a Windows server 2003 Active Directory and Network Infrastructure, Chapter 4, pp. 4-10.

QUESTION 102

You work as the network administrator at racetech.com. You are in the process of creating the Logical Design for a Network Services Infrastructure. You have recently received additional instruction to start designing a strategy for NetBIOS name resolution. The solution you are designing should meet the business and technical requirements of Race Technologies.

What should you do?

A. The DNS Server service should be installed on one domain controller in each branch office. The DNS server should be configured to forward all unanswered queries to the WINS server. All the computers should then be configured to have the IP address of the DNS servers.

B. The DNS servers in each branch office should be configured to forward all unanswered queries to a local WINS server. All the computers should then be configured to have the IP addresses of the DNS server in racetech.com forest root.

C. Two additional WINS servers should be installed in St. Louis. The WINS servers should be configured to use push/pull replication. All the computers should then be configured to have the IP addresses of the WINS servers.

D. One WINS server should be installed in each branch office. The WINS servers should be configured to use push/pull replication with the WINS server in St. Louis. All the computers should then be configured to have the IP address of the local WINS server.

Answer: D

Explanation: You should remember that the scenario asks for a NetBIOS name resolution strategy by making use of WINS server. Race Technologies requires the WINS service to be available to the network client computers when required. In the scenario there is a substantial amount of users so you should install each office with its own WINS server.

1. Race Technologies wants to have name resolution localized on the local network

2. Race Technologies wants to have the administrative effort minimized by using a single internal namespace. Race Technologies makes use of a Web site located outside the firewall for providing the company contact information

Incorrect Answers:

A, B: In the scenario each branch office should make use of their respective WINS server as this option will result in more network traffic towards St. Louis.

C: The Race Technologies network does not make use of any slow links so there is no

need to have the additional WINS servers installed.

Reference:

Walter Glenn, and Michael T. Simpson, MCSE 70-297 Training Kit - Designing a Windows server 2003 Active Directory and Network Infrastructure, Chapter 7, pp. 7-16 to 7-24.

QUESTION 103

You work as the network administrator at racetech.com. You are in the process of creating the Physical Design for an Active Directory and Network Infrastructure. You have recently received additional instruction to start designing a strategy for DHCP. The solution you are designing should meet the business and technical requirements.

What should you do?

- A. Two DHCP servers should be installed in each branch office and one DHCP server in St. Louis.
- B. Two DHCP servers should be installed in each branch office and two DHCP servers in St. Louis.
- C. One DHCP server should be installed in each branch office and one DHCP server in St. Louis.
- D. One DHCP server should be installed in each branch office and two DHCP servers in St. Louis.

Answer: B

Explanation: You should remember that Race Technologies has stated that the network will require a DHCP solution that is fault tolerant. By taking the actions in the answer you ensure that you meet the business and technical requirements of Race Technologies.

1. Race Technologies requires a DHCP solution that is fault tolerant within each office implemented

Incorrect Answers:

A, B, C:

You should not consider taking the actions in these answers because they will not provide the required fault tolerance and only has one server in each office.

Reference:

QUESTION 104

You work as the network administrator at racetech.com. You are in the process of creating the Logical Design for a Network Services Infrastructure. You have recently received additional instruction to start designing a DNS strategy. The solution you are designing should meet the business and technical requirements. What should you do?

- A. Application partitions should be created for the different zones on one domain controller. Replication should then be configured to occur on all DNS servers.

- B. The DNS Server service should be installed on all domain controllers. Primary zones and secondary zones should then be created.
- C. The DNS Server service should be installed on all domain controllers. Active Directory-integrated zones should then be created. The zones should finally be replicated to all DNS servers in the forest.
- D. The DNS Server service should be installed on all domain controllers. Active Directory-integrated zones should then be created. The zones should finally be replicated to all DNS servers in the domain.

Answer: D

Explanation: You should remember in the scenario that all the new network implementations should be fault tolerant. By configuring Active Directory integrated zones a copy of the zone is kept in Active Directory and finally replicated to all domain controllers.

1. Race Technologies additionally wants to have DNS replication of the forest root domain limited to forest domain controllers only
2. Race Technologies wants to have name resolution localized on the local network
3. Race Technologies has made a large fund available which should be used to purchase the critical hardware requirements because Race Technologies do not want any downtime experienced for network users

Incorrect Answers:

- A: You should not consider making this configuration in the scenario because this configuration stores information about sites that is used to build the Active Directory replication topology, DNS zones are not stored in the configuration partition.
- B: You should not make use if this configuration in the scenario because you are required to provide fault tolerance with each new addition to the network, this configuration is not fault tolerant.
- C: You should not consider using this configuration in the scenario because Race Technologies requires having DNS replication limited to forest domain controllers only.

Reference:

Walter Glenn, and Michael T. Simpson, MCSE 70-297 Training Kit - Designing a Windows server 2003 Active Directory and Network Infrastructure, Chapter 6, pp. 6-12 to 6-13.

QUESTION 105

You work as the network administrator at racetech.com. You are in the process of creating the Conceptual Design by Gathering and Analyzing Business and Technical Requirements. You have recently received additional instruction for the design. You are required to select the proper number of server for operations master roles?

- A. 5
- B. 21
- C. 14
- D. 11

Answer: D

Explanation: You should remember in the scenario that you are required to have the operation master roles hosted on different domain controllers. The Race Technologies network has a single forest with three domains. There are also three domain-level operations master roles: PDC emulator, RID master and infrastructure master as well as two forest-level roles: schema master and domain naming master. So you require $3 \times 3 + 2$ which is 11 domain controllers.

