



Exam : 070-285

Title : Designing a Microsoft Exchange Server
2003 Organization

Ver : 11-06-06

Topic 1, Woodgrove Bank, ScenarioBACKGROUND1.

Overview

Woodgrove Bank provides business banking and financial services throughout the world. The company is centrally administered from a main office in New York City.

1. Physical

Locations The company has 20 branch offices throughout the world.

Each branch office belongs to one of six regions.

No region contains more than four branch offices.

Each branch office has 800 users.

The main office has 1,000 users.

Many users work from home after business hours.

They access e-mail by using a Web interface.

1. Planned Changes

The company currently uses an outsourced Web-based messaging system.

They are implementing Exchange Server 2003.

Messages from the old messaging system will not be migrated.

There is no existing internal messaging environment.

SUPPORTING INFRASTRUCTURE1.

Directory Services

1. The company has a single Active Directory domain.

2. Each branch office has a single domain controller, which is configured as a global catalog server.

3. Each office connects directly to the Internet. The Internet connection in each office uses a perimeter network.

4. The internal firewall on the perimeter network in each branch office is configured so that domain member servers can be placed on the perimeter network.

1. Administration

1. The IT staff at the main office will control all new Exchange servers.

2. However, each region also has a server technician who must be able to modify the Exchange configuration on the server that contains mailboxes for that region.

BUSINESS REQUIREMENTS

1. Security

1. All servers that provide services to Internet users must be located in a perimeter network.

Other servers are not permitted in the perimeter networks.

2. The company requires end-to-end encryption when users access their e-mail by using the Internet.

3. All inbound e-mail must be scanned for viruses.

1. Interviews

Chief Executive Officer:

1. I know that the antivirus software for the Exchange system is purchased on a server-by-server basis.
2. I want to minimize the number of servers on which we must install the software.
3. We need to ensure that the failure of a single Microsoft Outlook Web Access server does not prevent our users from accessing their e-mail when they work from home.
4. We also need to ensure that the failure of any server will only have a minimal impact on the ability of users, in each branch office, to send and receive e-mail while they are in the office.

Messaging Infrastructure:

1. All user e-mail messages must be backed up daily.
2. If a failure occurs, as much data as possible must be recovered.
3. However, several mailboxes support customer service operations.
4. Messages sent to these mailboxes do not need to be backed up and they do not need to be recovered if a failure occurs.
5. Users who work from home will access e-mail by using their home Internet connections.
6. They will connect to a Microsoft Outlook Web Access server that is hosted at their local branch office.
7. All Outlook Web Access servers will be configured to require SSL-encrypted connections.

TECHNICAL REQUIREMENTS

1. E-Mail Clients: Users will use Microsoft Outlook to access e-mail in the new Exchange Server 2003 environment.

QUESTION 1

You need to design a storage strategy that meets all business and technical requirements.

What should you do?

- A. Create a storage group for each office. Within each storage group, create a single database.
- B. Create a storage group for each region. Within each storage group, create a single database.
- C. Create a storage group for each region. Within each storage group, create separate databases for each office in that region.
- D. Create a single storage group. Within that storage group, create a separate database for each office.

Answer: C

Explanation

All user e-mail messages must be backed up daily, so that in the event of a failure occurring, as much data as possible is recovered. The company has 20 branch offices throughout the world. Each branch office belongs to one of six regions. No region contains more than four branch offices. Each branch office has 800 users and has a single

domain controller, which is configured as a global catalog server. Each Exchange server can contain 4 storage groups, in which you can include 5 databases. In total you can split your users into 20 databases, which speeds up the recovery of any Exchange that crashes, by using a new Exchange feature called Recovery Storage Group.

They tell you that users will connect to a Microsoft Outlook Web Access server and that this server will be hosted at their local branch office. They have one central office, 6 regions and each branch contains no more than 4 offices.

This means that you require 7 Exchange servers 1 Server in the Central site and 1 per region, 4 storage groups per server, 1 database per group and 20 databases in each region branch office.

The Exchange store uses two types of databases: mailbox stores and public folder stores. These stores are organized into storage groups. An Exchange 2003 Enterprise server supports up to four storage groups. All of the databases in a storage group share a single set of transaction log files, a single backup schedule and a single set of logging and backup-related settings. How you configure your storage groups affects Exchange performance, including how long it takes to back up and restore Exchange databases. To achieve better performance, you should consider minimizing the total number of databases on each server. You should also maximize the total number of databases (five) per storage group, before creating any additional storage groups. To increase the time it takes to back up and restore Exchange, consider limiting the size of each of your Exchange databases so that you can recover each database in a reasonable amount of time.

Incorrect Answers:

A: This answer will result into many backup and restore time because every storage group uses its own transactions logs. It will work but it is not the best option in the scenario

B: This answer will result into a single database for several branch offices per region. This conflicts with the Chief Executive Officers point 4 : "We also need to ensure that the failure of any server will only have a minimal impact on the ability of users, in each branch office, to send and receive e-mail while they are in the office."

D: This will result in to less databases. This will only support 5 databases maximum.

Reference:

MS white paper Exchange Server 2003 High Availability Guide

MS white paper Exchange Server Using Exchange Server 2003 Recovery Storage Groups.doc

<http://go.microsoft.com/fwlink/?LinkId=23233>

QUESTION 2

You need to design an administrative model that meets all business and technical requirements.

What should you do?

A. Place the mailboxes for each region on a separate server. Create an administrative group for each region.

Assign each regional technician Exchange Full Administrator permission over that

region's administrative groups. Assign the main office IT staff Exchange Full Administrator permission over each administrative group.

B. Place the mailboxes for each region on a separate server. Create an administrative group for each region.

Assign each regional technician Exchange Full Administrator permission over all administrative groups.

Assign the main office IT staff Exchange Full Administrator permission over each administrative group.

C. Place the mailboxes from multiple regions on each server. Create an administrative group for each server.

Assign each regional technician Exchange Full Administrator permission over the administrative groups that contain servers that hold mailboxes for that region. Assign the main office IT staff Exchange Full Administrator permission over each administrative group.

D. Place the mailboxes from multiple regions on each server. Create a single administrative group for all servers. Assign each regional technician and the main office IT Staff Exchange Full Administrator permission over the administrative group.

Answer: A

Explanation

They tell you that the IT staff at the main office will control all new Exchange servers.

However, each region also has a server technician who must be able to modify the Exchange configuration on server that contains mailboxes for that region although they told us that must be able to modify the configuration they do not tell us if they need to be able to modify the permissions.

When you assign a user or a group Exchange Full Administrator permissions, the user or the group can fully administer Exchange Server computer information and modify permissions. Administrators, who have Exchange Full Administrator permission can install, upgrade, remove, and perform disaster recovery on servers in that Administrative Group.

Incorrect Answers

B: This will give too much permission for Regional Technicians over other Administrative Groups. This conflicts with the administration requirement point 2 :

"However, each region also has a server technician who must be able to modify the Exchange configuration on the server that contains mailboxes for that region."

C, D: These place mailboxes from multiple regions on each server. This conflicts with the Chief Executive Officers point 4 : "We also need to ensure that the failure of any server will only have a minimal impact on the ability of users, in each branch office, to send and receive e-mail while they are in the office."

Reference

Overview of Exchange Administrative Role Permissions in Exchange 2003 KB article 823018

QUESTION 3

You need to design a strategy for managing the messages that are sent to the customer service mailboxes.

What should you do?

A. Create a separate storage group and database to contain the customer service mailboxes.

Enable circular logging for this storage group.

B. Create a separate storage group and database to contain the customer service mailboxes.

Set the deleted item retention period for this database to zero.

C. Place the customer service mailboxes on a new mailbox store in the storage group that contains the main office user mailboxes. Enable circular logging for this storage group.

D. Place the customer service mailboxes on a new mailbox store in the storage group that contains the branch office user mailboxes. Set the deleted item retention period for this database to zero.

Answer: A

Explanation

Circular logging is a feature that allows log files to be overwritten by new log files after the transactions in the original log file have been committed to the database. Circular logging is defined at the storage group level and it should be taken into consideration when managing stores and storage groups. Although circular logging uses transaction log techniques, it does not maintain previous transaction log files for long periods of time.

Instead, Exchange Server maintains a few log files (typically, a set of four log files), renames older logs, and overwrites the oldest log when a new transaction log file is needed. By default, circular logging is disabled in Exchange Server. The main advantage of circular logging is that it reduces the use of hard disk space. You can use circular logging to reduce the buildup of transaction log files.

The main disadvantage of circular logging is that if the database fails, only the data from the last backup of the database will be restored. Only the most recent backup of the database is restored because more recent database transactions have been overwritten.

So we need to configure a separate storage group that contains all customer services mailboxes and choose not to backup that storage group. By enabling circular logging we have get more free disk space.

Incorrect Answers :

B,D: When you use the Exchange Task Wizard to delete a mailbox, by default, the mailbox is disconnected but not immediately deleted. The mailbox is flagged for deletion and can be recovered if necessary. The mailbox will be permanently deleted at the end of the mailbox retention period that is configured in the mailbox store properties. If the deleted item retention period is set to 0, the deleted items are permanently removed from the server immediately.

C: If we enable circular logging on a storage group, then it will be enabled on all databases. Then it would be enabled on non-customer service as well. This conflicts with the Messaging Infrastructure Officers point 2 : "If a failure occurs, as much data as possible must be recovered."

Reference

XADM: How Circular Logging Affects the Use of Transaction Logs KB article 147524

QUESTION 4

You need to design the Exchange 2003 server configuration for remote e-mail access.

What should you do?

- A. Configure the front-end servers in each branch office to be members of a new Active Directory site.
- B. Configure the back-end servers to have server encryption certificates issued by a commercial certification authority (CA).
- C. Configure two back-end servers to be members of a Network Load Balancing cluster. Configure Network Load Balancing for inbound RPC connections.
- D. Configure multiple front-end servers in each branch office to be members of a Network Load Balancing cluster. Configure Network Load Balancing for inbound HTTPS connections.

Answer: D

Explanation

Support for front-end and back-end server configuration

This configuration improves performance and provides scalability of Exchange Server 2003. In a front-end/back-end server configuration, OWA clients connect to Exchange servers designated as front-end servers. Front-end servers then proxy the client request to the back-end Exchange server where the user mailbox is located. The best way to secure the OWA connection is by configuring SSL on the frontend server.

If you deploy OWA in a front-end and back-end server topology, you cannot use SSL to encrypt traffic between the front-end server and the back-end server. A front-end server can use only port 80 to communicate with a back-end server.

If secure communication is required between the front-end and back-end servers, configure Internet Protocol security (IPSec) between the front-end and back-end servers.

Network Load Balancing (NLB) is a service provided by Microsoft Windows Server 2003. This service dynamically distributes Internet Protocol (IP) traffic to multiple front-end servers, transparently distributing client requests among the front-end servers and allowing clients to access their mailboxes by using a single server namespace. The clients recognize the front-end servers as a single server that responds to the requests of clients.

Incorrect Answers:

A: This is already been done by default. However we still do not comply with the Chief Executive Officers point 3 and 4.

B: The frontend servers should have certificates, because OWA client will connect to the frontend server.

C: The back-end server should not be Load balanced, the Front-end servers should be Load balanced. And it still does not comply with the Chief Executive Officers point 3.

QUESTION 5

You need to design the deployment of antivirus software. What should you do?

- A. Install the antivirus software on each mailbox storage server.

- B. Install the antivirus software on each Outlook Web Access server.
- C. Install the antivirus software on one Outlook Web Access server at each office.
- D. Install the antivirus software on a back-end server that contains no mailboxes.

Answer: A

Explanation

They do not offer an infrastructure using SMTP in and out connector to access Exchange server. If the requirement of the CIO is to reduce the numbers of servers that will have AV installed and also to protect the external and internal system, the AV should be installed in the Mailbox server. Front end servers do not have mail enabled recipients.

Incorrect Answers :

B,C: The Front-end OWA Servers do not contain mailboxes, so installing antivirus software on them will not be of any use.

D: The antivirus software should be installed on servers that contain mailboxes

Reference

MS white paper Slowing and Stopping E-Mail Transmitted Viruses in an Exchange 2003 Environment

QUESTION 6

You need to design access to e-mail by Internet users. What should you do?

- A. Configure front-end servers to use HTTP to communicate with back-end servers.
- B. Configure the internal firewall to allow IPSec traffic between front-end and back-end Exchange servers.
- C. Require all users to encrypt all outbound e-mail messages.
- D. Issue digital certificates to all remote users. Require the certificates to be used when authenticating to Outlook Web Access.

Answer: D

Explanation

Support for front-end and back-end server configuration

This configuration improves performance and provides scalability of Exchange Server 2003. In a front-end/back-end server configuration, OWA clients connect to Exchange servers designated as front-end servers. Front-end servers then proxy the client request to the back-end Exchange server where the user mailbox is located. The best way to secure the OWA connection is by configuring SSL on the frontend server and issue certificates to all remote users.

If you deploy OWA in a front-end and back-end server topology, you cannot use SSL to encrypt traffic between the front-end server and the back-end server. A front-end server can use only port 80 to communicate with a back-end server.

If secure communication is required between the front-end and back-end servers, configure Internet Protocol security (IPSec) between the front-end and back-end servers.

Incorrect Answers :

A: This will work. However it still conflicts with the security requirement 2 : "The company requires end-to-end encryption when users access their e-mail by using the Internet."

B: This is certainly a good thing to configure. However we must have a secured connection between the OWA client and the front-end server. So this conflicts with the security requirement 2 : "The company requires end-to-end encryption when users access their e-mail by using the Internet."

C: The remote users are connecting on the front-end server, thus they are actually working remotely on that server. Sending encrypted email from that server to other recipients still conflicts with the security requirement 2 : "The company requires end-to-end encryption when users access their e-mail by using the Internet." The connection to the front-end server must be secured, not the email messages.

Topic 2, Fourth Coffee, Scenario

Total time until final review 30 minutes

BACKGROUND

1. Overview

Fourth Coffee is an international company that operates 24 hours a day and supplies coffee to retailers around the world.

1. Physical Locations

The company has a main office and seven branch offices.

The main office is located in Sydney.

The branch offices are located in

1. Auckland
2. San Paulo
3. Johannesburg
4. London
5. Helsinki
6. Seattle
7. New York

*** Planned Changes**

The company plans to upgrade from Exchange Server 5.5 to Exchange Server 2003.

EXISTING MESSAGING ENVIRONMENT

1. Administrative Structure

1. The current Exchange Server 5.5 environment contains eight sites. Each office is configured as a separate site.
2. A centralized administrative model is used in the organization. All the Exchange administration and configuration take place at the main office.
3. Exchange administrators are responsible for the creation of mailboxes and configuration of the Exchange servers. The Exchange administrators do not have Domain Admin rights.
4. Domain administrators are responsible for daily administration and networking tasks.

1. Messaging Infrastructure

1. The name of the existing Exchange Server 5.5 organization is Fourth Coffee. The organization contains an SMTP address of @fourthcoffee.com.
2. The Exchange Server 5.5 routing topology was created by using X.400 connectors.
3. The main office has two dedicated Internet Mail Connectors that are responsible for sending and receiving e-mail messages from the Internet.

1. E-Mail Clients

1. Fourth Coffee uses Microsoft Outlook 2002 as its e-mail client.
2. The network currently supports MAPI, HTTP, HTTPS, and SMTP.

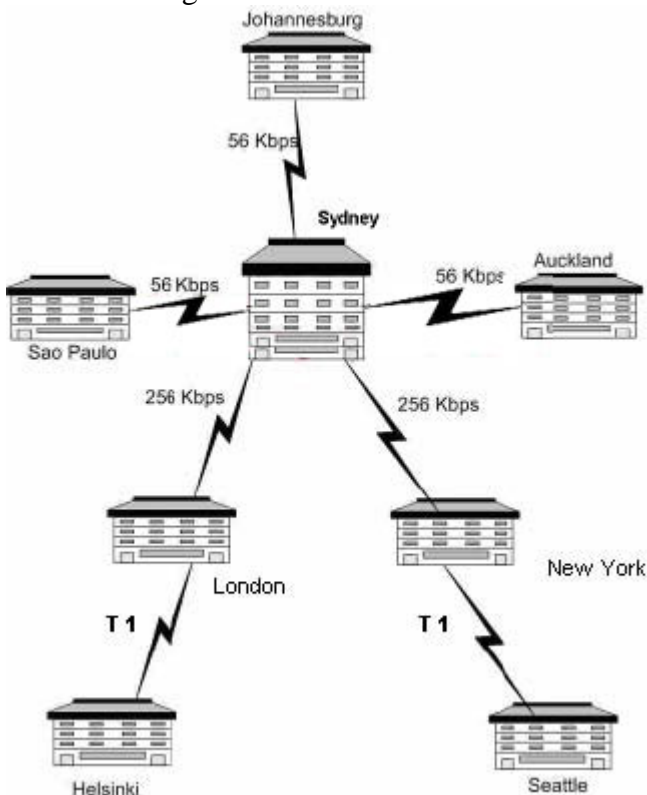
SUPPORTING INFRASTRUCTURE

1. Directory Services

1. Fourth Coffee is in the process of migrating to a single-domain forest named fourthcoffee.com.
2. The functional level of the domain and the forest is Windows Server 2003.
3. On the network, domain controllers are named DC2, DC2, etc., and global catalog servers are named GC1, GC2, etc.

1. Network Infrastructure

1. The existing network infrastructure is shown in the following diagram.



2. The WAN connection between the Seattle and New York offices is 10 percent utilized.
3. The WAN connection between the Helsinki and London offices is also 10 percent utilized. All the other WAN connections are approximately 65 percent utilized.
4. Because the WAN connection between Johannesburg and the main office is unreliable, VPN exists as a backup between the Johannesburg and Sydney offices. A VPN connection is created over a public network.

BUSINESS REQUIREMENTS

1. Security

1. The company requires that all users use Outlook Web Access or Microsoft Outlook 2003.

2. The company requires remote users to use encryption for remote connections.

1. Interviews

Chief Executive Officer:

1. Sales personnel need to be able to read and send e-mail messages and schedule meetings while they are offline.
2. E-mail messages and meeting requests should be sent automatically when the sales personnel connect to the Exchange servers from remote locations.

Chief Information Officer:

1. Due to competitive pressures, we want to change the name of our Exchange organization but still keep our SMTP namespace.
2. There is no budget for additional migration tools or external consultants.
3. During the migration process, managers must still be able to schedule meetings and view the calendars of other managers.

Exchange Administrator:

1. As part of the design and migration strategy, we want to consolidate the Exchange Server 5.5 servers.
2. We want to be able to migrate mailbox directory information and populate Active Directory with account information.

End User:

1. The public folder server is constantly unavailable.
2. We need to be able to access public folders on a regular basis.

TECHNICAL REQUIREMENTS

1. Messaging Infrastructure

1. Two connectors will be used to send and receive e-mail messages from the Internet.
2. The company wants all inbound Internet e-mail messages to flow through EX1. If EX1 is not available, the company wants the e-mail messages to flow through EX3. EX1 and EX3 are located at the main office.
3. The new environment must coexist with the existing Exchange Server 5.5 environment, including the public folders.
4. The company plans to install and configure Exchange Server 2003 on new computers.
5. All SMTP from the Internet for the fourthcoffee.com namespace must be delivered to the Exchange Server 2003 computer.
6. The company plans to use Microsoft Internet Security and Acceleration (ISA) Server, Enterprise Edition, to create a perimeter network. The server will be named ISA1.

1. Supporting Infrastructure

1. Users need to be able to access the online global address list in the case of a failure of a WAN connection or single server.
2. You must use the minimum number of global catalogs possible to ensure logon and global address list functionality without excessively burdening the network.
3. You also need to minimize the number of DNS lookups for mail deliver and ensure that DNS lookups take place on only the servers in the main office.

4. Shared resources in the existing Microsoft Windows NT domain must be accessible by users in both the new Active Directory domain and the Windows NT domain.

1. E-mail Client Infrastructure

1. The e-mail clients and desktop computers will be upgraded to use Outlook 2003 exclusively.

2. Client computers that connect to the Outlook Web Access servers use Internet Explorer 5.5 with SP2 or a more recent version.

3. The company wants MAPI, HTTPS, and SMTP to be the only protocols that are supported.

Topic 2, Fourth Coffee (6 Questions)

QUESTION 7

You need to design a migration path for migrating user accounts and mailboxes to the new environment.

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

A. Use the Migration Wizard to create and migrate mailboxes to Exchange Server 2003.

B. Use Active Directory Users and Computers to move user accounts and mailboxes to the new environment.

C. Use Microsoft Identity Integration Server (MIIS) to synchronize user accounts with the new environment.

D. Use the Active Directory Migration Tool (ADMT) to clone user accounts in Active Directory.

E. Use ClonePrincipal to migrate user accounts to the new environment.

Answer: A, D

Explanation

They ask that the new environment must coexist with the existing Exchange Server 5.5 environment, including the public folders. They also tell to you that Fourth Coffee is in the process of migrating to a single-domain forest named fourthcoffeee.com and that the functional level of the domain and the forest is Windows Server 2003. With Exchange 2003 SP1 you can use Exchange migration wizard to move mailbox in different sites to a new Exchange Organization. You will need to use ADMT v 2.2 to perform the migration, because you are not just migrating a user, but a user mailbox enabled in an Exchange Organization from different sites, because ADMT supported the security translation of Exchange 5.5 mailboxes. Also with the new beta ADMT v.3, new functionality enables you to perform interforest migrations of user mailboxes from a source domain to a target domain., also you need shared resources in the existing Microsoft Windows NT domain to be accessible by users in both the new Active Directory domain and the Windows NT domain.

Incorrect Answers:

B: This is not possible since we are migrating to a new forest

C: Microsoft Identity Integration Server is normally used to synchronize objects between Active Directory forests.

E:ClonePrincipal does migrate user accounts to the new environment but it does not

migrate ACL's to shared resources. This conflicts with the supporting infrastructure technician point 4 : "Shared resources in the existing Microsoft Windows NT domain must be accessible by users in both the new Active Directory domain and the Windows NT domain."

References

Exchange 2003 Deployment Guide - page 82.

<http://www.microsoft.com/technet/prodtechnol/exchange/2003/library/depguide.mspx>

How To Set Up ADMT for a Windows NT 4.0-to-Windows Server 2003 Migration

Migration Tool (ADMT) Version 3 release notes

Chapter 10 - Determining Domain Migration Strategies

<http://www.microsoft.com/technet/prodtechnol/windows2000serv/deploy/cookbook/cookchp4.mspx>

QUESTION 8

You need to design a migration strategy to migrate public folders from the existing Exchange Server 5.5 environment to the Exchange Server 2003 environment.

What should you do?

- A. Install and configure the Exchange utility. Use the utility to migrate and import all calendar information into each new mailbox.
- B. Install and configure the InterOrg Replication Utility. Use the utility to migrate public folder information from Exchange Server 5.5 to Exchange Server 2003.
- C. Install and configure a public folder connection agreement. Use this agreement to migrate the public folder information from Exchange Server 5.5 to Exchange Server 2003.
- D. Run the pfmigrate command to migrate the public folder information from Exchange Server 5.5 to Exchange Server 2003.

Answer: B

Explanation

If Exchange Server 2003 was deployed into a new Exchange Server organization instead of joining the existing Exchange Server 5.5 organization, you must use the Inter-Organization Replication tool to replicate free and busy information and public folder content between Exchange Server organizations. The tool allows for the coordination of meetings, appointments, contacts, and public folder information between disjointed Exchange organizations.

Incorrect Answers:

A: What exchange utility ? this answer is too vague

C: A public folder connection agreement is used to synchronize objects in the same forest.

D: If Exchange Server 2003 was deployed into an existing Exchange Server 5.5 organization, you can move mailboxes between servers using the Exchange Task Wizard. You can then migrate public folders using the Microsoft Exchange Public Folder Migration Tool (pfMigrate).

Reference:

<http://www.microsoft.com/technet/prodtechnol/exchange/guides/PlanE2k3MsgSys/e477a729-e0d9-44e3-816c-f3>

QUESTION 9

You need to ensure that SMTP e-mail messages can be delivered when the messages are sent to addresses that end with @fourthcoffee.com and are intended for the Exchange Server 5.5 environment.

Which three courses of action should you perform? (Each correct answer presents part of the solution. Choose three)

A. Create mail-enabled contacts in the fourthcoffee.com domain for each Exchange Server 5.5 recipient.

Establish the e-mail address to have an address that ends with @oldmail.fourthcoffee.com.

B. Create mail-enabled contacts in the fourthcoffee.com domain for each Exchange Server 5.5 recipient.

Establish the e-mail address to have an address that ends with @fourthcoffee.com

C. Configure each Exchange Server 5.5 recipient to have an address e-mail address that ends with @oldmail.fourthcoffee.com. Set the @oldmail.fourthcoffee.com address to be the default reply address.

D. Configure each Exchange Server 5.5 recipient to have an additional e-mail address that ends with @oldmail.fourthcoffee.com. Set the @fourthcoffee.com address to be the default reply address.

E. Configure each Exchange Server 5.5 recipient to use a single SMTP address that ends with @oldmail.fourthcoffee.com.

F. Configure an SMTP connector between the Exchange Server 2003 routing group at the Sydney office and the Exchange Server 5.5 site at the Sydney office.

Configure the connector namespace to be oldmail.fourthcoffee.com.

G. Configure an SMTP connector between the Exchange Server 2003 routing group at the Sydney office and the Exchange Server 5.5 site at the Sydney office.

Configure the connector namespace to be fourthcoffee.com.

Answer: A, D, F

Explanation

First, let's summon up the things we already know :

* Contacts that are configured with e-mail addresses are called mail-enabled contacts. A mail-enabled contact is a user who has neither an authentication account in Windows nor an Exchange mailbox in the associated Exchange organization. Mail-enabled contacts are visible in the global address list but receive their e-mail from an external system. An internal user can address an e-mail message to a contact simply by selecting the contact from the appropriate address list.

* from the Existing Messaging environment : "1. The name of the existing Exchange Server 5.5 organization is Fourth Coffee. The organization contains an SMTP address of @fourthcoffee.com."

* Interview with the Chief Information Officer : "1. Due to competitive pressures, we want to change the name of our Exchange organization but still keep our SMTP namespace."

* Interview with the Exchange Administrator : "1. As part of the design and migration

strategy, we want to consolidate the Exchange Server 5.5 servers." and "2. We want to be able to migrate mailbox directory information and populate Active Directory with account information."

* from the messaging technical requirements : "3. The new environment must coexist with the existing Exchange Server 5.5 environment, including the public folders." and "5. All SMTP from the Internet for the fourthcoffee.com namespace must be delivered to the Exchange Server 2003 computer."

Now we know that all inbound mail destined for fourthcoffee.com will delivered to a exchange 2003 server called EX1 or Ex3.

Some users still have a mailbox on the exchange 5.5 server and will connect directly to that exchange 5.5 server, thus we need to configure communication between the EX1 or Ex3 to to deliver email to the Exchange 5.5 environment. We also know that the exchange 2003 servers are in a different exchange organization name then the exchange 5.5 servers.

A. This means mail can be sent to addresses in exchange 2003 GAL and that email can be sent easily via SMTP to a different domain.

D. Each 5.5 mailbox would retain its original email address so routing would be maintained and the secondary email address means that oldmail.fourthcofee.com mail would be delivered too keeping the two systems talking over smtp.

F. This would mean internally sent emails would route to the 5.5 system and replies to the old fourthcofee.com email would also route (since the mail enabled contacts would hold both fourthcofee.com and oldmail.fourthcofee.com addresses and the routing group connector would know what to do with the mail (different mail domain).

Incorrect Answers:

B. This would mean mail would never leave the exchange 2003 server without additional configuration.

C. This would mean that external mail would route here (especially with an MX record set) and all mail sent from 5.5 would return to 5.5. It would give users a different email address for external and internal mails (old replies would be the issue).

E. This will give issues with previously sent emails if someone replies to an old mail.

G. This would mean mail would never leave the exchange 2003 server

QUESTION 10

You need to configure the DNS server to allow delivery of e-mail messages.

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

A. Create a host (A) resource record for EX1.fourthcoffee.com on the internal DNS Server.

B. Create a host (A) resource record for EX1.fourthcoffee.com on the external DNS Server.

C. Create a host (A) resource record for EX3.fourthcoffee.com on the internal DNS Server.

D. Create a host (A) resource record for EX3.fourthcoffee.com on the external DNS Server.

- E. Create a mail exchange (MX) resource record for EX1.fourthcoffee.com on the external DNS server.
Set the preference to 10.
- F. Create a mail exchanger (MX) resource record for EX1.fourthcoffee.com on the internal DNS server.
Set the preference to 10.
- G. Create a mail exchanger (MX) resource record for EX3.fourthcoffee.com on the external DNS server.
Set the preference to 20.
- H. Create a mail exchanger (MX) resource record for EX3.fourthcoffee.com on the internal DNS server.
Set the preference to 20.

Answer: B, D, E, G

Explanation

A mail exchanger record is a DNS record that the e-mail server names for your domain so that you can receive SMTP e-mail from Internet hosts. Transferring messages between SMTP hosts is dependent on DNS. When an SMTP host sends an e-mail message to another SMTP host, DNS resolves the domain name of the receiving host to its name and then the Transmission Control Protocol/Internet Protocol (TCP/IP) address by first using MX records.

To receive e-mail from the Internet, you must configure MX records for all SMTP mail domains hosted on your network. Remote SMTP hosts use the MX records in external DNS servers to locate the messaging servers for your domain name. You must configure the MX records for all your SMTP address spaces. Secondly, to be able to recognize what host matches with your MX record, you will need two A records, one for each host. The interview with the Messaging Infrastructure Technician told us that : "2. The company wants all inbound Internet e-mail messages to flow through EX1. If EX1 is not available, the company wants the e-mail messages to flow through EX3. EX1 and EX3 are located at the main office." In case your mail server fails you'd like to still be able to receive incoming e-mail messages. For that to happen we need to configure two MX records with two different priorities. One for EX1 with a priority of 10, and one for EX3 with a priority of 20.

QUESTION 11

You need to design a migration strategy to migrate the Exchange Server 5.5 mailboxes.
What should you do?

- A. Create and configure a one-way recipient connection agreement from Active Directory to Exchange Server 5.5.
- B. Create and configure a configuration connection agreement between Exchange Server 5.5 and Active Directory.
- C. Create and configure an inter-organizational recipient connection agreement from Exchange Server 5.5 to Active Directory.
- D. Create and configure a two-way recipient connection agreement between Exchange

Server 5.5 to Active Directory.

E. Use Microsoft Identity Integration Server (MIIS) to synchronize objects between Exchange Server 5.5 and Active Directory.

Answer: C

Explanation

As we already know by reading the Interview with the Chief Information Officer : "1. Due to competitive pressures, we want to change the name of our Exchange organization but still keep our SMTP namespace."

This results in two separate exchange organizations that need to be connected to each other.

The Active Directory Connector (ADC) is used to synchronize directory information from Exchange Server 5.5 servers to Active Directory. Connection agreements are created within the ADC to specify the source and destination containers used in the synchronization process.

You can set the inter-organization connection agreement option on the Advanced tab of a ADC connection agreement properties sheet. This option allows Microsoft Exchange Server version 5.5 and Microsoft Exchange 2003 servers that are in two separate Exchange organizations to replicate directory information. The inter-organization option doesn't handle how objects are created; it only handles how proxies are generated. If the inter-organization option is not selected, ADC does not:

- * Match Custom Recipients to a mailbox enabled user.
- * Stamp msExchMasterAccountSID or legacyExchangeDN.
- * Matches a mailbox to a user that is only mail enabled.

References:

Exchange 2003 Deployment Guide - page 89.

<http://www.microsoft.com/technet/prodtechnol/exchange/2003/library/depguide.msp>

Chapter 3 - Deploying the Active Directory Connector

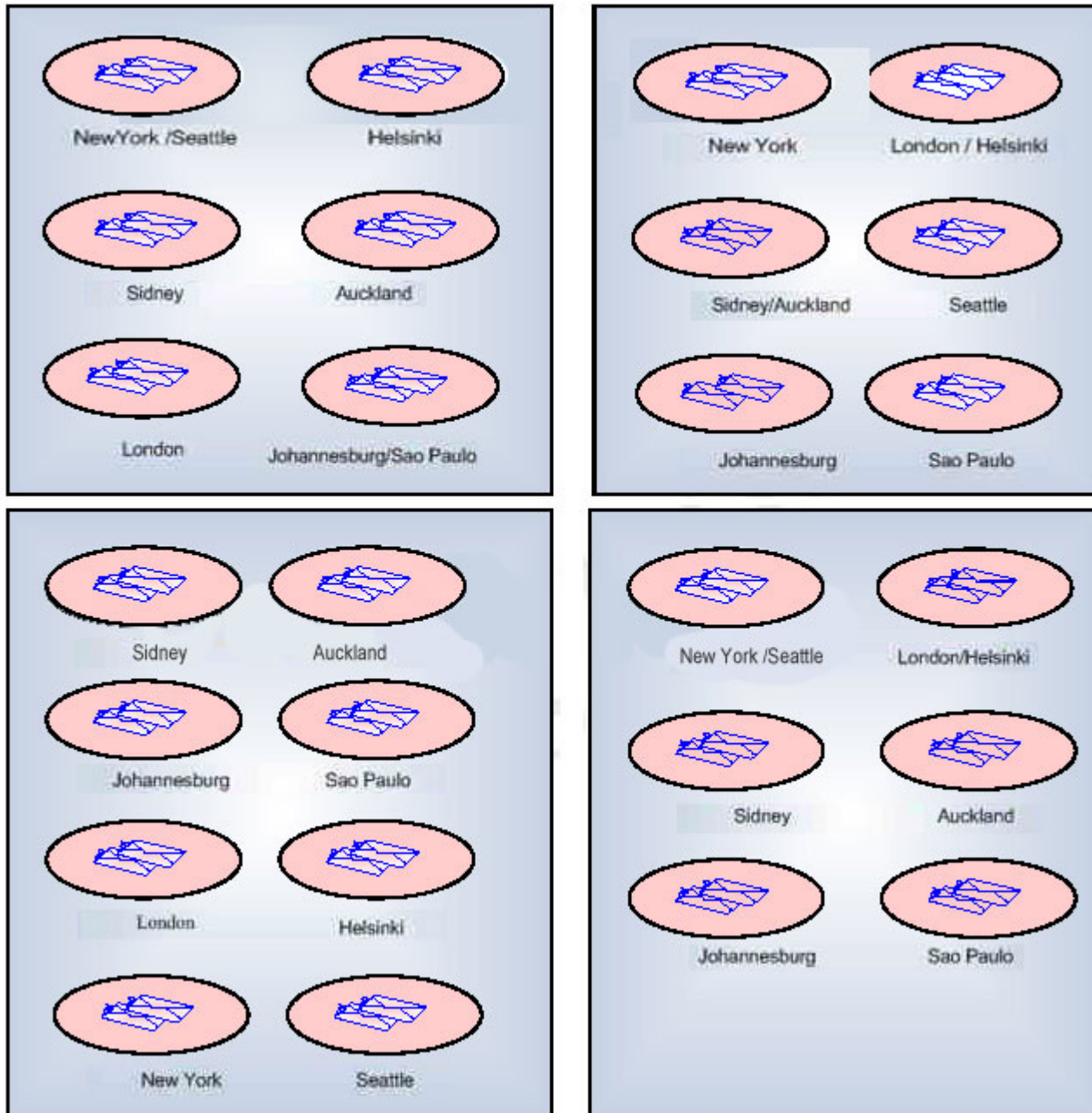
<http://www.microsoft.com/technet/prodtechnol/exchange/2000/depoly/upgrademigrate/series/deploymentguide/d>

Understanding Connection Agreements in Exchange

QUESTION 12

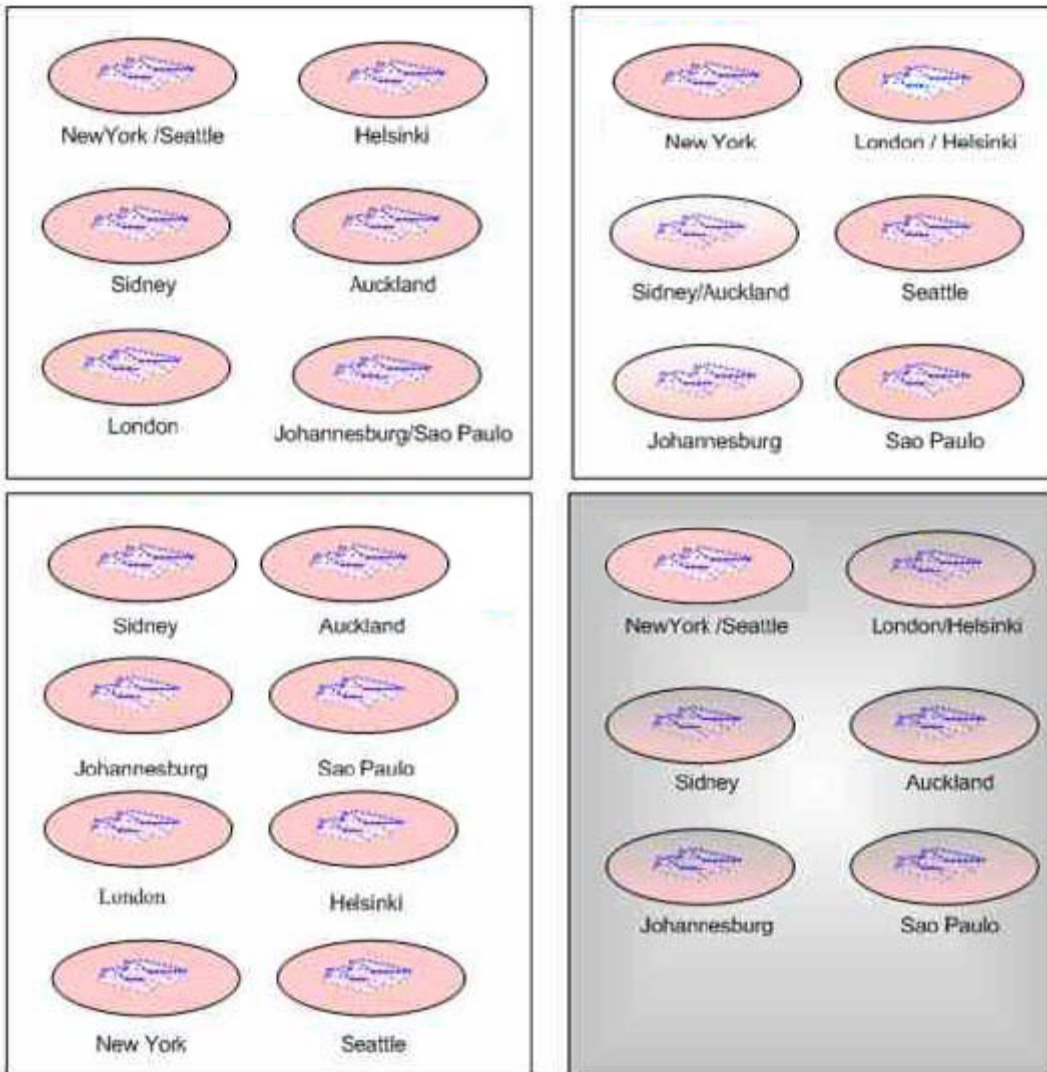
You need to minimize the amount of bandwidth that users use to access public folders.