1. Race Technologies wants to ensure that only one operations master role will be allowed per domain controller to provide fault tolerance

Incorrect Answers:

A, B, C:

The other mentioned amount of domain controllers should not be used in the scenario as you would not be able to meet the required security requirements as well as fault tolerance.

QUESTION 106

You work as the network administrator at racetech.com. You are in the process of creating the Physical Design for an Active Directory and Network Infrastructure. You have recently received additional instruction to start designing a remote access infrastructure. The solution you are designing should provide Internet access to all users.

What should you do?

- A. One server should be configured as a Routing and Remote Access VPN server.
- B. One server should be configured as a Routing and Remote Access NAT router.
- C. Internet Connection Sharing should be configured on all client computers.
- D. Automatic Private IP Addressing (APIPA) should be configured on all client computers.

Answer: B

Explanation: You should note that computers which run any member of the Windows Server 2003 family can be used to add the internal interface as a private interface to the Network Address Translation component of the Routing and Remote Access service to provide the remote access clients Internet access

1. Race Technologies should really start treating all network employees equally because only selected users have Internet access. Because the lack of Internet access prevents us from remaining competitive we cannot perform the necessary research about new technologies or prototypes available

Incorrect Answers:

A: You should not make use of this configuration in the scenario because the VPN server allows users to dial-in to the Race Technologies corporate network and provides access to internal network resources.

C: You should not consider making use of ICS in the scenario because ICS is meant ideally for small networks.

D: You should not consider making use of APIPA in the scenario because this is a feature for simple networks configured to obtain IP addressing information automatically.

Reference:

Jerry Honeycutt: Introducing Microsoft Windows Server 2003, Microsoft Press, Chapter 6. Walter Glenn, and Michael T. Simpson, MCSE 70-297 Training Kit - Designing a Windows server 2003 Active Directory and Network Infrastructure, Chapter 9, pp. 9-12.

QUESTION 107

You work as the network administrator at racetech.com. You are in the process of creating the Conceptual Design by Gathering and Analyzing Business and Technical Requirements. You have recently received additional instruction to start designing an Active Directory forest structure to meet the business and technical requirements of Race Technologies.

What should you do?

- A. A single forest that has three domains should be created: one for finance, one for HR, and one for the remaining departments.
- B. Multiple forests that have a single domain should be created in each forest to represent the departments.
- C. A single forest that has one domain should be created. OUs should then be used to separate the departments.
- D. A single forest that has multiple domains should be created to represent every department.

Answer: A

Explanation: In the scenario you should remember that the finance and HR department users have different security requirements and should each have their own domain to completely decentralized the administrative approach.

1. Race Technologies wants the new design to accommodate the finance and HR departments. Race Technologies does not currently meet the requirements addressed by the company's planned password policy
2. Race Technologies wants the new Active Directory environment to enable the security requirements of various departments which should be met. Race Technologies wants to accomplish this by installing Windows Server 2003 on all domain controllers
3. Race Technologies are planning on using a completely decentralized administrative approach where each group of administrators is responsible for its own departmental environment
4. Race Technologies want the networks WAN links to be fault tolerant

Incorrect Answers:

B, C, D: You should not consider using the other configurations in the scenario as they will not meet the security requirements of the HR and the finance departments network users.

Reference:

Walter Glenn, and Michael T. Simpson, MCSE 70-297 Training Kit - Designing a

Windows server 2003 Active Directory and Network Infrastructure, Chapter 3, pp. 3-4 to 3-7.

QUESTION 108

You work as the network administrator at racetech.com. You are in the process of creating the Conceptual Design by Gathering and Analyzing Business and Technical Requirements. You have recently received additional instruction to start designing a WAN implementation strategy. The solution you are designing should meet the business and technical requirements of Race Technologies.
What should you do?

- A. An Internet Authentication Service (IAS) server should be installed in each branch office.
- B. A VPN connection between each branch office should be configured.
- C. Multiple Active Directory site links should be configured.
- D. A demand-dial router should be configured.

Answer: D

Explanation: You should note in the scenario that a demand-dial connection is used by the Routing and Remote Access service to make point-to-point connections between LANs over which packets are routed. By configuring a demand-dial router you ensure that you adhere to the business and technical requirements of Race Technologies.

1. Race Technologies wants to have a new Routing and Remote Access solution installed
Incorrect Answers:

A, B, C: You should not consider making use of the other options in the scenario because you would effectively be violating the Race Technologies business and technical requirements which you are required to consider.

Reference:

Jerry Honeycutt: Introducing Microsoft Windows Server 2003, Microsoft Press, Chapter 6.

QUESTION 109

DRAG DROP

You work as the network administrator at racetech.com. You are in the process of creating the Conceptual Design by Gathering and Analyzing Business and Technical Requirements. You have recently received additional instruction to start designing a security for the strategy to provide the required security for the Income and Expenses information on RT-SR01.

You are required to identify the actions in the correct order they should be performed? (To answer, arrange the actions in the proper order. Use only actions that apply.)

Steps, select from these

Create a universal group named Expenses. Add users from the Designers department to the Expenses group.

Create a global group named Finance. Add the appropriate users from the Finance department to the finance group.

Create a domain local group named HR. Add the appropriate users from the Finance department to the Finance group. Assign the HR group permissions to RT-SR01.

Steps, place here

Place first step here.

Place second step here, if any.

Place third step here, if any.

Answer:

Steps, Select from theses

Steps, place here

Create a domain local group named HR. Add the appropriate users from the Finance department to the Finance group. Assign the HR group permissions to RT-SR01.