Which routing groups should you create? (To answer, select the appropriate set of routing groups in the answer area.)



Answer:

Explanation:



Explanation

The company has a main office and seven branch offices.

The main office is located in Sydney.

The branch offices are located in Auckland, San Paulo, Johannesburg, London, Helsinki, Seattle, and New York.

1. The WAN connection between the Seattle and New York offices is 10 percent utilized.
2. The WAN connection between the Helsinki and London offices is also 10 percent utilized.
3. All the other WAN connections are approximately 65 percent utilized.

1. The company wants all inbound Internet e-mail messages to flow through EX1. If EX1 is not available, the company wants the e-mail messages to flow through EX3.

2. EX1 and EX3 are located at the main office. In order to keep network traffic at a minimum, you need to configure the replication times based on your available bandwidth.

A routing group is a collection of Exchange servers with full-time, highbandwidth, reliable connections. Within a routing group, all mail is transferred directly between servers. The most important factor to consider when you are planning routing group

boundaries is the stability of the network connections between the servers running Exchange Server.

You can implement a centralized messaging system if your company is composed of offices that are all connected by high-bandwidth, reliable network links, regardless of the distance between offices. This means that all Exchange servers are located and managed in a central data center and you will have a single routing group.

You can introduce routing groups to control how messaging traffic is routed from one location to another if your company contains remote offices that are connected by low-bandwidth, high-latency, unreliable network links.

Topic 3, Lucerne Publishing, Scenario

Total time until final review 20 minutes

BACKGROUND

1. Overview

Lucerne Publishing employs staff writers, editors, and production specialists, as well as contract writers.

The company provides messaging services to employees 24 hours a day, seven days a week.

1. Physical Locations

1. The main office includes 2,500 users.
2. A total of 50 users work from the remote locations and connect to the company resources by using various ISPs.

1. Planned Changes

1. The company currently uses an outsourced e-mail service and is implementing Exchange Server 2003 to replace that service.
2. E-mail messages from the service will not be migrated to Exchange.
3. The existing messaging infrastructure is outsourced.

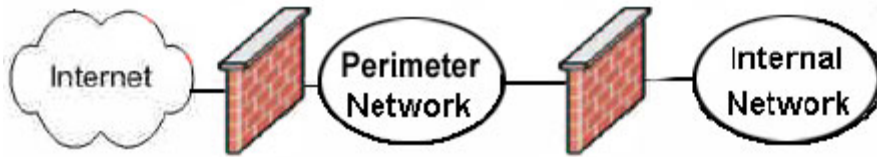
SUPPORTING INFRASTRUCTURE

1. Directory Services

1. The company network consists of a single Active Directory domain.
 2. All users have accounts in the Active Directory domain.
- ##### **1. Administrative Structure**
1. The company has a central Information Technology (IT) staff at the main office.
 2. One group of administrators is in the Default Domain Admins group and is responsible for all Active Directory administration.
 3. Another group of administrators is in a domain user group named Server Admins and is responsible for managing server and client hardware, operating systems, and applications.

1. Network Infrastructure

1. The main office has a high-speed connection to the Internet.
2. The main office network includes a perimeter network that connects the internal network to the Internet.
3. The network configuration of the main office is shown in the following diagram.



BUSINESS REQUIREMENTS

1. Security

1. All users must be able to send digitally signed messages no matter how they are accessing their e-mail
2. Email servers must be protected from external threats, however, requirements for configuring the firewalls must be minimized.
3. Members of the Server Admins group must not be required to have administrative permissions in Active Directory. However, they must be able to back up operating system files and shut down the operating system on Exchange Server 2003 computers.

1. Interviews

Chief Executive Officer:

1. We must have the most up-to-date and accurate backups of our e-mail.
2. We want to minimize the impact of this requirement on Exchange performance.
3. We want to use Windows-compatible backup software.
4. All non-executive mailboxes must have a size limit of 250 MB.
5. This limit must be the default for new mailboxes so that configuration management is minimized.
6. However, executive mailboxes must have a size limit of 500 MB.
7. This limit can be applied after the mailbox is created.
8. We also need to create the simplest possible storage configuration on the Exchange servers.

Chief Information Officer:

1. We plan to have one or more Exchange servers running Microsoft Outlook Web Access.
2. For both internal and remote users, we must minimize the impact of a single hardware failure in the messaging system.
3. However, we want to minimize the number of total servers used to run Exchange.
4. We want no more than 1,500 mailboxes on a single Exchange mailbox server.

TECHNICAL REQUIREMENTS

1. Messaging Infrastructure

1. The company will deploy Exchange Server 2003 as the new messaging platform.

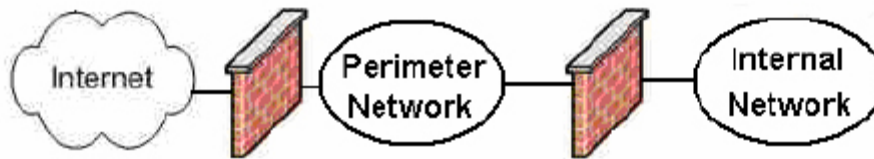
1. Supporting Infrastructure

1. Network traffic between the Exchange servers must be minimized

1. E-mail Client Infrastructure

1. All client computers at the main office run Microsoft Outlook 2003.
2. The company will run Outlook Web Access to give remote users access to e-mail.
3. Remote users will use Internet Explorer 6.0 or later to access e-mail.

1. Network Infrastructure



Topic 3, Lucerne Publishing (7 Questions)

QUESTION 13

You need to design a configuration for the mailbox servers. What should you do?

A. Create two Exchange Server 2003 computers.

Place the mailboxes for main office users on one server, and place the mailboxes for remote users on the other server.

B. Create a Network Load Balancing cluster that contains two Exchange Server 2003 computers.

Place half of the user mailboxes on one server, and place half of the user mailboxes on the other server.

C. Create a Microsoft Cluster Server cluster that contains two Exchange Server 2003 computers.

Place all of the user mailboxes on one server and configure the other server as a failover node.

D. Create a Microsoft Cluster Server cluster that contains two Exchange Server 2003 computers.

Place half of the user mailboxes on one server, and place half of the user mailboxes on the other server.

Answer: D

Explanation

The Interview with the Chief Information Officer tells us that : For both internal and remote users, we must minimize the impact of a single hardware failure in the messaging system. (Requirement 2) and : We want no more than 1,500 mailboxes on a single Exchange mailbox server. (Requirement 4) Windows Server 2003 provides two clustering technologies: server clusters and Network Load Balancing (NLB). Server cluster primarily provides high availability (for example mailbox servers); you can provide fault tolerance for your front-end servers by implementing Network Load Balancing, a service that is provided by Windows Server 2003. Network Load Balancing dynamically distributes IP traffic to multiple frontend servers, transparently distributing client requests among front-end servers and enabling clients to access their mailboxes by using a single server namespace. The clients recognize front-end servers as a single server that responds to their requests. If a front-end server becomes unavailable, the workload is redistributed to the remaining servers. Network Load Balancing provides load balancing and also a high level of fault tolerance, which is essential to ensuring high availability for client access to the front-end servers.

Incorrect Answers:

A. Then we would have 2500 mailboxes on one exchange server. This conflicts with the Chief Information Officer requirement 4 : We want no more than 1,500 mailboxes on a single Exchange mailbox server.

B. Network Load Balancing is not being used on back-end servers that contain mailboxes. It is used on front-end servers.

C. Then we would have 2500 mailboxes on one exchange server. This conflicts with the Chief Information Officer requirement 4 : We want no more than 1,500 mailboxes on a single Exchange mailbox server.

Reference:

MS white paper Exchange Server 2003 High Availability Guide

QUESTION 14

You need to design a configuration for Exchange Server storage that meets the business and technical requirements. What should you do?

A. Create a single storage group. Create one database for all users.

B. Create two storage groups. In each storage group, create one database.

Place mailboxes for remote users in one storage group database, and place all other mailboxes in the other storage group database.

C. Create two storage groups. In each storage group, create one database.

Place executive mailboxes in one storage group database, and place all other mailboxes in the other storage group database.

D. Create two storage groups.

In one storage group, create a database, and place all mailboxes for remote users and executives in the database.

In the other storage group, create a database for all other mailboxes.

Answer: C

Explanation

The Exchange store uses two types of databases: mailbox stores and public folder stores. These stores are organized into storage groups. An Exchange 2003 Enterprise server supports up to four storage groups. All of the databases in a storage group share a single set of transaction log files, a single backup schedule and a single set of logging and backup-related settings. How you configure your storage groups affects Exchange performance, including how long it takes to back up and restore Exchange databases. To achieve better performance, you should consider minimizing the total number of databases on each server. You should also maximize the total number of databases (five) per storage group, before creating any additional storage groups. To increase the time it takes to back up and restore Exchange, consider limiting the size of each of your Exchange databases so that you can recover each database in a reasonable amount of time.

The Interview with the Chief Executive Officer states that executive and non-executive mailboxes should have different mailbox size limits, therefore we need two databases. One for the executive mailboxes and one for the non-executive mailboxes.

Incorrect Answers:

- A. This will conflict with the Chief Executive Officer's requirements 4,5,6 & 7. that we need 2 databases
- B. We need 2 separate databases. One for the executive mailboxes and one for the non-executive mailboxes. there is no need to have a seperate database for the remote users.
- D. There is no requirement that tells us to give remote users a default mailbox limit of 500MB.

Reference:

MS white paper Exchange Server 2003 High Availability Guide

MS white paper Exchange Server Using Exchange Server 2003 Recovery Storage

Groups.doc

<http://go.microsoft.com/fwlink/?LinkId=23233>

QUESTION 15

You need to design a configuration for the Microsoft Outlook Web Access servers. What should you do?

- A. Create a Network Load Balancing cluster that contains the Outlook Web Access servers.
- B. Create a Microsoft Cluster Server cluster that contains the Outlook Web Access servers.
- C. Create public DNS host (A) resource records for each Outlook Web Access server. Instruct each user to connect to the server that contains his or her mailbox.
- D. Install Microsoft Application Center 2000 on the Outlook Web Access servers. Create a Web cluster that contains all of the Outlook Web Access servers.

Answer: A

Explanation

We need a high availability solution for the Front-end servers since the Chief Information Officer stated in requirement 2 : "For both internal and remote users, we must minimize the impact of a single hardware failure in the messaging system." You can provide fault tolerance for your front-end servers by implementing Network Load Balancing, a service that is provided by Windows Server 2003. Network Load Balancing dynamically distributes IP traffic to multiple frontend servers, transparently distributing client requests among front-end servers and enabling clients to access their mailboxes by using a single server namespace. The clients recognize front-end servers as a single server that responds to their requests. If a front-end server becomes unavailable, the workload is redistributed to the remaining servers. Network Load Balancing provides load balancing and also a high level of fault tolerance, which is essential to ensuring high availability for client access to the front-end servers.

Incorrect Answers:

- B. A cluster is being used in a back-end solution, not in a front-end.
- C. This conflicts with the Chief Information Officer stated in requirement 2 : "For both internal and remote users, we must minimize the impact of a single hardware failure in the messaging system." If one front-end server dies then the users will not be able to

access their mailbox.

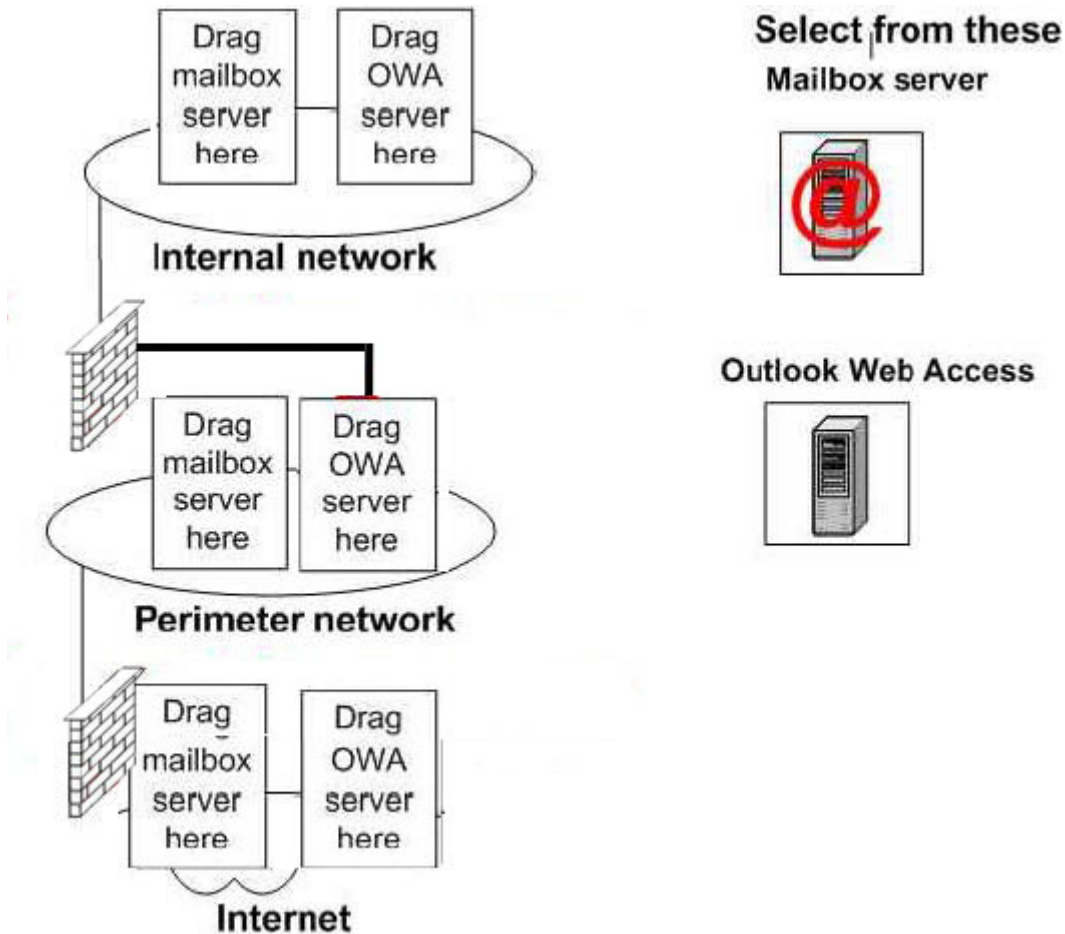
D.

Microsoft Application Center 2000 is Microsoft's deployment and management tool for high-availability Web applications built on the Microsoft Windows(r) 2000 operating system

QUESTION 16

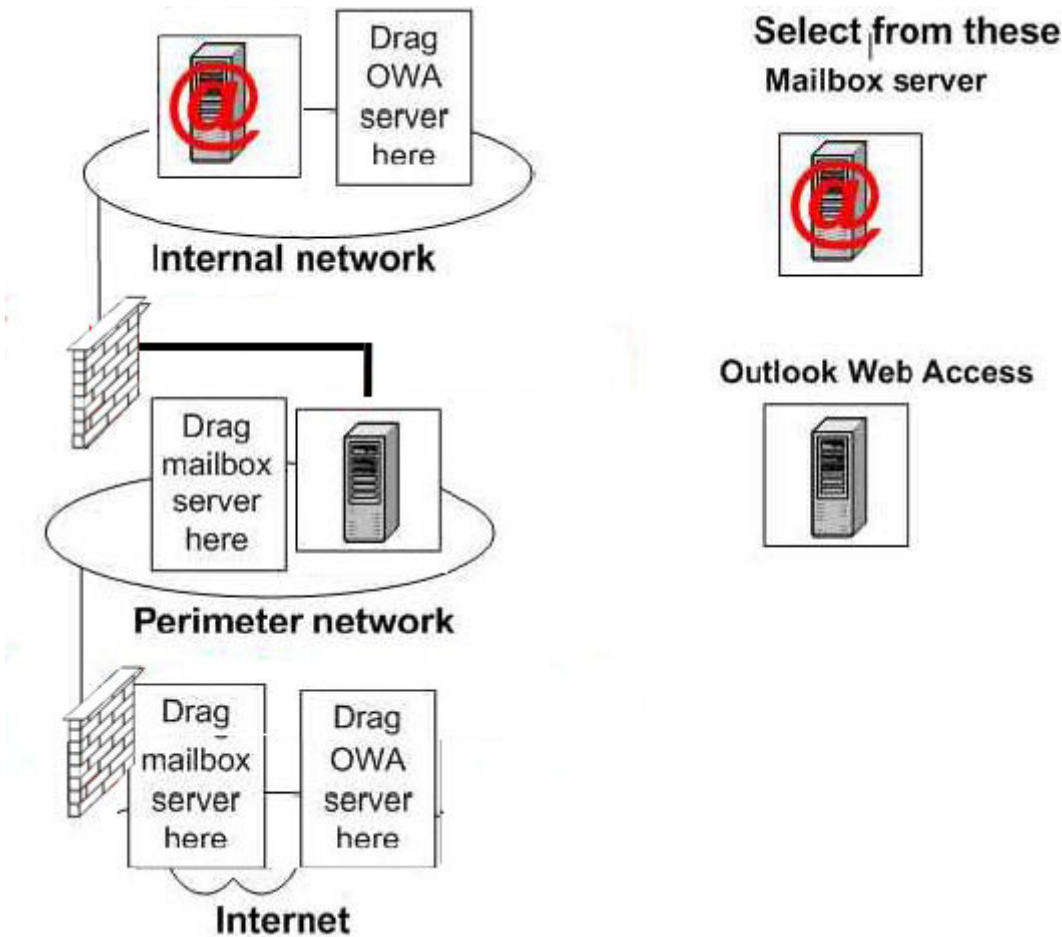
You need to design the network locations for the mailbox servers and Outlook Web Access servers. What should you do?

To answer, drag a mailbox server to the correct location or locations in the answer area.



Answer:

Explanation:



If you are deploying front-end servers to provide Internet client access and you want to make these services highly available, you must place at least two frontend servers for each protocol on the perimeter network.

The Back-end servers have mailboxes on them, they should be secured and being placed in the internal network.

You can use IPSec to secure intranet communication, not just message traffic, such as securing traffic between front-end and back-end servers.