Create a global group named Finance. Add the appropriate users from the Finance department to the Finance group.

Create a universal group named Expenses. Add users from the Designers department to the Expenses group.

Explanation:

In the scenario you are required to configure the security implementation in the exact order used in the scenario or the implementation will not meet the required security settings. By completing the configuration implementation in this order you ensure that the required security settings are met.

Reference:

QUESTION 110

You work as the network administrator at racetech.com. You are in the process of creating the Conceptual Design by Gathering and Analyzing Business and Technical Requirements. You have recently received additional instruction to start designing a strategy for a password management solution. The solution you are designing should meet the business and technical requirements of Race Technologies.

What should you do? (Choose two)

- A. The password management controls should be delegated to the Domain Users group.
- B. The password management controls should be delegated to the help desk staff.
- C. The Default Domain Controller Policy should be configured to enforce password expiration settings.
- D. The Default Domain Policy should be configured to enforce password expiration settings.

Answer: A, C

Explanation: In the scenario you should note that the Security groups are used for

grouping domain users into a single logical administrative unit. You are able to assign permissions to Security groups as long as the users remain members of the group.

1. Race Technologies are planning on using a completely decentralized administrative approach where each group of administrators is responsible for its own departmental environment

Incorrect Answers:

B, D: You should not consider taking these actions in the scenario because the options used will not be able to meet the required design for the Race Technologies network infrastructure.

Reference:

Walter Glenn, and Michael T. Simpson, MCSE 70-297 Training Kit - Designing a Windows server 2003 Active Directory and Network Infrastructure, Chapter 4 , pp. 4-26.

QUESTION 111

You work as the network administrator at racetech.com. You have recently received instruction to start designing the network security policy solution of Race Technologies. You are in the process of creating and designing the network security policy solution which must adhere to the Race Technologies network corporate security policy. You are additionally required to select which actions should be performed? (Choose all that apply.)

- A. A policy should be enabled which forces users to log off when their logon hours expire.
- B. A password policy should be configured that requires strong passwords.
- C. The branch offices network users should be allowed to log on between the hours of 8:00 A.M and 5:00 P.M., Monday through Friday.
- D. A password policy should be configured which requires all users to change their passwords once a month.

Answer: A B, C, D, E

Explanation: In the scenario you should consider taking all the actions mentioned because the actions all adhere to the Race Technologies network security policy. By taking the actions in the answer you ensure that your design enforces the corporate security policy of Race Technologies.

1. The designers and mechanics of Race Technologies hours of operation are 8:00 A.M. to 5:00 P.M., Monday through Friday.
2. We want to have the users change their passwords frequently and be configured with logon hours. The reason for this is because the current network does not enforcement frequent password changes and logon hours

QUESTION 112

You work as the network administrator at citycentrl.com. You are in the process of creating the Logical Design for a Network Services Infrastructure. You have received additional instruction to start designing a DNS name resolution strategy

for Race Technologies. The DNS name resolution strategy you are designing should allow all users access to internal and external web sites. What should you do?

- A. The DNS server should be configured to forward all unanswered queries to a DNS server located at the ISP.
- B. The DNS server located at the ISP should be added to the list of name servers for the racetech.com DNS zone.
- C. Zone transfers should be allowed to any DNS server.
- D. A new stub zone should be created for the DNS zone on the DNS server.

Answer: A

Explanation: In the scenario you are required to provide Internet Access to the network users of Race Technologies. You should remember when a DNS server receives a query, it will first check to see whether it can answer the query authoritatively if not the query will be forwarded. This ensures that the network users are able to connect to the Internet.

1. Race Technologies wants to have name resolution localized on the local network. Race Technologies additionally requires the users to be able to access internal and external Websites

Incorrect Answers:

B: This option should not be used in the scenario because this will have the internal racetech.com name space exposed to Internet users.

C: In the scenario you should not have the zone transfers configured to any server as this will not meet the requirements of Race Technologies.

D: You should not consider configuring a stub zone on the DNS server because a stub zone is a copy of a zone containing only the resource records required to identify an authoritative DNS server.

Reference:

J. C. Mackin, and Ian McLean, MCSA/MCSE self-paced training kit (exam 70-291): implementing, managing, and maintaining a Microsoft Windows Server 2003 network infrastructure, Microsoft, Chapter 4, pp. 4-19 to 4-16.

Topic 10, Bilco Health, Scenario

Background

Bilco Health is a private health care company that operates several hospitals and clinics in Canada.

Physical Locations

Bilco Health has its headquarters in Montreal and branch offices in Quebec and Toronto. Each branch office operates a single hospital and has three clinics attached to it while headquarters only operates a single hospital. The business offices are located at the Administration building of the relevant hospital.

There are 820 users at headquarters. The total number of users that fall under the Quebec office, including users at the three clinics attached to the branch office is 160, and for the

Toronto office it is 120.

Planned Changes

Bilco Health has grown considerably over the last 12 months. It is anticipated that this growth will continue as Bilco Health plans to open a hospital in Vancouver in the next few years. As the company has grown, available bandwidth has become critical. The company has a database that must be available 24 hours a day, seven days a week. To meet this requirement, Bilco Health wants to implement a Windows Server 2003 environment.