QUESTION 17

You need to design access to Microsoft Outlook Web Access for remote users. What should you do?

- A. Place all user mailboxes on back-end servers. Deploy Outlook Web Access on three front-end servers that are members of the Network Load Balancing cluster.
- B. Place all user mailboxes on back-end servers that are members of a Network Load Balancing cluster. Deploy Outlook Web Access on the back-end servers.
- C. Place mailboxes for remote users on one back-end server and place all mailboxes for main office users on another back-end server. Deploy Outlook Web Access on the back-end server that contains the mailboxes for remote users.
- D. Place all user mailboxes on two back-end servers that are members of a Network Load Balancing cluster. Place mailboxes for remote users and mailboxes for main office users

into separate storage groups. Deploy Outlook Web Access on three front-end servers. Configure the front-end servers to access only the back-end Network Load Balancing cluster.

Answer: A

Explanation:

The Interview with the Chief Information Officer tells us that : For both internal and remote users, we must minimize the impact of a single hardware failure in the messaging system. (Requirement 2) and : We want no more than 1,500 mailboxes on a single Exchange mailbox server. (Requirement 4) Windows Server 2003 provides two clustering technologies: server clusters and Network Load Balancing (NLB). Server cluster primarily provides high availability (for example mailbox servers);you can provide fault tolerance for your front-end servers by implementing Network Load Balancing, a service that is provided by Windows Server 2003. Network Load Balancing dynamically distributes IP traffic to multiple frontend servers, transparently distributing client requests among front-end servers and enabling clients to access their mailboxes by using a single server namespace. The clients recognize front-end servers as a single server that responds to their requests. If a front-end server becomes unavailable, the workload is redistributed to the remaining servers. Network Load Balancing provides load balancing and also a high level of fault tolerance, which is essential to ensuring high availability for client access to the front-end servers.

Incorrect Answers:

- B. Back-end servers should be clustered, not Load Balanced.
- C. Outlook Web Access should be deployed on front-end servers, not back-end.
- D. Back-end servers should be clustered, not Load Balanced.

QUESTION 18

You need to design a security strategy for a remote e-mail access. What should you do?

- A. Require remote users to access e-mails by using Outlook Mobile Access.
- B. Require Outlook Web Access users to install the secure MIME ActiveX-Control and to encrypt all messages.
- C. On Outlook Web Access servers that accept connections from the Internet configure IIS to require SSL for all connections.
- D. On Outlook Web Access servers that accept connections from the Internet configure IIS to require Integrated Windows Authentication.

Answer: C

Explanation

It would require less administrative effort to provide access over https for OWA access. They also require being able to send digitally signed messages and encrypted messages so that they can use a PKI infrastructure by using public certificates or to use an S/MIME. And this needs to be secure in this case over SSL
To enable S/MIME connectivity for Outlook Web Access by downloading and installing

the S/MIME ActiveX control.

S/MIME provides two security services: Digital signatures and Message encryption. Message encryption makes the text of a message unreadable by performing an encryption operation on it when it is sent. When the message is received, the text is made readable again by performing a decryption operation when the message is read.

The encryption operation that is performed when the message is sent captures the e-mail message and encrypts it using information that is specific to the intended recipient. The encrypted message replaces the original message, and then the message is sent to the recipient.

Incorrect Answers:

A. If you want to access your mailbox using a smart phone or another WAP device you can use Outlook Mobile Access (OMA). However this is not required in this scenario.

B. The question states to design a secure strategy for remote email access. Not the e-mail messages itselfs.

D. This would still not encrypt the communication between the email client and the OWA server.

Reference

Quick Start for SMIME in Exchange Server 2003

<http://www.microsoft.com/technet/prodtechnol/exchange/2003/library/qssmimes.msp>

Exchange Server 2003 Message Security Guide.

<http://www.microsoft.com/technet/prodtechnol/exchange/2003/library/exmessec.msp>

QUESTION 19

You need to design an administrative model that meets the business and technical requirements. What should you do?

A. Assign permissions to manage Mailbox and Exchange Server configuration to the server-admins group.

B. Assign permissions to manage Mailbox and Exchange Server configuration to the domain-admins group.

C. Assign permissions to manage Mailboxes to the server-admins group. Assign permissions to manage Exchange Servers configuration to the domain-admins group.

D. Assign permissions to manage Mailboxes to the domain-admins group. Assign permissions to manage Exchange Servers configuration to the server-admins group.

Answer: D

Explanation

The security requirement 3 states : "Members of the Server Admins group must not be required to have administrative permissions in Active Directory. However, they must be able to back up operating system files and shut down the operating system on Exchange Server 2003 computers." The only answer that matches this is answer D.

Members of the server-admin group must be able to manage and shutdown Exchange servers or backup without permissions to Active Directory. The Exchange

Administration Delegation Wizard applies the standardized security roles at either the organization level or the administrative group level in Exchange System Manager . By

using the wizard, you can set all the permissions on the Exchange objects in both Active Directory and the IIS metabase with several clicks. You can set permissions using the Exchange Delegation Wizard and apply these settings to a whole Exchange organization or to a specific administrative group. Because permissions are inherited, these permissions control who can view or modify settings at the server level. By default, these permissions are configured to support the standard Exchange administrator types (Exchange View Only Administrator, Exchange Administrator, and Exchange Full Administrator)

Incorrect Answers:

A,C. The Server Admins group should not be able to manage mailboxes

B. Members of the server-admin group must be able to manage and shutdown Exchange servers or backup without permissions to Active Directory. This answer only assigns permissions to the Domain Admins group.

Reference

Exchange Server 2003 Administration Guide

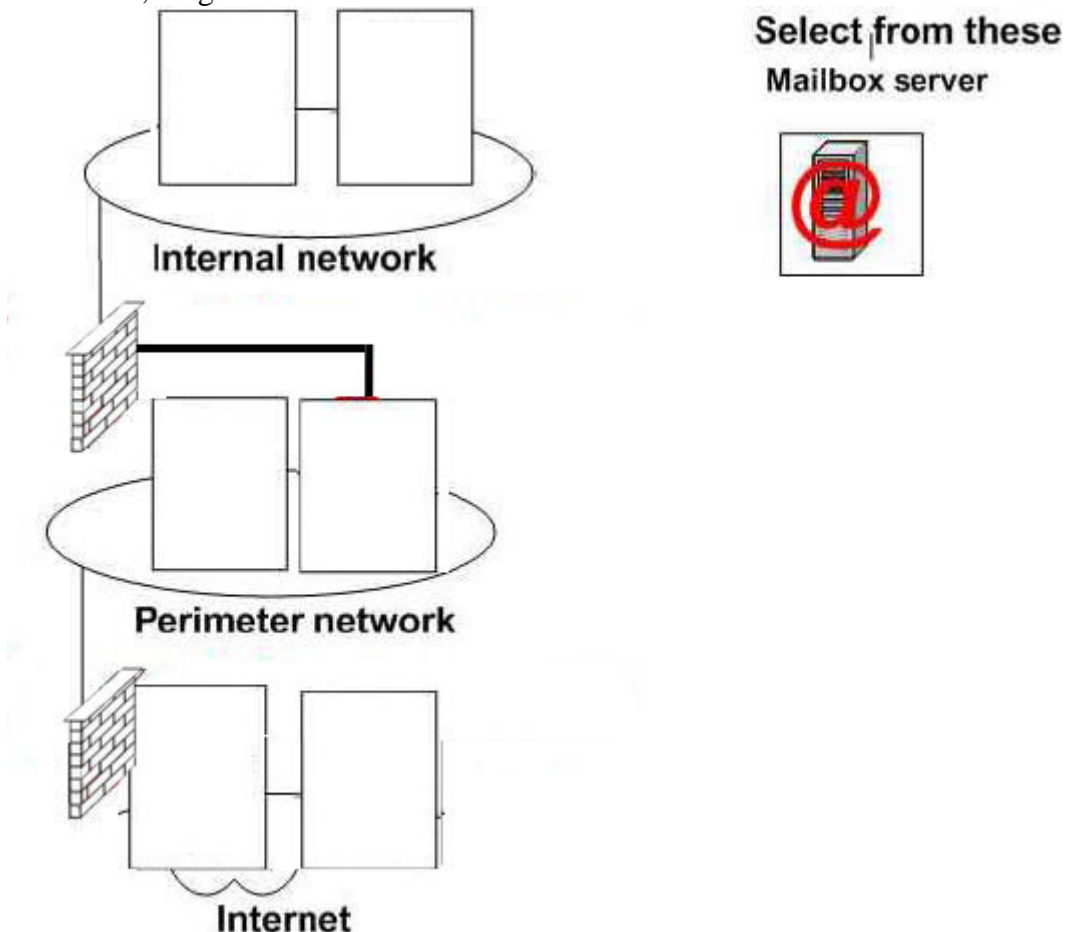
<http://www.microsoft.com/technet/prodtechnol/exchange/2003/library/admingde.mspx>

QUESTION 20

You need to design the network locations for the mailbox servers.

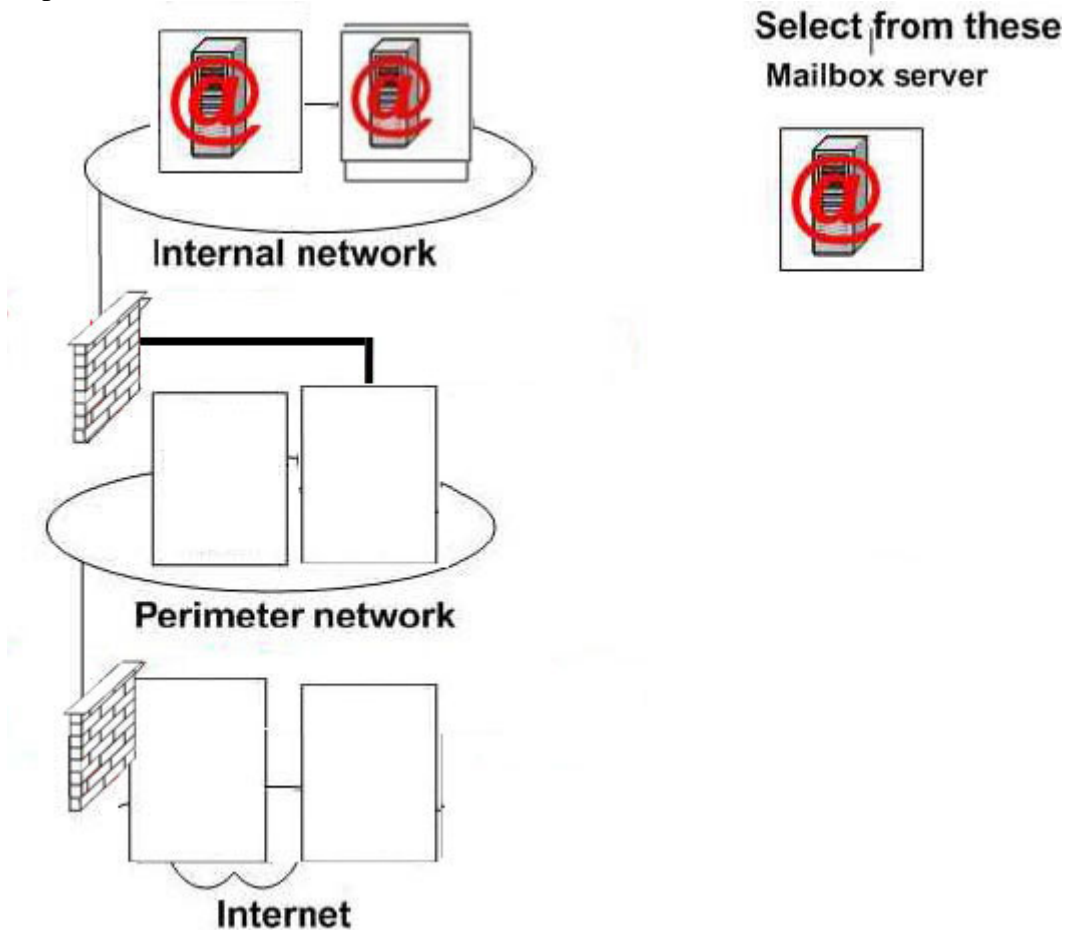
What should you do?

To answer, drag a mailbox server to the correct location or locations in the answer area.



Answer:

Explanation:



If you are deploying front-end servers to provide Internet client access and you want to make these services highly available, you must place at least two frontend servers for each protocol on the perimeter network. The Back-end servers have mailboxes on them, they should be secured and being placed in the internal network.

You can use IPSec to secure intranet communication, not just message traffic, such as securing traffic between front-end and back-end servers.

The Interview with the Chief Information Officer tells us that : For both internal and remote users, we must minimize the impact of a single hardware failure in the messaging system. (Requirement 2) and : We want no more than 1,500 mailboxes on a single Exchange mailbox server. (Requirement 4) Windows Server 2003 provides two clustering technologies: server clusters and Network Load Balancing (NLB). Server clusters primarily provide high availability (For example mailbox servers).

Now we know that we need two mailbox servers on the internal network.

Topic 4, City Power & Light, Scenario

Total time until final review 30 minutes

BACKGROUND

1. Overview

City Power & Light is a utilities company that operates throughout the United States.

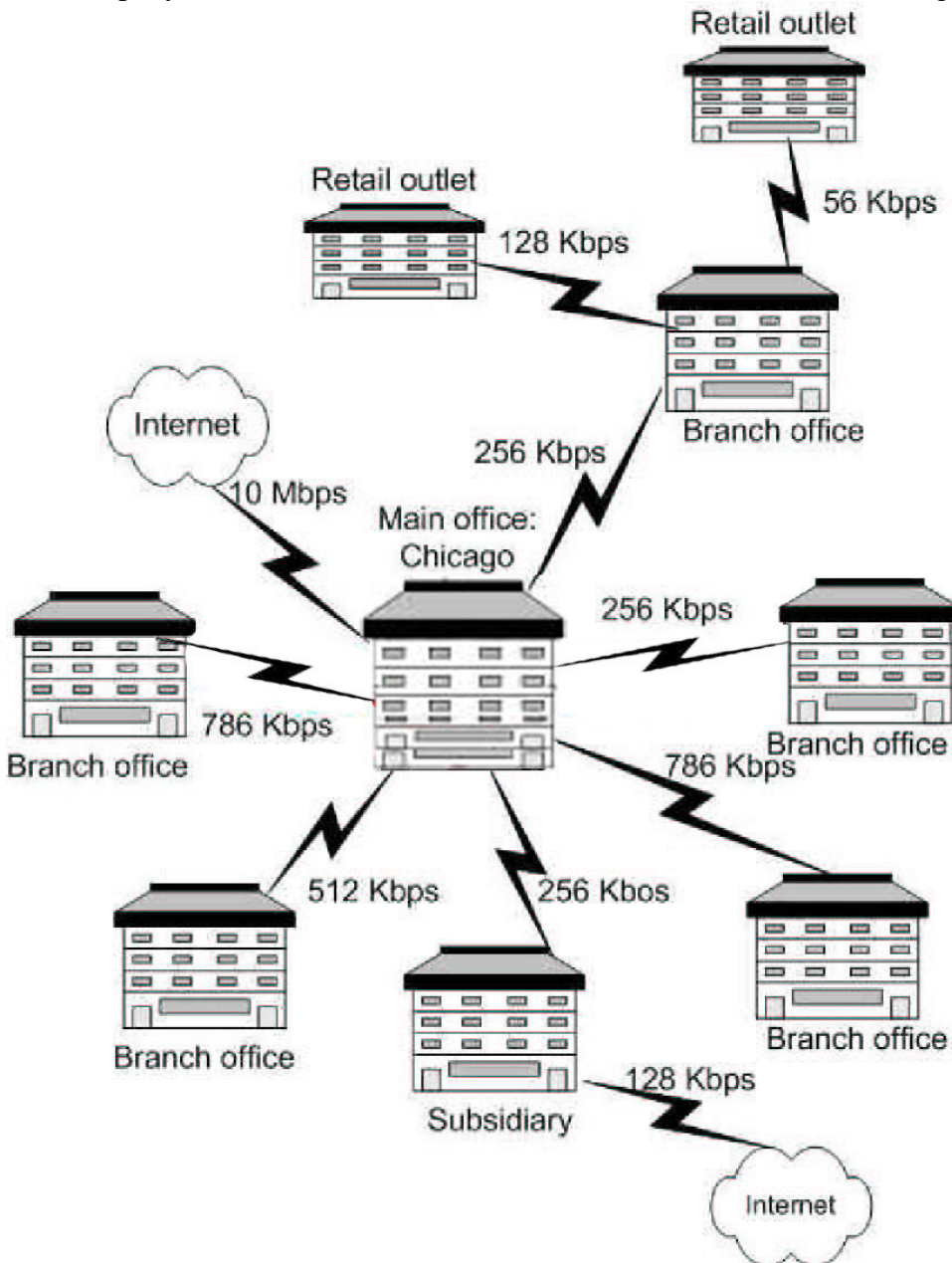
1. Physical Locations

The main office for City Power & Light is located in Chicago.

Other offices are

1. 5 Branch offices,
2. 200 Retail outlets,
3. 1 Subsidiary location.

The company locations and WAN connections are shown in the following diagram.



The number of users in each location is shown in the following table.

Office Location	Number of Users
Main office	1,400
Branch offices	25 in each office
Retail outlets	3 to 7 per retail outlet
Subsidiary	50

1. **Planned Changes**

1. City Power & Light uses Exchange Server 5.5 computers for all of its messaging services.
2. The company plans to upgrade to Exchange Server 2003.
3. The subsidiary also uses Exchange 5.5 servers in a separate organization.
4. The subsidiary will be closed over the next year, and all users will be moved to one of the existing company locations.

PROBLEM STATEMENTS

1. Information Technology (IT)
1. Administration at City Power & Light is decentralized.
2. A primary goal is to centralized IT administration.