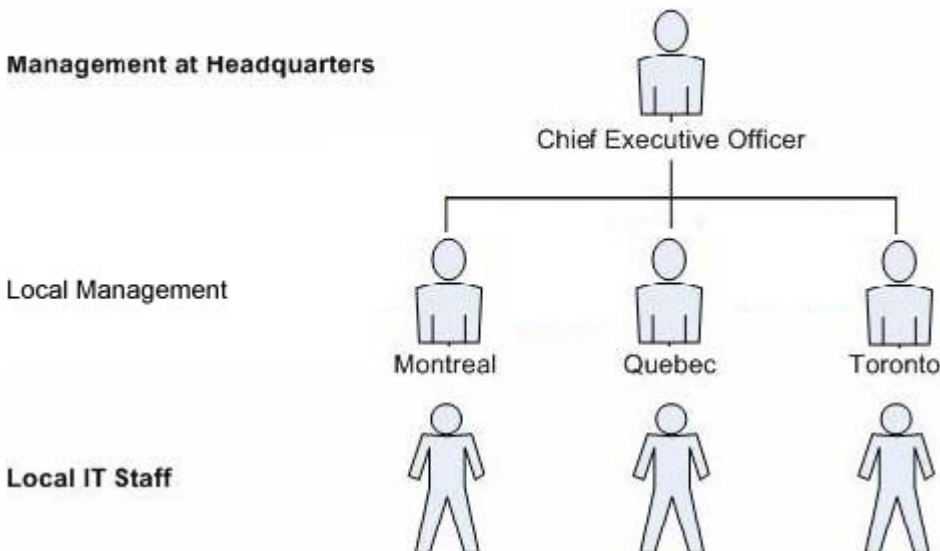
Business Processes

Bilco Health has a UNIX-based application named BH_App that maintains all patient records, including patient's medical histories. Each hospital runs a separate instance of the BH_App application. The clinics do not run an instance of the BH_App application but access the application at the hospital it is attached to. Bilco Health users use Windows XP Professional computers to update the patient records. All records are periodically sent to Montreal where it is entered into the company's database named BH_MediDB. The BH_MediDB is used for reporting purposes.

The Montreal office and each branch office have its own IT department. There are no IT department staff members at any of the clinics. The IT department at the branch offices supports the clinics attached to it.

The organizational structure of the company is shown in the Organizational Structure exhibit.

Organizational Structure



Directory Services

Bilco Health does not use Windows domain structure.

The BH_App application runs on UNIX servers at headquarters and at the branch offices. Each UNIX server has its own security accounts database.

Each office uses a standard user account and password that are used by network administrators in the office. The IT department in each branch office work independently, but company- wide decisions are made at headquarters.

Network Infrastructure

All client computers on the Bilco Health network run Windows XP Professional and each

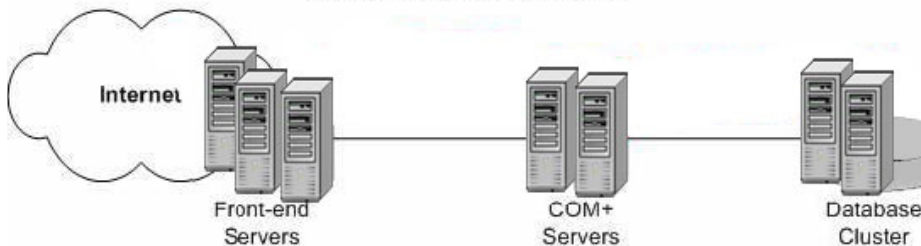
office has a separate switched 100-Mbps Ethernet network. Each branch office is connected to headquarters, and to its satellite offices by 64 Kbps ISDN lines. Bilco Health uses VPN connections over the Internet as a backup to connect the various offices.

Problem Statements

Chief Executive Officer

"We need ensure that our customers receive the most reliable service possible. We want to upgrade the BH_App application to BH_App_v2. The BH_App_v2 application will be a multitier application. The BH_App_v2 application Architecture diagram shows the architecture for the new application."

Application Architecture



"The BH_App application requires an available bandwidth of 32 Kbps to ensure adequate bandwidth for the BH_App application. However, the available bandwidth has decreased at a constant rate over the last year. The available bandwidth is shown in the Available Bandwidth exhibit. At the current rate, we will have bandwidth problems with the application by October. We must try to minimize network traffic through the ISDN lines because budget does not allow us to upgrade these lines. We are not sure how much bandwidth the BH_App_v2 application will require."

Available Bandwidth



Chief Information Officer

"Data security is my main concern. Data from the BH_MediDB database is now saved in different locations. I am concerned about who has access to the data. I'm also concerned about data recovery in the event of a disaster."

"We've also experienced problems with the confidentiality of customer information. We need to improve security to meet legal requirements regarding the confidentiality of patient's records."

Network Security Administrator

"We want security of the BH_MediDB database to be Active Directory integrated and centralized at the Montreal office. Network administrators must have Full Control permissions for the BH_MediDB database. For security reasons, we want network administrators to access the servers on which the BH_MediDB database is installed by using smart card authentication, but they must be able to log on to other computers without using a smart card."

"We currently perform our own administration at each office but the DNS servers will be administered only by network administrators from the Montreal office."

"The clinics do not have their own IT staff. Therefore no servers will be deployed at the clinics."

"Each office is located in a different region, and each region has different legal requirements. We must ensure that our user account policies at the different offices comply with the legal requirements of the region that they are located in."

Chief Network Administrator

"We will implement a Windows Server 2003 Active Directory domain. When we change our infrastructure, all offices must share the namespace bilco.com."

"I'm concerned that a failure at the Montreal office will affect our network. We must ensure that data can be recovered in the event of a disaster and that the network is available 24 hours a day, seven days a week."

"All Bilco Health users must have Microsoft Office and the BH_App_v2 application deployed on their client computers. The BH_App_v2 application will connect directly to the BH_MediDB database using the NetBIOS name of BHMEDIDB."

"We must keep replication traffic between the sites to a minimum to conserve bandwidth."

"All doctors that require remote access to the network must be subject to the same remote access policies that will be defined by administrators in Montreal."

Customer Service Representative

"Many of our patients have complained that they cannot make appointments by phone, we want our customers to be able to make appointments online. The BH_MediDB database will support online bookings."

"Doctors at the clinics often visit patients at their homes and must be able to access the patient's records remotely."

Topic 10, Bilco Health (12 Questions)

QUESTION 113

You need to determine whether the network bandwidth that is currently available is sufficient to run the BH_App_v2 application.

What should you do? (Each correct answer presents part of the solution. Choose THREE.)

A. Collect information about the BH_App_v2 application by running a debug version of the application.

B. Collect data about the bandwidth usage of each ISDN link by running Performance Monitor.

- C. Analyze the data that is transmitted over the network for the BH_App_v2 application by running Network Monitor.
- D. Collect data about the BH_App_v2 application by installing SNMP on all computers that are connected to the application.
- E. Analyze the bandwidth is required for the BH_App_v2 application by building a test environment for the application.

Answer: B, C, E

Explanation: Performance Monitor can be used to obtain statistics on total bandwidth usage. The Network Monitor is designed for real-time reporting of data to a console interface, and can be reported in graph, histogram, or numeric form. A test environment would be ideal in this case to prevent disruption of the active network.

Incorrect Answers:

A: Debugging is used to test that the application operates as expected before it is deployed to the production environment. It does not determine bandwidth requirements of the application.

D: SNMP allows for the monitoring the status of network components. It cannot be used to determine bandwidth requirements.

Reference:

Dan Holme, and Orin Thomas; MCSA/MCSE Self-Paced Training Kit (Exam 70-290): Managing and Maintaining a Microsoft Windows Server 2003 Environment, Chapter 12, pp. 12-18.

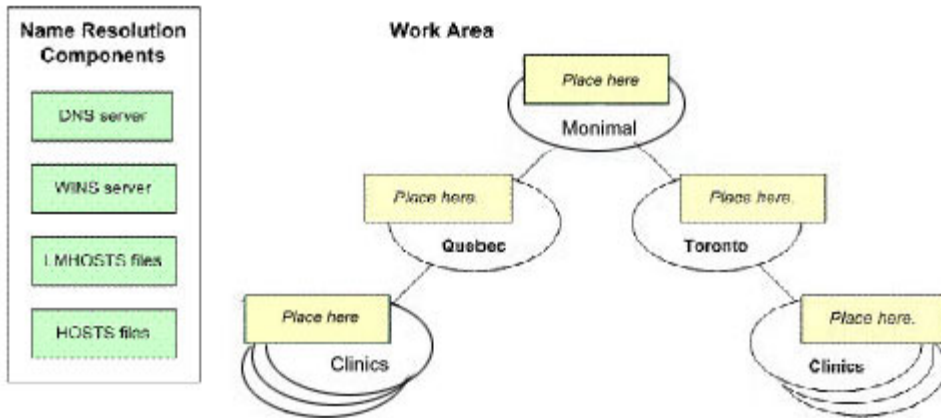
Craig Zacker; MCSE Self-Paced Training Kit (Exam 70-293): Planning and Maintaining a Microsoft Windows Server 2003 Network Infrastructure, Glossary, G-50.

QUESTION 114

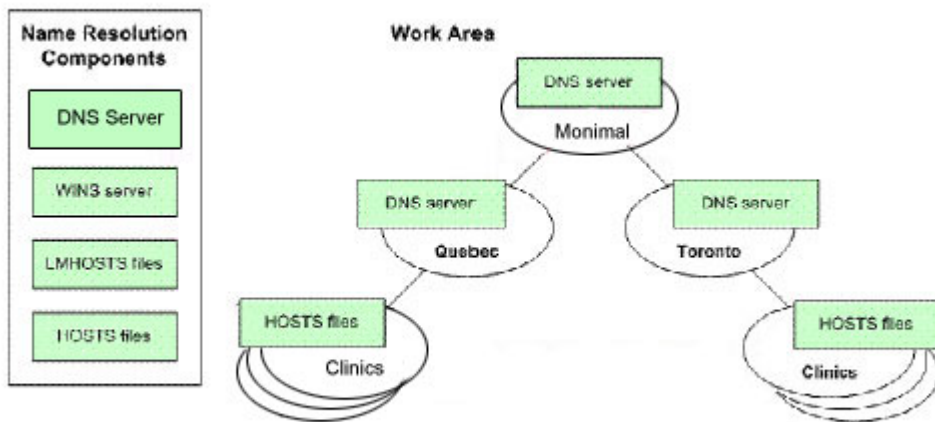
DRAG DROP

You need to design a name resolution strategy for the BH_App_v2 application. You need to ensure that your solution meets the Bilco Health's technical and business requirements.

What should you do? (To answer, drag the appropriate name resolution component to the correct location or locations in the work area.)



Answer:



Explanation:

The Chief Network administrator said the following:

* "All Bilco Health users must have Microsoft Office and the BH_App_v2 application deployed on their client computers. The BH_App_v2 application will connect directly to the BH_MediDB database using the NetBIOS name of BHMEDIDB."

Windows Internet Name Service (WINS) Server provides computer name resolution by translating NetBIOS names to IP addresses. For applications that depend on NetBIOS name resolution, will need WINS to support these applications in a routed environment. No servers are located at the clinics therefore you need LMHOSTS files at the clinics.