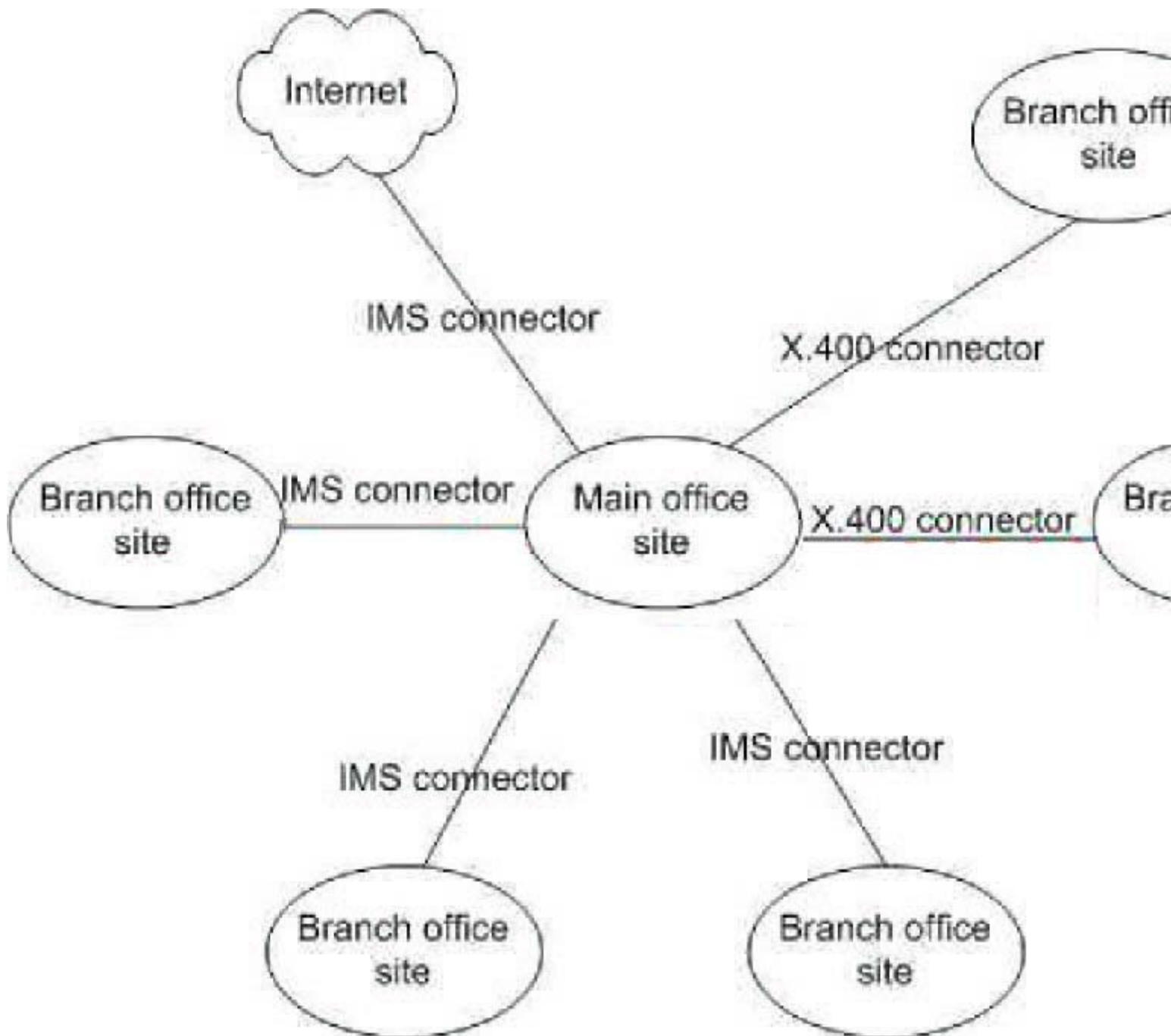
EXISTING MESSAGING ENVIRONMENT

1. Administrative Structure

1. Each branch office has at least one user who is a member of the Domain Admins group.
2. In total, there are about 75 users in the Domain Admins group, which has full control of the Exchange organization.

1. Messaging Infrastructure

The existing Exchange 5.5 site configuration is shown in the following diagram.



1. The main office contains three Exchange 5.5 servers.
2. One of the main office servers is a bridgehead server that is dedicated for connections to the Internet and the other sites.
3. The other two servers at the main office are mailbox servers.
4. Each branch office contains one Exchange 5.5 server.
5. City Power & Lights uses public folders extensively.
6. The public folder hierarchy is complicated, and permissions are assigned by using individual mailboxes and distributed lists throughout the public folder tree.
7. All public folders are replicated to each Exchange server in each office.

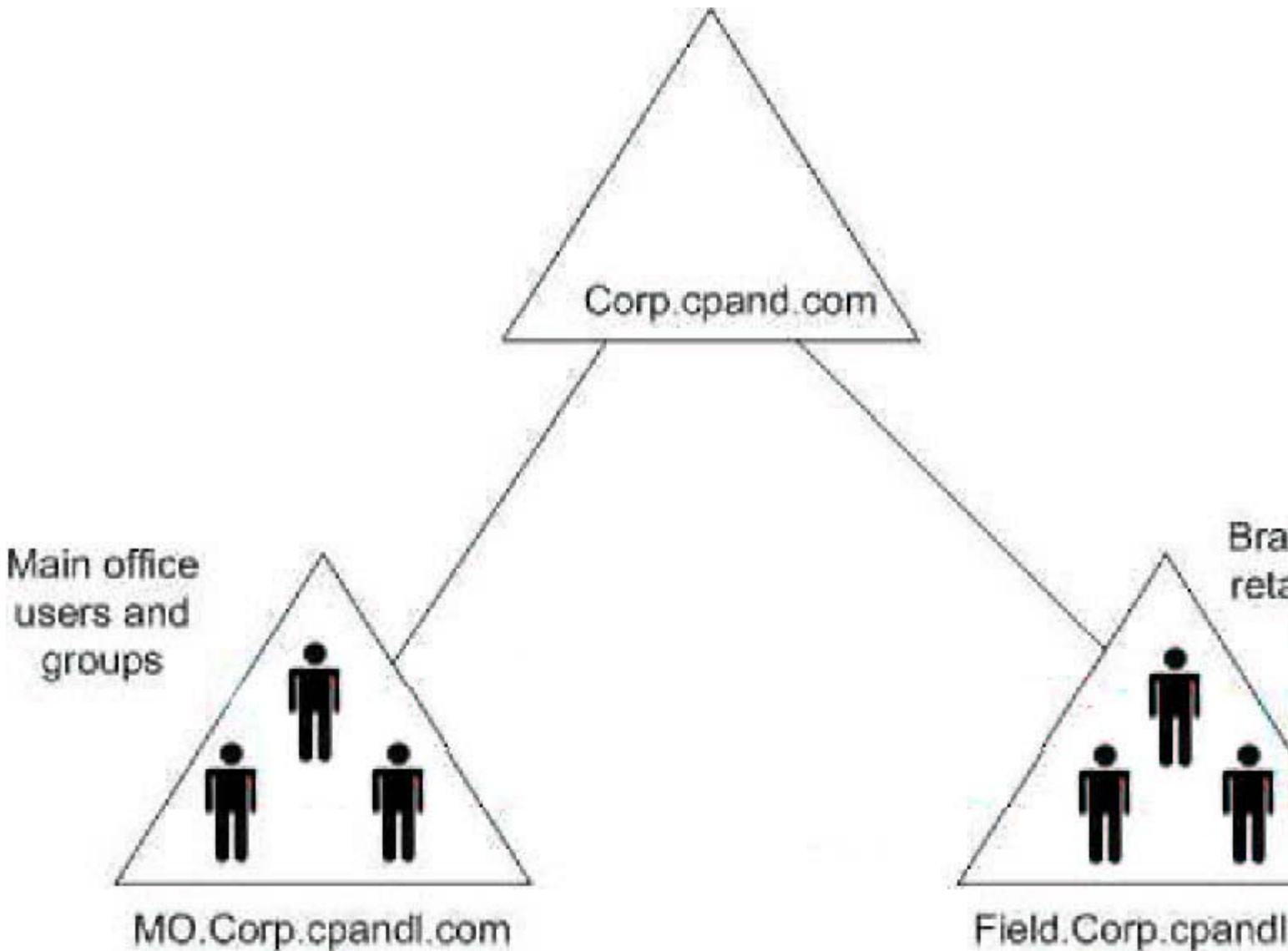
8. The company is trying to eliminate the practice of using individual mailboxes for public folder permissions.
 9. At least 100 distribution lists have been created just to manage permissions on the public folders.
 10. The distribution lists include members from multiple domains.
1. E-mail Clients
 1. All users at the main office and branch offices use either Outlook 2000 or Outlook 2003.
 2. Users at the retail outlets use Microsoft Outlook Express configured with POP3 accounts.
 3. The users connect to the Exchange server located in the nearest branch office.

SUPPORTING INFRASTRUCTURE

1. Directory Services

City Power & Light has completed the migration to Microsoft Windows Server 2003 Active Directory.

The Active Directory domain configuration is shown in the following diagram.



1. The Corp domain is running at Windows Server 2003 functional level.
2. The MO and Field domains were created by upgrading Windows NT 4.0 domains to Windows Server 2003 Active Directory.
3. Both domains still contain Windows NT 4.0 backup domain controllers.
4. The subsidiary runs a single Windows NT 4.0 domain.

1. Network Infrastructure

1. The company recently upgraded the WAN connections between company locations.
2. No additional WAN upgrades are planned.

1. Administration

1. Each time the domain controllers and Exchange servers are removed from the branch offices, the company needs to remove the branch office administrators from the domain-level administration groups.

1. Security

1. The company is concerned about users at the retail outlets accessing their e-mail messages across the Internet.
2. The client connection to the mailbox servers must be encrypted from the client computers to the mailbox server that hosts each user's mailbox.
3. The company has a perimeter network for all servers that are accessed from the Internet.

1. Interviews

Chief Information Officer:

1. We need to reduce the number of Exchange servers as much as possible.
2. By the end of the project, we must have only Exchange 2003 servers deployed.
3. The exception is the subsidiary. We are phasing out the Exchange 5.5 server over the next year.
4. We also have a long-term strategy to eliminate the Field.Corp.cpandl.com domain.
5. Although we will not be able to do this for a while, your implementation efforts should support that long-term strategy

Network Administrator:

1. We want to reduce the number of users in the Domain Admins group to fewer than five.
2. We also need to restrict who can manage the Exchange 2003 servers.
3. We want only the Domain Admins group and a Messaging Admins group to manage all the Exchange servers.
4. The Messaging Admins group should be able to administer the Exchange organization, but it should not be able to assign anyone else permission to manage the servers.
5. In addition, we want one administrator in each office that contains an Exchange server to be able to create mailboxes on the Exchange server in that office.
6. The administrator should not be able to modify any Exchange settings and should not be able to create mailboxes on an Exchange server in any other office.
7. We also want to configure some policies - such as an IPSec policies - on the Exchange servers without affecting other servers in the environment.
8. The Windows NT backup domain controllers are running old applications.
9. We cannot remove these servers as part of the project.

Messaging Administrator:

1. We want to delegate the task of moving user mailboxes to the group that administers Active Directory user accounts.
2. They are trained on how to use the Active Directory administration tools, but they should not use any Exchange administration tools.

Project Manager:

1. We will be cleaning up the subsidiary location over the next year.
2. We will be moving a few users each week to existing company locations.
3. We want the subsidiary user accounts to be displayed in our global address list (GAL) before and after the users move.
4. We also want the corporate user accounts to be displayed in the GAL at the subsidiary.
5. We want to make sure that no changes are made either to GAL by synchronization process until after an administrator reviews the changes.

TECHNICAL REQUIREMENTS

Messaging Infrastructure

1. All e-mail messages that are sent between the main office and the subsidiary must cross the WAN connection between the company locations.
2. All Internet e-mail messages sent to or from the subsidiary location need to use the existing Internet Mail Service connector at the subsidiary.

Supporting Infrastructure

1. The network configuration for the retail outlets will change.
2. The business application used by the retail outlets has been converged into a Web application.
3. The retail outlets need only an Internet connection to access the application.
4. As a result, all WAN connections to the retail outlets are being replaced with an Internet connection.

E-mail Client Infrastructure

1. The users at the retail outlets need to be able to access their mailboxes, public folders and calendars when they are in the office.
2. They do not need to be able to access their e-mail when the Internet connection is down.
3. The retail offices do not have local network administrators, and therefore the client configuration for the retail offices needs to be as simple as possible.
4. All mailboxes for users in the retail outlets will be centralized on one of the Exchange 2003 servers at the main office.
5. The company is undecided on which Exchange servers will be replaced in the branch office.
6. The company is prepared to accept a decrease in e-mail client performance for users in the branch offices, when the Exchange servers are removed.
7. The company had decided that Exchange 5.5 server will be replaced with an Exchange 2003 server in offices where they are more than 30 mailboxes in the office or the WAN connection to the main office is 640 Kbps or less.

Topic 4, City Power & Light (6 Questions)

QUESTION 21

You need to create an administrative design that will enable the organization to centralize the management of the Exchange Server 2003 computers. Which two actions should you perform? (Each correct answer presents part of the solution. Choose two)

- A. Create a new domain named Exchange.Corp.cpandl.com and locate all the Exchange servers in the domain.
- B. Create a new organizational unit (OU) named Exchange OU and move all the Exchange servers into the OU.
- C. Locate all the Exchange servers in the Domain Controller OU.
- D. Assign Full Exchange Administrator rights to the Domain Admins group and to the Exchange Admins Group.
- E. Assign Full Exchange Administrator rights to the Domain Admins group. Assign

Exchange Administrator rights to the Exchange Admins group.

F. Assign Full Exchange Administrator rights to the Domain Admins group.

Add the Exchange Admins group to the Administrators group on each Exchange server.

Answer: B, E

Explanation

The Interview with the Network Administrator tells us that :

3. We want only the Domain Admins group and a Messaging Admins group to manage all the Exchange servers.

4. The Messaging Admins group should be able to administer the Exchange organization, but it should not be able to assign anyone else permission to manage the servers.

5. In addition, we want one administrator in each office that contains an Exchange server to be able to create mailboxes on the Exchange server in that office.

6. The administrator should not be able to modify any Exchange settings and should not be able to create mailboxes on an Exchange server in any other office.

You need to manage business and administrator requests, by creating a new organizational unit (OU) for each office that contains an Exchange Server and placing each Exchange server for that office in their OU. This will enable you to apply central policies for each office. Also, they want a Domain Admins group and a Messaging Admins group to manage all the Exchange servers exclusively and they want only one administrator in each office that contains an Exchange server able to create mailboxes on the Exchange server in that office and that the administrator should not be able to modify any Exchange settings or create mailboxes on an Exchange server in any other office. By assigning Full Exchange Administrator rights to the Domain Admins group and to the Messaging Admins group at the organizational level, you take care of all requirements.

Exchange Full Administrator

When you assign a user or a group Exchange Full Administrator permissions, the user or the group can fully administer Exchange Server computer information and modify permissions.

Exchange Administrator

When you assign a user or a group Exchange Administrator permissions, the user or the group can fully administer Exchange Server computer information.

Exchange View Only Administrator

When you assign a user or a group Exchange View Only Administrator permissions, the user or the group can view Exchange Server configuration information.

Reference

Overview of Exchange Administrative Role Permissions in Exchange 2003 KB article 823018

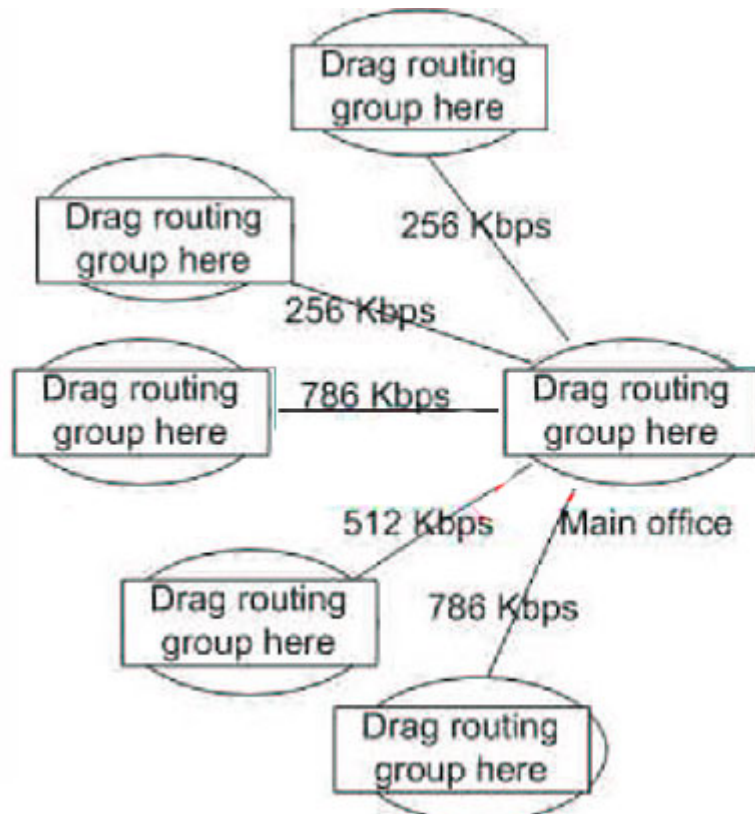
QUESTION 22

You need to design a routing group configuration for the Exchange organization.

Which offices should you configure to have a routing group?

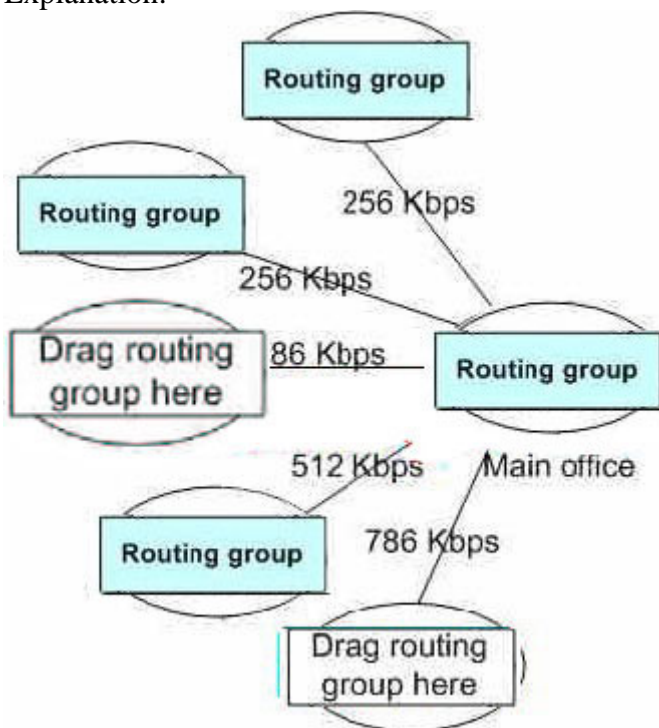
To answer, drag a routing group to the correct location or locations in the answer area. Select three.

Routing group



Answer:

Explanation:



A routing group is a collection of Exchange servers with full-time, highbandwidth,

reliable connections. Within a routing group, all mail is transferred directly between servers. The most important factor to consider when you are planning routing group boundaries is the stability of the network connections between the servers running Exchange Server.

You can implement a centralized messaging system if your company is composed of offices that are all connected by high-bandwidth, reliable network links, regardless of the distance between offices. This means that all Exchange servers are located and managed in a central data center and you will have a single routing group.

You can introduce routing groups to control how messaging traffic is routed from one location to another if your company contains remote offices that are connected by low-bandwidth, high-latency, unreliable network links.

Regarding to the E-mail technical requirements point 7 : "The company had decided that Exchange 5.5 server will be replaced with an Exchange 2003 server in offices where they are more than 30 mailboxes in the office or the WAN connection to the main office is 640 Kbps or less." Therefore we need a routing group configured for every location that has a network connection of 640 Kbps or less. All other locations can be placed into a single routing group in the main office. This is good because the chief information officer wants you to reduce the number of exchange servers in the company.

QUESTION 23

You need to design a strategy for migrating to the mailboxes from Exchange Server 5.5 to Exchange Server 2003. What should you do?

- A. Use the Exchange Migration Wizard to migrate all the mailboxes to the Exchange 2003 Servers.
- B. Use the Exchange Mailbox Merge Wizard (Exmerge) to migrate all the mailboxes to use the Exchange 2003 servers.
- C. Use the Exchange Server Migration Wizard to migrate all the mailboxes to the Exchange 2003 Servers.
- D. Export the contents of each mailbox to a .pst file. Create a new mailbox on the Exchange 2003 servers for each existing mailbox. Import the .pst file contents into each new mailbox.

Answer: C

Explanation

If Exchange Server 2003 was deployed into a new Exchange Server organization instead of joining the existing Exchange Server 5.5 organization, you must use the Exchange Server Migration Wizard to move mailboxes, and then use the Inter-Organization Replication Tool to migrate public folders and free and busy information between the Exchange organizations.

Incorrect Answers

- A. If Exchange Server 2003 was deployed into an existing Exchange Server 5.5 organization, you can move mailboxes between servers using the Exchange Task Wizard.
- B. Exmerge is normally used in recovery procedures.
- D. Export the contents of each mailbox to a .pst file. Create a new mailbox on the

Exchange 2003 servers for each existing mailbox. Import the .pst file contents into each new mailbox. this will work but require more administrative effort

Reference

Appendix A - Tools Used with Exchange

Exchange 2003 Deployment Guide Chapter 5 - Inter-Organizational Migration

QUESTION 24

You need to design a solution so that users in the retail outlets can access their e-mail on the Exchange 2003 servers. What should you do?

A. Install an Exchange 2003 server infrastructure that will support POP3 connections from the Internet.

Install a user certificate on each client computer at the retail outlets.

Instruct the users to sign and encrypt all outbound e-mail messages.

B. Install an Exchange 2003 server infrastructure that will support encrypted POP3 connections from the Internet. Configure the client computer in the retail outlets to use an encrypted connection to the POP3 server.

C. Install an Exchange 2003 server infrastructure that will support encrypted Microsoft Outlook Web Access connections from the Internet. Instruct all users at the retail outlets to access their e-mail by using Microsoft Internet Explorer 5.5 or later to connect to the secure Microsoft Outlook Web Access server.

D. Install an Exchange 2003 server infrastructure that will support encrypted IMAP4 connections from the Internet. Configure the client computers in the retail outlets to use an encrypted connection to the IMAP4 server.

Answer: C

Explanation

OWA enables users to access their Exchange Server 2003 mailbox by using a Web browser such as Microsoft Internet Explorer. OWA can also provide access to mailbox data from UNIX, Macintosh, and Microsoft Windows(r)-based computers without the installation of any messaging client. These users can view and work with any public folder, mailbox, global address list, or calendar from the Web interface.

By default, OWA is configured to use HTTP. This means that all user logon information is passed in clear text to the computer running Exchange Server 2003. This issue can be easily addressed by using SSL to encrypt all user sessions. However, some clients may cache the user logon credentials so that if the user does not close all Web browser sessions,

another user may be able to access the user's e-mail without logging on. This security concern is addressed by reducing the timeout for cached credentials with forms-based authentication.

The steps for securing OWA communications by using SSL are as follows:

1. Install a Web Server certificate on an Exchange server.
2. Enable SSL listening ports on the Exchange server.
3. Configure SSL in the e-mail applications.

A number of authentication methods are available for Outlook Web Access. You must select an authentication method depending on the capabilities of the client operating

system and the specific security policies. You can enable or disable these authentication methods by using the IIS Manager and modifying the properties of the virtual directories that are used by OW

A. Anonymous access is disabled by default on the Exchange Server virtual directories that provide access to mailbox or public folder contents. You can enable anonymous access to provide limited access for specific public folders and directory information. Anonymous authentication is supported by all clients, and it is an easy way to allow access to unsecured content in public folders. Basic authentication uses clear text to perform a simple challenge and response authentication. Basic authentication requires users to specify their user name, domain, and password to gain access to mailbox data. If you are going to enable basic authentication to provide access to OWA, you must implement SSL to encrypt the user name and password. Integrated Windows authentication provides the highest level of security for clients running Internet Explorer 5.0 or later because it uses Kerberos protocol version 5 to authenticate users. If you deploy OWA in a front-end and back-end server topology, only anonymous and basic authentication are supported on the front-end server. You cannot use Integrated Windows authentication. The only option for securing authentication traffic between the OWA client and the front-end server is to deploy SSL.

They tell you that the company is prepared to accept a decrease in e-mail client performance for users in the branch offices when the Exchange servers are removed. Also, all mailboxes for users in the retail outlets will be centralized on one of the Exchange 2003 servers at the main office and they do not need to be able to access their e-mail when the Internet connection is down, but they do need to access their mailboxes, public folders and calendars when they For that reason the best answer is C with OWA you can access either your mailbox or public folders, some attributes are missing if they still using Internet Explorer 5,

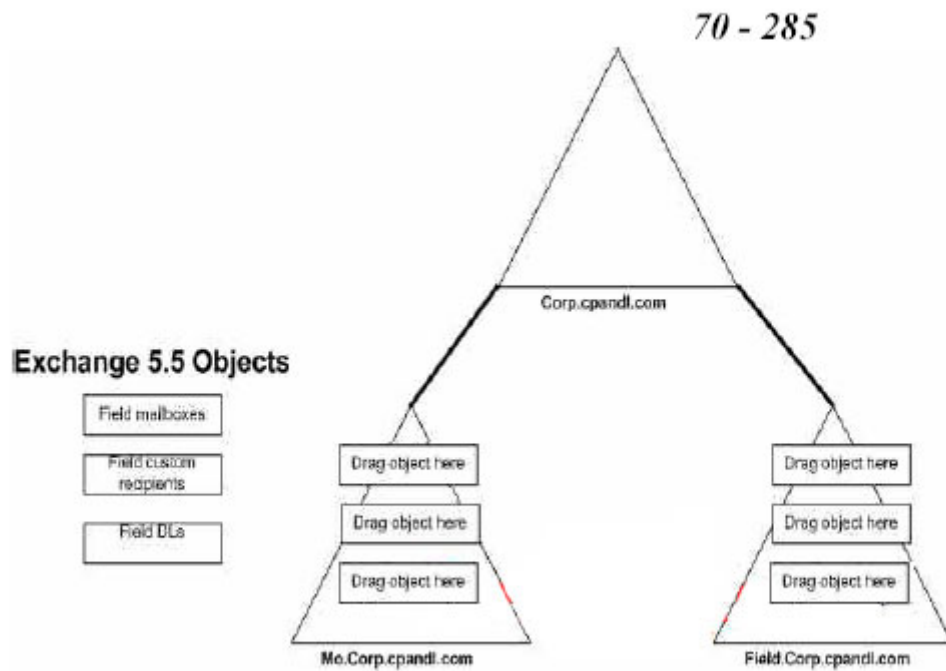
Incorrect Answers

- A, B. You cannot access over POP protocol to the public folders.
- D. You can do it if they are going to use a web application.

QUESTION 25

In preparation for migrating mailboxes and public folders to Exchange Server 2003, you need to create a design for replicating the mailboxes, custom recipients, and distribution lists (DLs) from the Exchange Server 5.5 Field sites to Active Directory. What should you do?

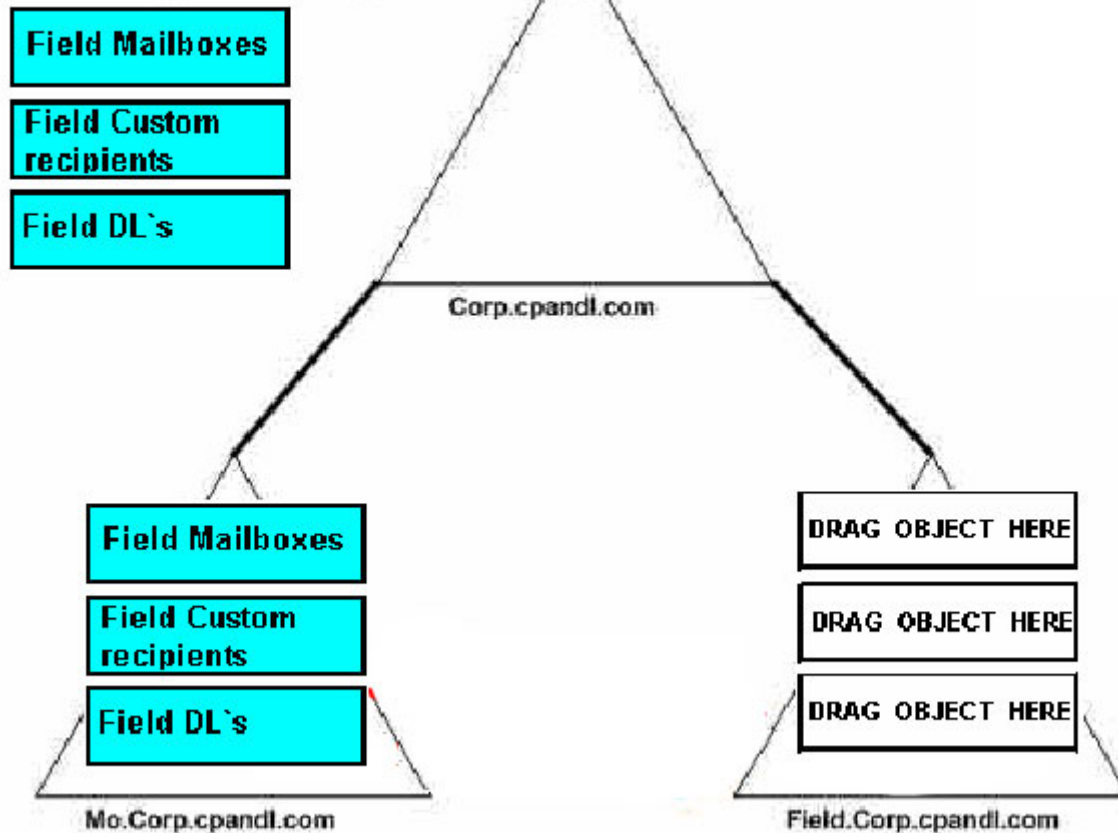
To answer, drag the appropriate Exchange 5.5 object or objects to the correct location or locations in the answer area.



Answer:

Explanation:

Exchange 5.5 Objects



For Exchange Server 5.5 and Exchange Server 2003 public folders to function properly in a mixed mode environment, the follow conditions must be met:

- * Public folder objects must exist in Active Directory. In order for public folder replication between Exchange Server 5.5 and Exchange Server 2003 to function efficiently, directory details must replicate correctly between the Exchange Server 5.5 directory and Active Directory.
- * A public folder hierarchy must be created on each server that has a public folder database.
- * The actual public folder content must be replicated.
- * A domain with a functional level of Windows 2000 native or Windows Server 2003 is needed to allow distribution lists and public folder permissions to be migrated correctly. If you use Exchange Server 5.5 distribution lists to secure access to public folders, the distribution lists must either be converted to Active Directory universal security groups or must be recreated as a security group so that you can secure public folder access in Exchange Server 2003. Because Exchange Server 5.5 distribution lists can have members from across the organization, the only equivalent group in Active Directory is a universal security group, because the membership of a universal security group can span the entire forest. You must have a domain with a functional level of Windows 2000 native or Windows Server 2003 to upgrade universal distribution groups to universal security groups. This is required to allow distribution lists and public folder permissions to be

migrated correctly. So the Distribution lists should be in the root domain. They want subsidiary user accounts to be displayed in our global address list (GAL) before and after the users move, also that corporate user accounts are displayed in the GAL at the subsidiary and to make sure that no changes are made either to GAL by synchronization process until after an administrator reviews the changes. They need to replicate all Exchange 5.5 objects to AD in MO.corpcandll.com and your implementation efforts should support that long-term strategy to eliminate the Field.Corp.cpandl.com domain, because they have an exception in the subsidiary that will maintain an Exchange 5.5 server over the next year they need to replicate all between both domains until the last Exchange 5.5 is seized.

QUESTION 26

You need to design a connection agreement for Active Directory Connector to synchronize directory information with the subsidiary location. Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

- A. Configure a one-way connection agreement that replicates from the subsidiary's Exchange 5.5 organization to Active Directory.
- B. Configure a one-way connection agreement that replicates from Active Directory to the subsidiary's Exchange 5.5 organization.
- C. Configure two one-way connection agreements that replicate between the subsidiary's Exchange 5.5 organization and Active Directory.
- D. Configure the connection agreement to replicate all objects.
- E. Configure the connection agreement to replicate only mailboxes.
- F. Configure the connection agreement to save deletions in an LDAP Data Interchange Format file.

Answer: A, E

Explanation

Connection agreements define the relationship between the existing Exchange Server 5.5 directory and Active Directory, specifying the portions of each directory that the ADC will synchronize and the rules by which the synchronization will occur. There are three different types of connection agreements:

- * Recipient connection agreements. Recipient connection agreements replicate recipient objects and the data they contain between the Exchange directory and Active Directory.
- * Public folder connection agreements. Public folder connection agreements replicate public folder objects and the data they contain between the Exchange directory and Active Directory.
- * Configuration connection agreements. During your initial Exchange Server 2003 installation, Exchange Server 2003 Setup creates a configuration connection agreement between Active Directory and your Exchange 5.5 site. Configuration connection agreements replicate Exchange-specific configuration information between the Exchange 5.5 directory and Active Directory. These agreements help Exchange Server 2003 to co-exist with previous versions of Exchange.

MIIS 2003 uses its GAL synchronization feature to create a common GAL that is used across all the Exchange Organizations. From an individual user's perspective, he or she sees all organization users in the GAL in Outlook. MIIS 2003 does not use the Active Directory Connector (ADC) to synchronize the GAL between the Exchange 5.5 and 2003 organization. So the GAL requirements that the Project Manager told us are not applicable to this ADC question.

We want to phase out the exchange 5.5 server in the next year and move mailboxes to the new exchange 2003 server, therefore we need to setup an one-way connection agreement ADC from exchange 5.5 to the active directory site.

Topic 5, Northwind Traders, Scenario

Case Time until final review 20 minutes

BACKGROUND

1. Overview

Northwind Traders imports various kinds of merchandise from around the world. They require its messaging system to be available Monday through Friday from 9:00 A.M. to 5:00 P.M. local time. E-mail is the primary means of communication between company employees and overseas vendors.

1. Physical Locations

The company has offices in New York and Los Angeles. The New York office has 400 users + 50 (18 months) Los Angeles office has 150 users. A total of 50 New York users also work from home and access e-mail by using a Web interface.

1. Planned Changes

1. The company currently uses a POP3 messaging system. This system will be replaced with Exchange Server 2003.
2. Messages will not be migrated from the old system to Exchange.
3. The company will deploy Microsoft Outlook Web Access so that employees working from home can access e-mail.
4. In 18 months, the company will purchase a subsidiary, which will add 50 users to the New York office.
5. All of these users will access e-mail by using Outlook Web Access.

EXISTING MESSAGING ENVIRONMENT

1. Administrative Structure

1. Server administrators at each office create and manage the mailboxes on the POP3 messaging system.

1. Messaging Infrastructure

1. The company has a third-party certification authority (CA) deployed on the network.
2. The CA is integrated with Active Directory.

1. E-mail Clients

1. All office users run Microsoft Outlook 2003 and Internet Explorer 6.0 on their client computers.
2. Home users run Microsoft Internet Explorer 6.0 or later.

SUPPORTING INFRASTRUCTURE

1. Directory Services

1. The company has a single Active Directory domain with two sites.
2. Each site contains two domain controllers.
3. One domain controller at the New York office is configured to be a global catalog server.
4. There are no other global catalog servers.

1. Network Infrastructure

1. Each office has a dedicated 1.544-Mbps connection to the Internet.
2. The offices are connected to each other by a dedicated 3-Mbps connection.
3. This connection is less than 20 percent utilized.
4. Each office has a perimeter network that connects it to the Internet.

1. Administration

1. A central IT administration group works at the New York office this group is responsible
2. Active Directory administration and has administrative permissions on all company servers
3. Hardware maintenance for Exchange servers.
4. Each office also has a server administration group that has administrative permissions on all servers in that office.

BUSINESS REQUIREMENTS

Security

1. All connections to Outlook Web Access must be encrypted.
2. Server administrators in each office must be able to manage the Exchange servers, including performing backup and recovery operations, without having permissions to create or modify user and group objects in Active Directory.
3. Server administrators from each office must be able to manage all Exchange servers in the company.

1. Interviews

Chief Executive Officer:

1. If a mailbox store fails, we must not lose more than one hour of data.
2. If a single store fails because of file corruption or other database-related reasons, no more than 150 users must be affected.
3. I am told that we have about 3 GB of nightly backup capacity, so our backup and recovery strategy must work within that limitation.
4. Additionally, we must simplify our backup strategy as much as possible.
5. In the past, our competition has sent forged e-mail messages to our vendors so that the messages appeared to be coming from us.
6. The new messaging system must allow us to ensure that messages to our vendors are identifiable as coming from us.
7. However, we cannot afford to spend additional money on these security measures.

Chief Information Officer:

1. Corporate security policies prohibit domain communications, including logon and password change traffic, from passing through any firewall on our network.
2. We also need to minimize the address book traffic that the Exchange system creates on our WAN connection.
3. We need to minimize the number of new servers we purchase for Exchange, and we need to minimize the number of global catalog servers on the network.

TECHNICAL REQUIREMENTS

1. E-mail Client Infrastructure

1. All company vendors use Microsoft Outlook 2000 or later for e-mail.
2. Company policies state that all e-mail users will be limited to 100 MB of mailbox storage space.
3. The company wants to build the Exchange system so that future hardware purchases that are necessary to provide e-mail to the subsidiary users are minimized.
4. The servers that the company is purchasing for Exchange have adequate disk space to accommodate the subsidiary users.

Topic 5, Northwind Traders (4 Questions)

QUESTION 27

You need to design an administrative model for the Exchange Server environment. What should you do?

A. Create a single organizational unit (OU). Place the user accounts for each office in the OU.

Delegate control over the OU to the office's server administrators and the central IT staff.

B. Create a single Exchange administrative group. Place all Exchange servers into that administrative group.

Assign permissions for the administrative group to the officer's server administrators and the central IT staff.

C.

Create an Exchange administrative group for each office. Place the Exchange servers for each office into that office's administrative group. Assign permissions for the administrative group to the office's server administrators. Allow the central IT staff to manage user mailboxes.

D. Create an organizational unit (OU) for each office. Place the user accounts for each office into the appropriate OU. Delegate control over each OU to the office's server administrators. Allow the central IT staff to manage user mailboxes.

Answer: B

Explanation

This question is little tricky between the meaning of Active Directory delegation and Exchange Server delegation, to be able to accomplish the required task also some of the required permissions can not be assigned just using AD users and computer GUI or Exchange System Administrator tool, to be able to resolve the dilemma you will need to use ADSIEDIT.MSC Tool from Windows 2003 Server tools, to assign required permissions because they do not use a custom Active Directory delegation that is

required for this task.

Incorrect answers

A. Delegate control over the OU to the office's server administrators and the central IT staff of users does not give them any Exchange Organization admin permissions, this need to be delegated over specific objects and they do not give us such information they do not tell us create a custom task You assign Write permissions to the attributes associated with mailboxes by using the Active Directory Users and Computers utility or by using a third-party utility for account delegation management using adsiedit.msc tool and you will be able to manage users but not the servers because the OU just contain just users not computers

C. There is not any needs to create two Exchange administrative groups because Server administrators from each office must be able to manage all Exchange servers in the company and central IT administration group works at the New York office has administrative permissions on all company servers.