Incorrect Answers:

Domain Name Service (DNS) servers and HOSTS files are used for host name to IP address resolution, not NetBIOS name to IP address resolution.

Reference:

William Boswell; Inside Windows Server 2003, Addison Wesley, Chapter 4.

QUESTION 115

You need to ensure that there is sufficient network bandwidth available to for the BH_App_v2 application. You need to ensure that your solution meets Bilco Health's business requirements.

What should you do? (Choose all that apply.)

- A. Upgrade all ISDN lines before October.
- B. Upgrade all ISDN lines before deploying the BH_App_v2 application.
- C. Analyze the cause of the peak bandwidth usage in March and July last year.
- D. Analyze the bandwidth requirements for the BH_App_v2 application.

Answer: C, D

Explanation: This option allows you to obtain a baseline of the network usage.

Incorrect Answers:

A, B: These options are invalid, since the case study stated that there is no budget to upgrade the ISDN lines.

QUESTION 116

You need to design a strategy for migrating the UNIX user accounts to Active Directory for Bilco Health. You need to ensure that your solution meets the technical and business requirements.

What should you do? (Each correct answer presents part of the solution. Choose THREE.)

- A. Import the user accounts as inetOrgPerson objects.
- B. Use the Ldifde command to import the user accounts into Active Directory.
- C. Export the user accounts and their passwords from the UNIX servers to a text file.
- D. Assign random passwords to each user object, and securely distribute the password to the users.
- E. Instruct users to use the same name and password that they used on the UNIX servers.

Answer: B, C, D

Explanation:

The LDIFDE tool can be used to import user accounts into AD, so it is correct to export the accounts to a text file and then import them using LDIFDE. However, passwords cannot be added using LDIFDE upon object creation. Passwords can be modified by using the following command:

```
ldifde -i -f chPwd.ldif -t 636 -s dcname -b username domain password
```

Here's the line in the MS doc that refers to that:

The password attribute used by Active Directory is "unicodePwd." This attribute can be written under restricted conditions, but cannot be read. This attribute can only be modified, not added on object creation or read by a search.

A strong password is a password that provides an effective defense against unauthorized access to a resource.

Incorrect Answers:

A: InetOrgPerson is an object-similar to a user object-that is used to migrate users from other Lightweight Directory Access Protocol (LDAP) directory services to Active Directory, not from one OS to another.

E: This cannot be done, since the password attribute for UNIX and Active Directory is different.

Reference:

Knowledge Base article 263991:

<http://support.microsoft.com/default.aspx?scid=http://support.microsoft.com:80/support/kb/articles/Q263/9/91AS>

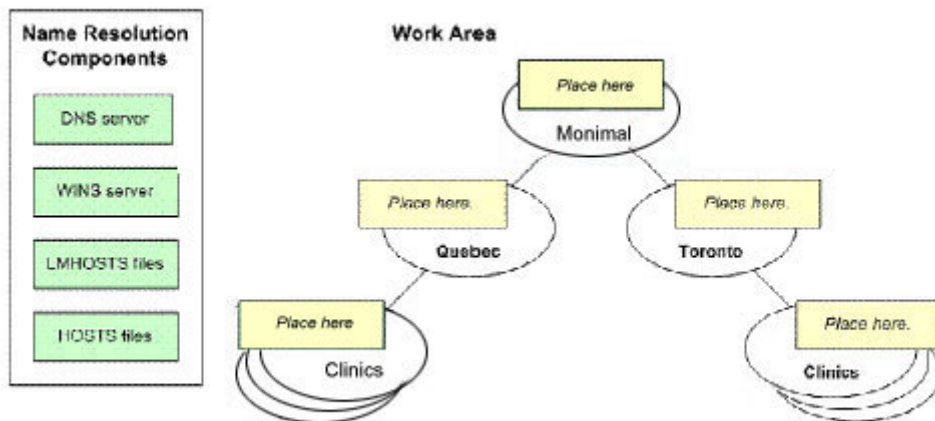
Walter Glenn, and Michael T. Simpson; MCSE 70-297 Training Kit - Designing a Windows server 2003 Active Directory and Network Infrastructure, Glossary, pp. G-6.

QUESTION 117

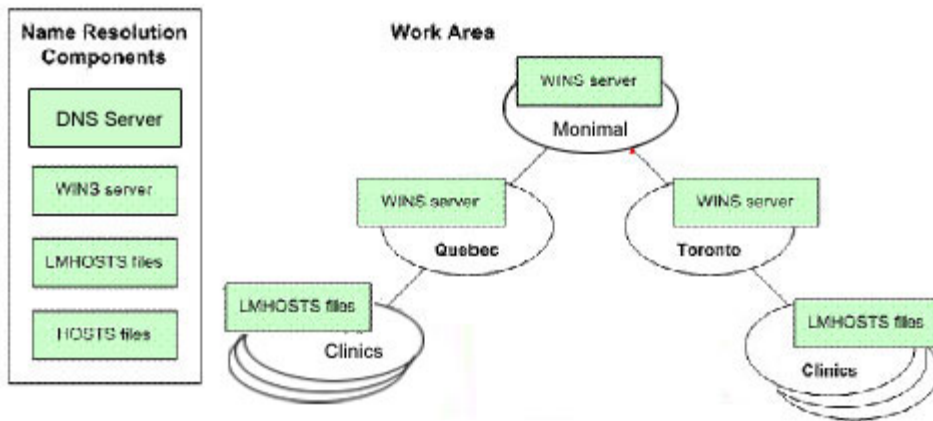
DRAG DROP

You need to design a host name resolution for all computers on the Bilco Health network. You need to ensure that your solution meets Bilco Health's business requirements.