D. This give permissions to central IT staff to create mailbox but central IT administration group works at the New York office and must has administrative permissions on all company servers this include Exchange servers providing permissions to Server administrators from each office and manage mailboxes do not take consideration the question.

Reference

Minimum permissions necessary to perform Exchange-related tasks KB article 316792

QUESTION 28

You need to design a strategy for providing e-mail access to the subsidiary users.

What should you do?

A. Deploy POP3 and IMAP4 services on Exchange front-end servers.

Make the front-end servers accessible from the Internet by means of POP3, IMAP4, and SMTP only.

B. Deploy Microsoft Outlook Web Access on Exchange mailbox servers.

Make the mailbox servers accessible from the Internet by means of HTTPS and SMTP only.

C. Deploy Microsoft Outlook Web Access on Exchange front-end servers.

Make the front-end servers accessible from the Internet by means of HTTPS only.

D. Deploy an additional Exchange mailbox server that contains all subsidiary mailboxes.

Deploy Microsoft Outlook Web Access on the server.

Make the server accessible from the Internet by means of HTTPS only.

Answer: C

Explanation

The planned changes stated that the subsidiary users are going to use Outlook Web Access (OWA) and the security requirements point 1 states : "All connections to Outlook Web Access must be encrypted."

You can provide fault tolerance for your front-end servers by implementing Network Load Balancing, a service that is provided by Windows Server 2003. Network Load

Balancing dynamically distributes IP traffic to multiple frontend servers, transparently distributing client requests among front-end servers and enabling clients to access their mailboxes by using a single server namespace. The clients recognize front-end servers as a single server that responds to their requests. If a front-end server becomes unavailable, the workload is redistributed to the remaining servers. Network Load Balancing provides load balancing and also a high level of fault tolerance, which is essential to ensuring high availability for client access to the front-end servers.

If we use SSL to encrypt data between your clients and your Exchange servers, then front-end servers can handle all encryption and decryption processing. This improves performance by removing processing tasks from back-end servers while still allowing the data to be encrypted between the client computer and the Exchange servers.

Incorrect Answers:

A. The planned changes stated that the subsidiary users are going to use Outlook Web Access (OWA), not POP3 or IMAP4.

B,D. Outlook Web Access (OWA) should be configured on front-end servers, not back-end mailbox servers.

QUESTION 29

You need to design security for messages exchanged between Northwind Traders employees and its vendors.

What should you do?

A. Require employees to access e-mail only over connections that use SSL.

B. Place Exchange mailbox stores on NTFS volumes.

Use Encrypting File System (EFS) to encrypt the stores.

C. Use the internal certification authority (CA) to issue certificates to all employees.

Require employees to digitally sign outbound e-mail.

D. Use the internal certification authority (CA) to issue certificates to all employees and vendors.

Instruct employees and vendors to use secure MIME to encrypt all e-mail sent between them.

Answer: C

Explanation

Microsoft(r) Office Outlook(r) 2003 provides ways for users to manage their digital IDs the combination of a user's certificate and public and private encryption key set. Digital IDs help to keep users' e-mail messages secure by letting them exchange cryptographic messages.

In order to exchange cryptographic e-mail messages with another user, you must have each other's public keys. You provide access to your public key through a certificate.

There are several ways to provide your digital ID to others. For example, you can:

- * Digitally sign an e-mail message.

- * Use a directory service, such as the Microsoft Exchange Global Address Book.

- * Provide a certificate in a digitally signed e-mail message

To provide your public key to another user by using an e-mail message, compose an

e-mail message and digitally sign it by using your certificate. When Outlook users receive the signed message, they can right-click on your name on the To line and then click Add to Contacts. The address information is saved in Contacts, and your certificate is saved in the registry.

QUESTION 30

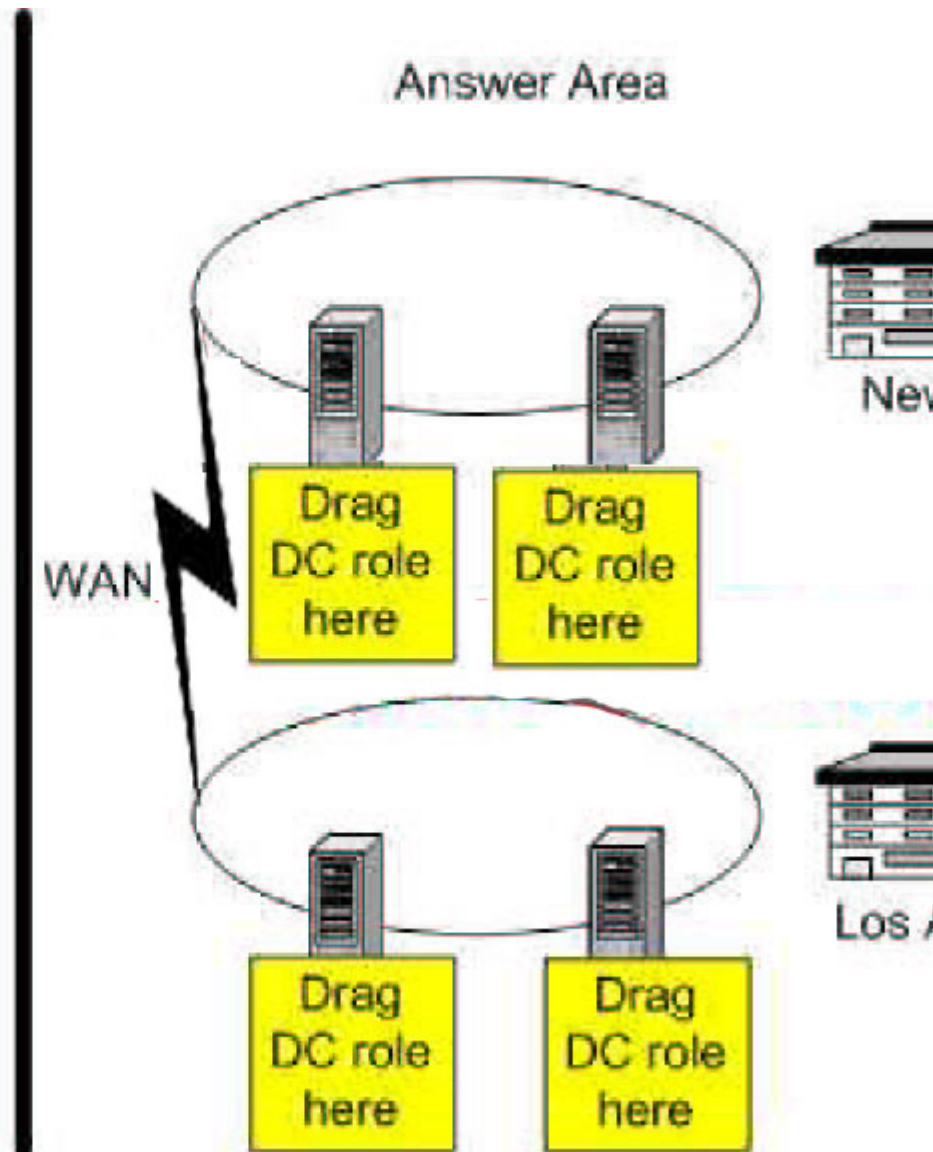
You need to designate which domain controllers will be global catalog servers in the new environment.

What should you do?

To answer, drag the domain controller role to the correct location or locations in the answer area.

Domain Controller Role

DC with
global
catalog

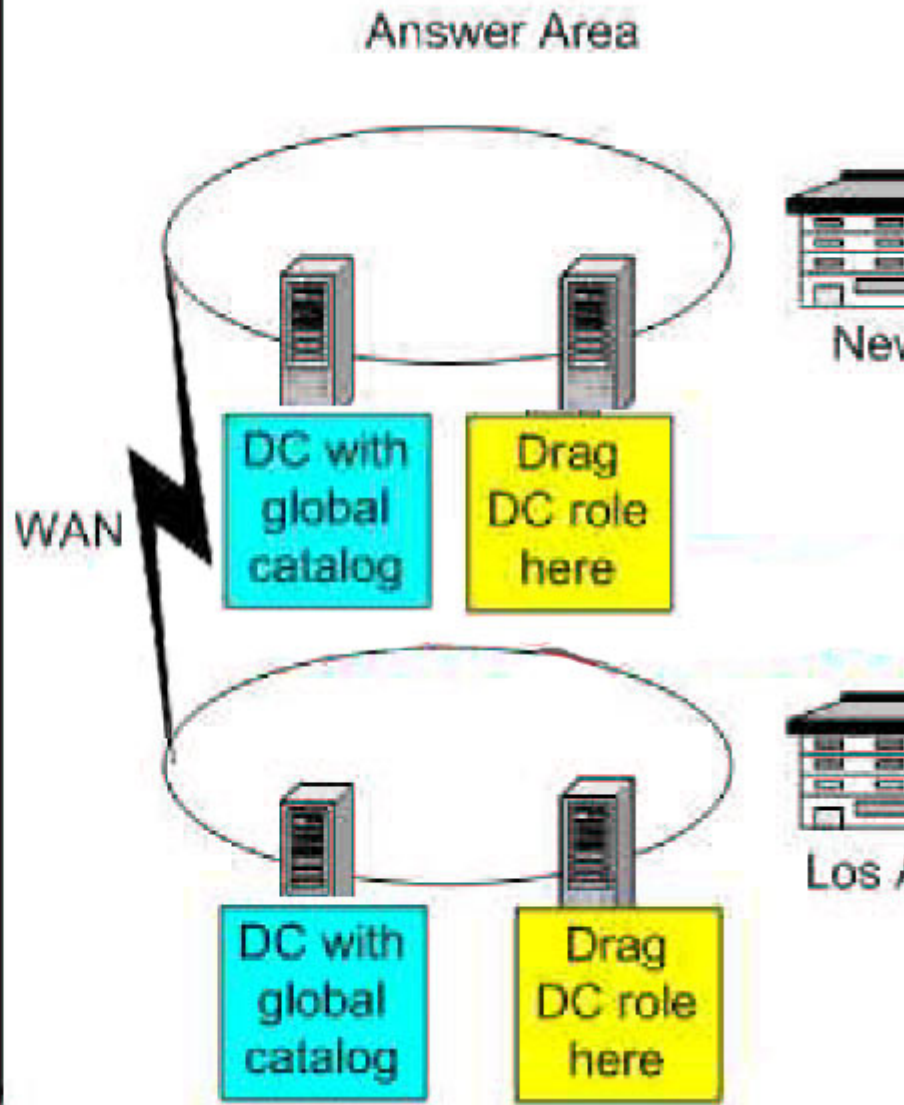


Answer:

Explanation:

Domain Controller Role

DC with
global
catalog



The function of a global catalog server in Active Directory is to maintain a partial attribute set for user objects across all domains in the forest. You may need to make changes in the placement of these servers to provide better support for your Exchange servers.

* Both Exchange Server and Outlook need a local global catalog server. The global catalog server is critical for Exchange Server services, including log on, group membership, store services, and access to the global address list (GAL).

* Deploying global catalog servers locally to both servers and users can, with proper configuration, make address lookups more efficient.

* Contacting a global catalog server across a slow connection increases network traffic and impairs the user experience.

The Chief Information Officer told us that : "2. We also need to minimize the address book traffic that the Exchange system creates on our WAN connection." Therefore we

will need to put another global catalog in Los Angeles site to minimize address book traffic that Exchange system creates on their WAN connection when make Address book queries and because they already have one and You need to designate which domain controllers will be global catalog servers in the new environment. We can keep the Global Catalog server in the New York Office to service requests in that office.

Topic 6, Certkiller .com, Scenario

BACKGROUND

1. Overview

Certkiller .com is a large retail company that has 2,000 locations all across North America and South America and 10,000 employees.

1. Physical Locations

The main office is in Washington DC.

Branch offices are in Mexico City, Buenos Aires, and Rio de Janeiro.

The main office and each branch office connect to satellite offices in the same country.

The locations of offices and the number of users in each office are shown in the following table.

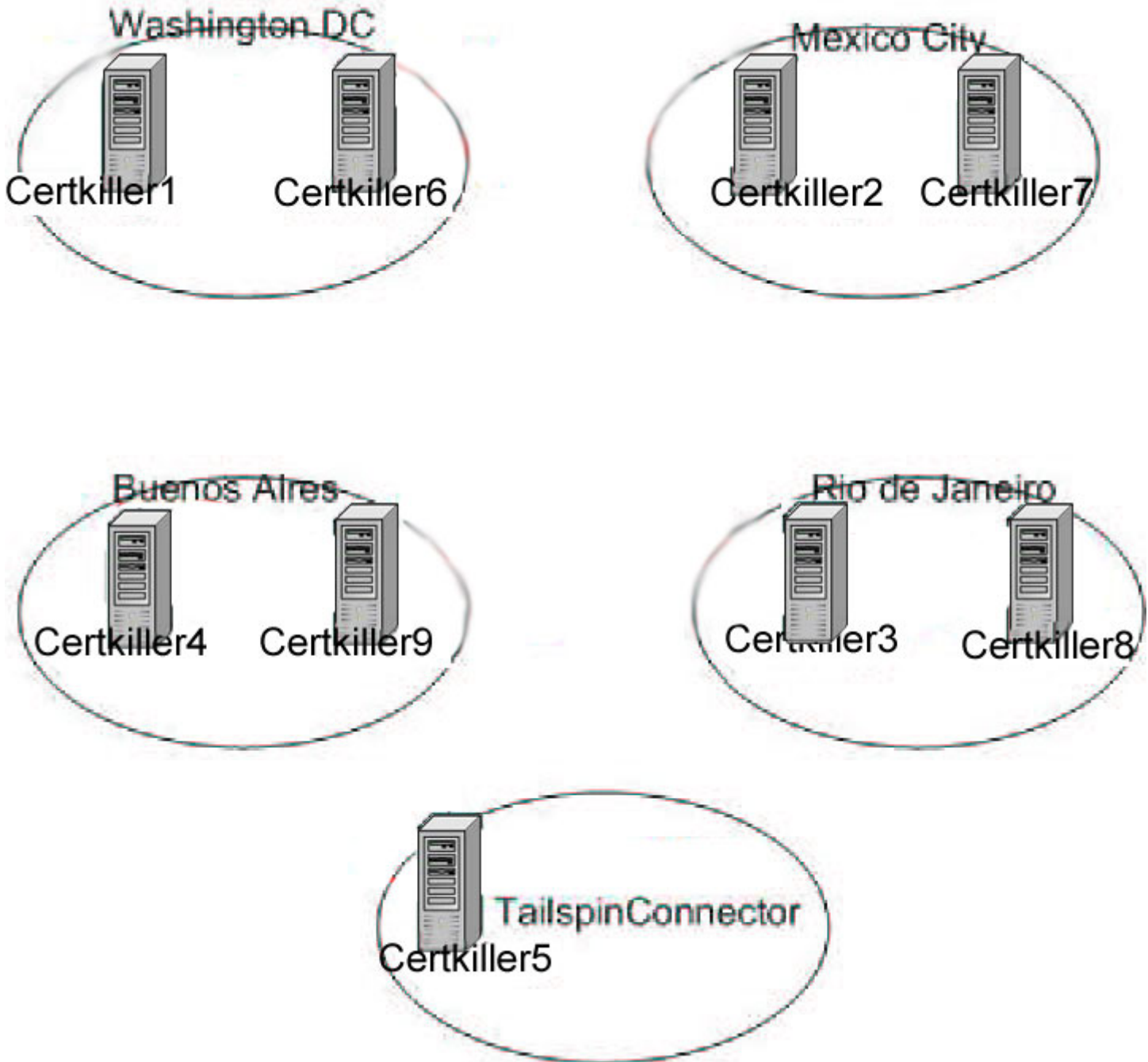
Main or Branch Office	Number of Users in Main or Branch Office	Country in Which Satellite Offices Are Located	Total Number of Users in Satellite Offices
Washington DC	1,000	USA	5,000
Mexico City	500	Mexico	1,500
Buenos Aires	100	Argentina	400
Rio de Janeiro	50	Brazil	1,450

1. Planned Changes

Certkiller .com plans to migrate the current Exchange 2000 Server messaging environment to Exchange Server 2003.

EXISTING MESSAGING ENVIRONMENT

1. Administrative Structure



The administrative groups for Certkiller .com are shown in the following diagram.

1. Messaging Infrastructure
1. All Exchange servers run Exchange 2000 Server with the most recent service pack.
2. The operating system on each Exchange server is Microsoft Windows 2000 Server with the most recent service pack.
3. The only link between users at Certkiller .com and Tailspin Toys is the Lotus CC: Mail Connector.
4. All mail-enabled user accounts have an Internet SMTP alias that complies with the following format: username@ Certkiller .com.
5. The serves are used as shown the following table.

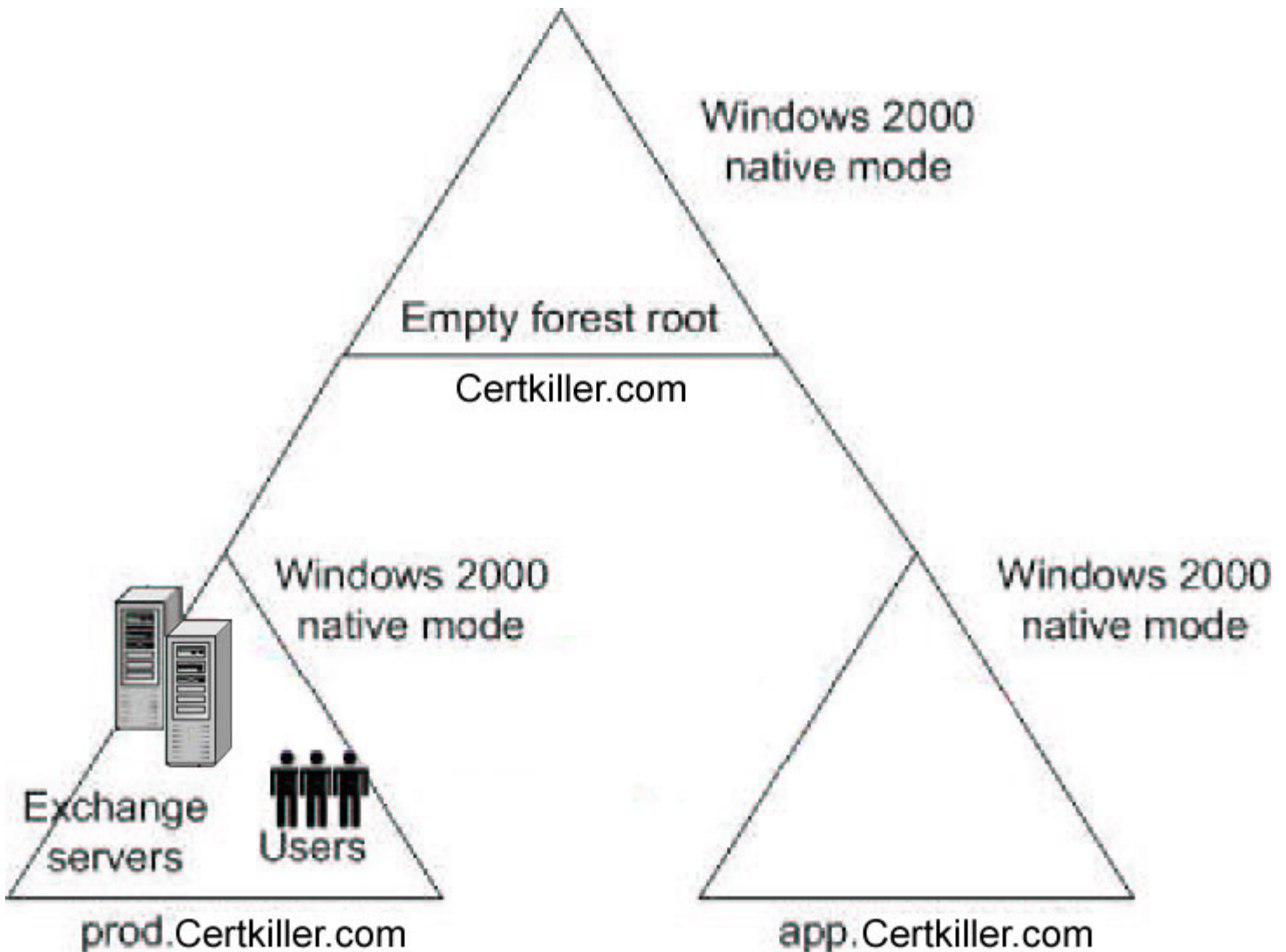
Server Function	Server Names
Front-end server	CERTKILLER6, CERTKILLER7, CERTKILLER8, CERTKILLER9
Mailbox and public folder information store	CERTKILLER1, CERTKILLER2, CERTKILLER3, CERTKILLER4
Lotus cc:Mail connector	CERTKILLER5

6. You plan to purchase two additional servers for the Washington DC office after the upgrade.
 7. You plan to name these servers Certkiller 10 and Certkiller 11.
 8. You plan to install Windows Server 2003 and Exchange Server 2003 on these servers and configure them in the future as needed.
1. E-mail Clients
 1. All users who work in the main office or in a branch office connect to their mailboxes and public folders by using Microsoft Outlook 2000.
 2. All users who work in a satellite office connect to their mailboxes and public folders over a virtual private network (VPN) connection on the Internet by using an IMAP4 client of their own choosing. Not all e-mail clients support IMAP4 referrals.
 3. Users at Tailspin Toys use Lotus CC: Mail to retrieve and send their e-mail messages.