What should you do? (To answer, drag the appropriate name resolution component to the correct location or locations in the work area.)



Answer:



Explanation:

Domain Name Service (DNS) Server provides computer name resolution by translating host names to IP addresses. No servers are located at the clinics therefore you need HOSTS files at the clinics.

Incorrect Answers:

Windows Internet Name Services (WINS) servers and LMHOSTS files are used for NetBIOS name to IP address resolution, not host name to IP address resolution.

Reference:

William Boswell; Inside Windows Server 2003, Addison Wesley, Chapter 4.

QUESTION 118

You need to design a strategy to optimize the DNS name resolution for the Bilco Health clinics that connect to the branch offices. You need to ensure that your solution meets business and technical requirements.

What should you do?

- A. Configure a caching-only DNS server at each clinic.
- B. Configure a HOSTS file on each client computer at each clinic.
- C. Configure a DNS server to use WINS forward lookup at each clinic.
- D. Configure a LMHOSTS file on each client computer at each clinic.

Answer: B

Explanation: No servers will be installed at the clinics therefore you can only use HOSTS files at the clinics. HOSTS files are a predecessor to DNS and are files with static mappings of hostnames to IP addresses.

Incorrect Answers:

A: A caching-only DNS server, as its name implies, caches the answers to queries and returns the results. This saves time and reduces network traffic because calls to multiple DNS servers are not required. However, no servers are installed at the clinics; therefore you cannot implement a caching-only DNS server at the clinics.

C: No servers will be installed at the clinics therefore you cannot use DNS server at the clinics.

D: LMHOSTS files are a predecessor to WINS and are files with static mappings of NetBIOS names to IP addresses.

Reference:

Walter Glenn, and Michael T. Simpson; MCSE 70-297 Training Kit - Designing a Windows server 2003 Active Directory and Network Infrastructure, Chapter 6, pp.6-6, and Chapter 1, pp. 1-19.

J. C. Mackin, and Ian McLean; MCSA/MCSE self-paced training kit (exam 70-291): Implementing, managing, and maintaining a Microsoft Windows Server 2003 network infrastructure, Chapter 5, pp. 5-34, and Chapter 4, pp. 4-29.

QUESTION 119

You need to design a Active Directory infrastructure for Bilco Health. You need to ensure that your solution meets the business and technical requirements. You run ADSizer to analyze domain controller requirements. ADSizer suggest only one domain controller for Montreal.

What should you do?

- A. Install at least two domain controllers in Montreal.
- B. Install the domain controller in Montreal and configure it as a bridgehead server.
- C. Install the domain controller in Montreal and configure it as a global catalog server.
- D. Distribute the users among sites in ADSizer and recalculate the domain controller requirements.

Answer: A

Explanation: The Chief Network Administrator is concerned that a failure at the Montreal office will affect the network. He wants to ensure that data can be recovered in the event of a disaster and that the network is available 24 hours a day, seven days a week. This means that we need fault tolerance; hence we need two domain controllers.

Incorrect Answers:

B: A bridgehead server is a server that is responsible for transferring directory replication information between sites.

C: A global catalog server is a domain controller that stores a read-only copy of all Active Directory objects in a forest, with the exception of objects stored in application directory partitions. Global catalog servers are used to store universal group membership information, authenticate users who log on using a UPN, and facilitate searches for objects across the entire forest.

D: The problem is not to distribute the users in the Montreal office among sites; rather ADSizer believes that one DC can handle the logon requests. The case study states the need for 24-7 availability, and two domain controllers in a site would allow for this as it increases fault tolerance.

Reference:

QUESTION 120

You need to ensure that the BH_App_v2 application has the appropriate network

bandwidth.

What should you do?

- A. Enable site link bridging on all site links.
- B. Upgrade all network links before deploying the BH_App_v2 application.
- C. Configure all site links to allow replication only after business hours.
- D. Configure the BH_App_v2 application to perform replication only after business hours.

Answer: D

Explanation: Network bandwidth is limited and will not be upgraded. This means you need to allow replication when network traffic is at its lowest, i.e., after hours.

Incorrect Answers:

A: Site links only affect Active Directory replication, not replication for other data.

Therefore, creating site link bridges will have no effect on the application.

B: The CEO said budget does not allow us to upgrade the ISDN lines so this is not an option.

C: Site links only affect Active Directory replication, not replication for other data.

Limiting Active Directory replication to after hours will mean more bandwidth for the application during office hours but it would be better to have the application perform replication after hours when bandwidth should be at its lowest.

Reference:

QUESTION 121

You need to design an IP address assignment strategy for Bilco Health. You need to ensure that all computers have valid IP addresses even if the DHCP server cannot be contacted for 24 hours.

What should you do?

- A. Increase the default lease period on the DHCP servers.
- B. Split all address ranges across multiple DHCP servers.
- C. Configure static IP addresses on all client computers.
- D. Allow client computers to use Automatic Private IP Addressing (APIPA).

Answer: B

Explanation: We need the users to receive an IP address from the DHCP server even if it is not available for 24 hours. Configuring 2 DHCP servers, with split address ranges, would add redundancy.

Incorrect Answers:

A: It is a best practice not to set your lease duration too high, because other DHCP clients on your network may be unable to obtain an IP address lease if all addresses are used up before current leases expire.

C: Static IP addressing does not require the use of DHCP but is much more complex to manage in large networks.

D: If you do not have a DHCP server, the new interface will obtain a network address using Automatic Private IP Addressing (APIPA).

Reference:

Deborah Littlejohn Shinder, and Dr. Thomas W. Shinder; MCSA/MCSE Implementing, Managing, and Maintaining a Windows Server 2003 Network Infrastructure Guide & DVD Training System, Chapter 3, pp. 164.

William Boswell; Inside Windows Server 2003, Addison Wesley, Chapter 3.

QUESTION 122

You need to design an administration strategy for the the BH_MediDB database servers. You need to ensure that your solution meets business and technical requirements.

What should you do? (Each correct answer presents part of the solution. Choose TWO.)

- A. Create an organizational unit (OU) named BH_MediUsers for the BH_MediDB database users.
- B. Create an organizational unit (OU) named BH_MediServers for the BH_MediDB database servers.
- C. Create a Group Policy object (GPO) that enforces IPsec for the BH_MediUsers OU.
- D. Create a Group Policy object (GPO) that enforces the use of smart cards for the BH_MediServers OU.
- E. Use the account properties to force all users who have to log on to the BH_MediDB database servers to use smart cards.

Answer: B, D

Explanation: The case study says "Network Administrators should only be allowed to access NewApp database server by using smart card authentication. However, network administrator must be able to log on to users computers to fix problems without using a smart card".

Answer C and F combined would create the OU for the NewApp servers and then force anyone logging into the server directly (network administrators) to use smart cards. Since customers and users will be using the web based NewApp they will not be logging on interactively so the GPO won't apply to them

An organizational unit (OU) is an Active Directory container object used within a domain. An OU is a logical container into which you can place users, groups, computers, and other OUs. It can contain objects only from its parent domain. An OU is the smallest scope to which you can apply a Group Policy or delegate authority.

Smart Card Is Required For Interactive Logon - is an option used to designate that the user must use a smart card during the authentication process, which is found in Account Properties by clicking the account tab. Smart cards are portable, tamper-resistant hardware devices that store unique identification information for a user. They are inserted into a card reader attached to a computer and provide an additional physical identification component to the authentication process.

Incorrect Answers:

E: Turning this setting on would require smart card logon to all computers not just the app servers because it is tied with the user account not the server account.

Reference:

Dan Holme, and Orin Thomas; MCSA/MCSE Self-Paced Training Kit: Upgrading Your Certification to Microsoft Windows Server 2003: Managing, Maintaining, Planning, and Implementing a Microsoft Windows Server 2003 environment: Exams 70-292 and 70-296, Chapter, pp. 44-6 to 44-8.

QUESTION 123

You need to design a remote access strategy for Bilco Health. You need to ensure that your solution meets requirements of the Chief Network Administrator. What should you do? (Each correct answer presents part of the solution. Choose TWO.)

- A. Install an Internet Authentication Service (IAS) server at each office.
- B. Install a Routing and Remote Access (RRAS) server at each branch office and an Internet Authentication Service (IAS) server at headquarters.
- C. Configure all remote access computers as RADIUS clients.
- D. Configure remote access policies that only allow VPN access.
- E. Configure remote access policies that only allow dial-in access.
- F. Configure Routing and Remote Access (RRAS) servers as RADIUS clients.

Answer: B, F

Explanation: The Chief Network Administrator has the following requirement:

* "All doctors that require remote access to the network must be subject to the same remote access policies that will be defined by administrators in Montreal."

Therefore you need an IAS at headquarters that can control remote access policies. This will allow administrators at Montreal to design and manage remote access. All remote users must be subject to the same remote access policies so you should not have any other IAS servers. Instead, the branch offices should have RRAS servers configured as RADIUS clients so that they can forward connection requests from remote clients to the IAS server at Montreal.

Incorrect Answers:

- A: Having an IAS server at each office would mean duplicating remote access policies and would make it difficult for administrators at Montreal to manage centrally.
- C: Remote access users will connect to their nearest branch office which would have RRAS servers and not IAS servers. Therefore the RRAS servers should be configured as RADIUS clients and not the remote client computers. The RRAS servers would then be able to forward connection requests from remote clients to the IAS server at Montreal.
- D, E: You should implement RADIUS access rather than dial-in or VPN access.

Reference:

QUESTION 124

You need to design a site topology for the Bilco Heath network. You need to ensure

that your solution meets the business and technical requirements.
What should you do?

- A. Increase the replication interval between sites.
- B. Use SMTP as the protocol for replication.
- C. Base site links on the physical topology.
- D. Disable the Knowledge Consistency Checker (KCC).
- E. Manually configure site replication.

Answer: C

Explanation:

A site link is an Active Directory object that represents the physical connectivity between two or more sites. For replication to occur between sites, you must establish a link between the sites. There are two components to this link: the actual physical connection between the sites (usually a WAN link) and a site link object. The site link object determines the protocol used for transferring replication traffic (IP or SMTP) and governs when replication is scheduled to occur.

Incorrect Answers:

- A: The scenario states: "Replication latency between sites must be minimized." This option reduces the amount of traffic over the links, but also increases replication latency.
- B: SMTP can be used for replication between sites that are not connected with permanent connections (which are required for RPCs).
- D: Knowledge Consistency Checker (KCC) is a built-in service that runs on all domain controllers and automatically establishes replication connections between domain controllers in the same site and between bridgehead servers in different sites.

Reference:

Walter Glenn, and Michael T. Simpson; MCSE 70-297 Training Kit - Designing a Windows server 2003 Active Directory and Network Infrastructure, Chapter 5, pp. 5-23 to 5-27, and Glossary, pp. G-7.