SUPPORTING INFRASTRUCTURE

1. Directory Services

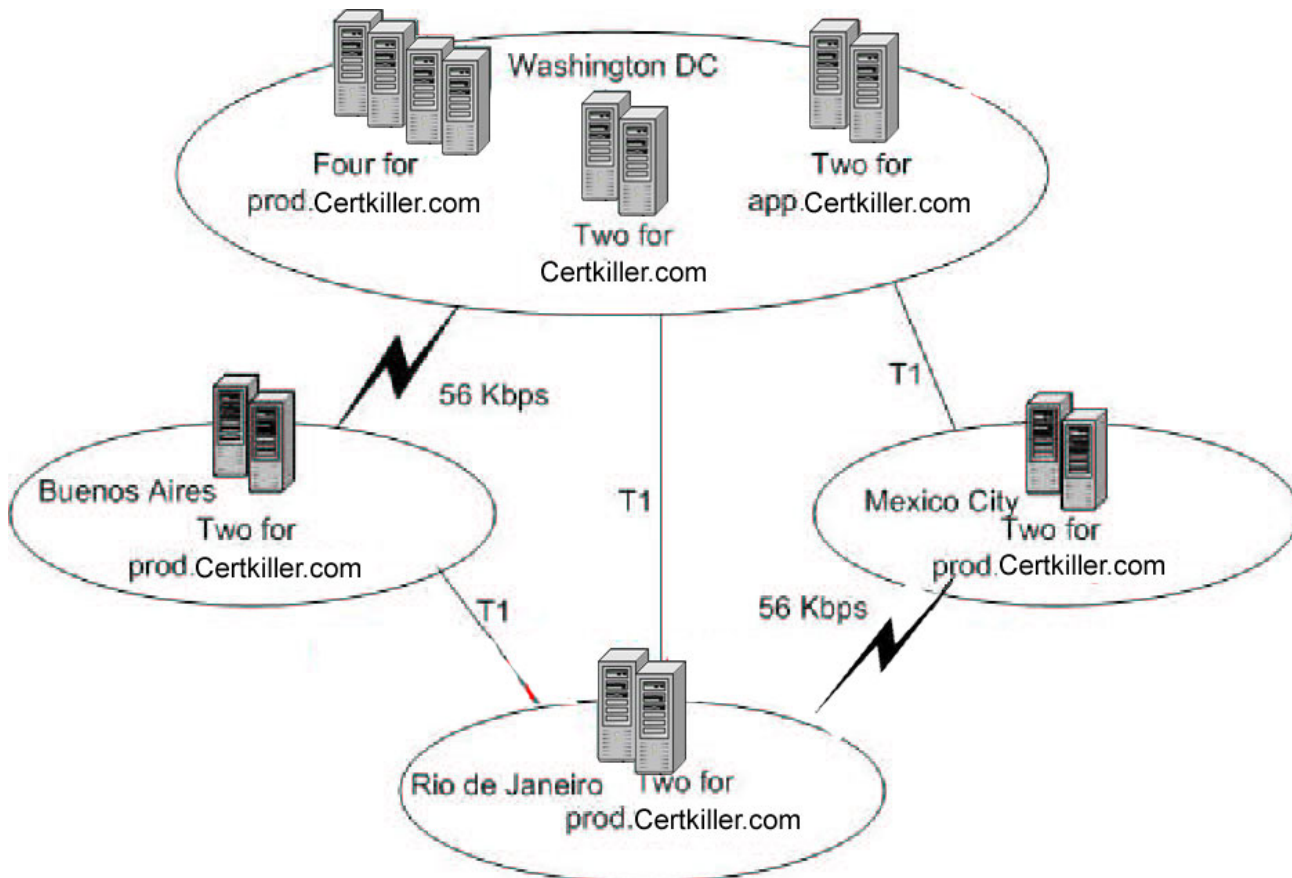
The Active Directory infrastructure is shown in the following diagram.



1. The main office and its associated satellite offices are configured as a single site, and each branch office and its associated satellite offices are configured as a separate site.
2. The app. Certkiller .com domain was created to support a third-party application. There are no user accounts in this domain.

1. Network Infrastructure

The placement of global catalog servers is shown the following diagram.



1. The main office in Washington DC and the branch offices in Buenos Aires and Rio de Janeiro each have an independent connection to the Internet by using a local ISP.
2. Each of these locations is configured to accept VPN client connections.
3. Two Windows Server 2003 member servers named DNS1 and DNS2 are located in the main office and are configured as DNS servers for the external zone named Certkiller .com.
4. The routing costs for all WAN connections are set to the same value.

BUSINESS REQUIREMENTS

1. The company needs to take advantage of new features in Exchange Server 2003. You must implement these new features for the largest number of users in the shortest time.
2. Messages that have large attachments must be scheduled to be transferred between branch or satellite offices and the main office during off-peak hours only.
3. You must not change the method that users in satellite offices use to access their messages after upgrade. Insufficient resources are available to train these users to use a new e-mail client or connection method.
4. An analysis of home use indicates that users in Mexico do not access the network from home as often as users in the outer countries.
5. No more than one server can be upgraded on any single day.

TECHNICAL REQUIREMENTS

1. Messaging Infrastructure
 1. You must maintain connectivity to existing messaging systems and for the Tailspin Toys users.
 2. You must ensure that users in the satellite offices in Mexico are able to access public

folders on the servers in the Mexico City office when they attempt to browse public folder content.

3. You must not add any additional hardware until the upgrade is complete.

1. Supporting Infrastructure

1. During the upgrade procedure, you must not change the existing domain structure.

2. You must not change the existing administrative model.

3. You need to ensure that messaging traffic over connections that are slower than T1 take place only when there are disruptions to the T1 connections.

4. You need to ensure that incoming Internet SMTP traffic is load-balanced across SMTP servers.

Topic 6, Certkiller .com, (6 Questions)

QUESTION 31

You need to configure the DNS resource records for incoming e-mail messages from the Internet.

What should you do?

A. Configure mailbox (MB) resource records in the external DNS domain.

Configure each record so that it has the same refresh interval.

B. Configure mailbox (MB) resource records in the external DNS domain.

Configure each record so that it has the same default Time to Live (TTL) interval.

C. Configure mail exchanger (MX) resource records in the external DNS domain.

Configure each record to have the same preference and a different mail exchanger.

D. Configure mail exchanger (MX) resource records in the external DNS domain.

Configure each record to have the same preference and the same mail exchanger.

Answer: C

Explanation

The supporting network infrastructure told us that : "3. Two Windows Server 2003 member servers named DNS1 and DNS2 are located in the main office and are configured as DNS servers for the external zone named Certkiller .com." and the Technical requirements told us that : "4. You need to ensure that incoming Internet SMTP traffic is load-balanced across SMTP servers."

A mail exchanger record is a DNS record that the e-mail server names for your domain so that you can receive SMTP e-mail from Internet hosts. Transferring messages between SMTP hosts is dependent on DNS. When an SMTP host sends an e-mail message to another SMTP host, DNS resolves the domain name of the receiving host to its name and then the Transmission Control Protocol/Internet Protocol (TCP/IP) address by first using MX records.

To receive e-mail from the Internet, you must configure MX records for all SMTP mail domains hosted on your network. Remote SMTP hosts use the MX records in external DNS servers to locate the messaging servers for your domain name. You must configure the MX records for all your SMTP address spaces. Secondly, to be able to recognize what host matches with your MX record, you will need two A records, one for each host. Certkiller .com wants to configure some load balancing features for their incoming mail servers. For that to happen, the company must set up a number of mail servers, each one

with a different IP address. Then new MX Records will be added to the DNS1 and DNS2 server, pointing to the mail servers, all with the same priority.

QUESTION 32

You need to configure connectors between each routing group.

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

- A. Create and configure SMTP connectors between the routing groups.
Do not create additional connectors between the routing groups.
- B. Create and configure routing group connectors between the routing groups.
Do not create additional connectors between routing groups.
- C. Create and configure low-cost group connectors and high-cost SMTP connectors between the routing groups.
- D. Create and configure high-cost routing group connectors and low-cost SMTP connectors between the routing groups.

Answer: A, B

Explanation

Routing describes how Exchange Server transfers messages from one server to another. When multiple routing groups exist, messages are routed between routing groups using routing group connectors. When planning your routing topology, you need to plan for the most efficient transfer of messages. Your plan must include which connector will be used to connect routing groups as well as the locations of connectors to messaging systems outside your Exchange Server organization. Careful planning can reduce the volume of network traffic and optimize Exchange Server and Windows services.

Connectors between routing groups are ways to funnel mail. In situations where you have multiple connections to a possible destination, you can define connectors between routing groups to control message flow. Within a routing group, communication between servers is point-to-point, so you cannot determine paths and costs to ensure that the least expensive route between two servers is chosen. However, by creating routing groups, you can assign costs to various paths to ensure the most efficient route is used. Cost is the variable Exchange Server uses to determine the most efficient messaging route.

Exchange Server considers the lowest cost route the most efficient. Exchange Server uses a more expensive route only if a server or connector is unavailable on the route with the lowest cost. You should assign the lowest costs to the most preferred routes, such as those with the highest available network bandwidth.

The preferred connection method to connect two routing groups is a Routing Group connector. Although it is possible to connect routing groups with an SMTP connector or an X.400 connector, you should use a Routing Group connector because this connector is designed and intended specifically for connecting routing groups. A Routing Group connector uses SMTP and can be configured to schedule message transfers.

QUESTION 33

You are preparing the supporting network infrastructure for the upgrade to Exchange Server 2003. You want to accomplish this upgrade by using the minimum

amount of administrative effort.

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

- A. Run the setup.exe /domainprep command on a domain controller in the prod. Certkiller .com domain.
- B. Run the setup.exe /domainprep command on a domain controller in the app. Certkiller .com domain.
- C. Run the setup-exe /domainprep command on a domain controller in the Certkiller .com domain.
- D. Log on to the domain by using a user account that is a member of the Domain Admins group.
- E. Log on to the domain by using a user account that is a member of the Schema Admins group.

Answer: C, D

Explanation

They do not offer setup.exe /forestprep as option you must assume that ForestPrep already been ran in the Organization. To upgrade from AD Exchange 2000 objects Schema to AD Exchange 2003 Schema. Once you have prepared the Windows Active Directory forest using ForestPrep, you must also prepare each domain in the forest that will run Exchange Server 2003 using DomainPrep. In addition, you must run DomainPrep in the forest root domain and each domain that will contain Exchange Server 2003 mailbox-enabled objects or that has users or groups that will manage Exchange Server 2003 computers.

DomainPrep does all the tasks for Exchange Setup which require Domain Admin rights to accomplish. These tasks are:

Create two groups;The Exchange Enterprise Servers Group (EES) and the Exchange Domain Servers group (EDS)

Create the Microsoft Exchange System Objects container (also known as the Domain Proxy Container) in the Active Directory

Add permission (mainly for the EES and EDS)to the domain,AdminSDHolder,and MS Exchange System Objects containers

Add permission to the EES,EDS,and the pre-Windows 2003 Compatible Access Group

Add the EES to the local security policy"Manage auditing and security log"on every Domain Controller in the domain

Note: The Recipient Update Service (RUS) will keep these permissions up to date when Exchange is installed in new domains and when new Exchange Full Administrators are delegated.

Thus running DomainPrep requires an account that has Domain Admin level permissions, but does NOT require any Exchange Admin permissions. This way you don't have to give your email administrator Domain Admin permissions in order to install the first Exchange in a given domain.

That's it. 2 groups, an object, and some permissions for the groups. That's all DomainPrep is. It doesn't create any directories, install any binaries, or add any regkeys. It's actually

very lightweight and runs in seconds.

So then why do I need to run DomainPrep in my Root (or Parent) Domain if I'm not going to have any Exchange servers or users with Exchange mailboxes in that domain?

The short answer is "Because that's usually where the GC is".

The main issue has to do with DSAccess. DSAccess is what Exchange services use to access information in the Active Directory. In order for it to find the correct information, DSAccess needs to talk to Global Catalog servers, even if those servers are not in a domain where Exchange is installed. DSAccess will only talk to GCs that it has rights to. It will check to see if it has rights to that GC by checking if it has privileges to the Security Access Control List (SACL) on the GC. These rights are only propagated by the Recipient Update Service (RUS) and you can only create a RUS for domains that have been DomainPrepped.

If you follow this chain, you'll see that it comes down to "DSAccess needs to be able to talk to a GC", and in order to do that the GC has to be in a domain which has been DomainPrepped and has a RUS pointed at it.

So if you have a parent-child domain configuration, with Exchange only in the child domain, and GCs in the parent domain, you will have to run DomainPrep in the parent domain AND create a new RUS on an Exchange server in the child domain and point that RUS at the parent domain.

Now I know you're all asking the question "What if you don't have a GC, or Exchange servers, or users getting Exchange mailboxes in the parent domain?" The answer is:

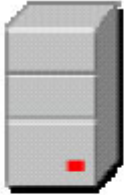
"Then you don't need to DomainPrep the parent domain."

So if all your GCs are in the child domain, and none are in the parent domain, and there are never going to be any Exchange resources in the parent domain, then you don't need to DomainPrep it or create a RUS for it. But that configuration doesn't happen very often and the consequences for not DomainPrepping the parent are bad enough (like the Exchange Information Store service won't start) that we tell everyone to always domainprep the parent domain.

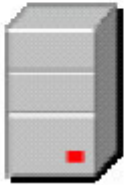
So this question seems like a trick question. We have a domain with mail-enabled users, so at first we think to domain prep that domain. But since we have a root domain with Global Catalog we also need to domain prep that domain.

QUESTION 34

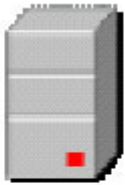
You need to upgrade the Exchange servers in the main office, while meeting the goals and constraints of Certkiller .com. From the graph select which server or servers should you upgrade?



Certkiller1



Certkiller5

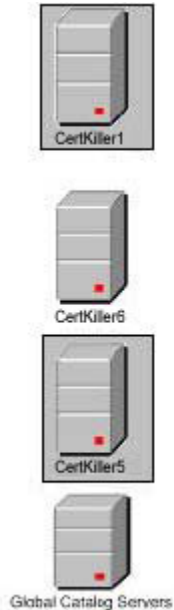


Certkiller6



Guess Connect Service

Answer:
Explanation



Microsoft Exchange Server 2003 supports using a server architecture that distributes server tasks among front-end and back-end servers. In this architecture, a front-end server accepts requests from clients and proxies them to the appropriate back-end server for processing.

A front-end server is a specially configured server running either Exchange Server 2003 or Exchange 2000 Server. Front-end servers should not maintain user mailboxes or public folders. Their role is to proxy all client requests to an Exchange Server back-end server.

A back-end server is an Exchange Server with a standard, default configuration. There is no configuration option to designate a server as a back-end server. The term back-end server refers to all servers in an organization that are not frontend servers.

If your Exchange 2000 organization takes advantage of front-end and back-end architecture, you must upgrade your front-end servers before you upgrade your back-end servers.

At first we must upgrade the front-end server (Certkiller 6) and the the back-end server (Certkiller 1). There is no need to upgrade the Global Catalog servers since they are allready running on windows 2000 with the latest service pack.

QUESTION 35

You need to upgrade the Exchange servers in the Mexico City, Buenos Aires, and Rio de Janeiro branch offices. In which order should you upgrade the servers.

To answer, move the appropriate server names from the list of server names to the answer area and arrange them in the correct order. (Use only server names that apply)

Server names

CERTKILLER2

CERTKILLER3

CERTKILLER4

CERTKILLER7

CERTKILLER8

CERTKILLER9

Steps place here

Place first step here

Place second step, if any, here

Place third step, if any, here

Place fourth step, if any, here

Place 5th step, if any, here

Place 6th step, if any, here

Answer:

Server names

Answer Area

Certkiller7

Certkiller2

Certkiller8

Certkiller3

Certkiller9

Certkiller4

Explanation

Microsoft Exchange Server 2003 supports using a server architecture that distributes server tasks among front-end and back-end servers. In this architecture, a front-end server accepts requests from clients and proxies them to the appropriate back-end server for processing.

A front-end server is a specially configured server running either Exchange Server 2003 or Exchange 2000 Server. Front-end servers should not maintain user mailboxes or public folders. Their role is to proxy all client requests to an Exchange Server back-end server.

A back-end server is an Exchange Server with a standard, default configuration. There is no configuration option to designate a server as a back-end server. The term back-end

server refers to all servers in an organization that are not frontend servers.

If your Exchange 2000 organization takes advantage of front-end and back-end architecture, you must upgrade your front-end servers before you upgrade your back-end servers.

Certkiller .com has several administrative groups, so we should upgrade all administrative groups one by one. We must upgrade the front-end and back-end before we move on to upgrade the next administrative group.

We know that : "1. The company needs to take advantage of new features in Exchange Server 2003. You must implement these new features for the largest number of users in the shortest time."and that the main Office have 5000 users, Mexico City have 1500 users, Buenos Aires have 400 users and Rio de Janeiro have 1450 users.

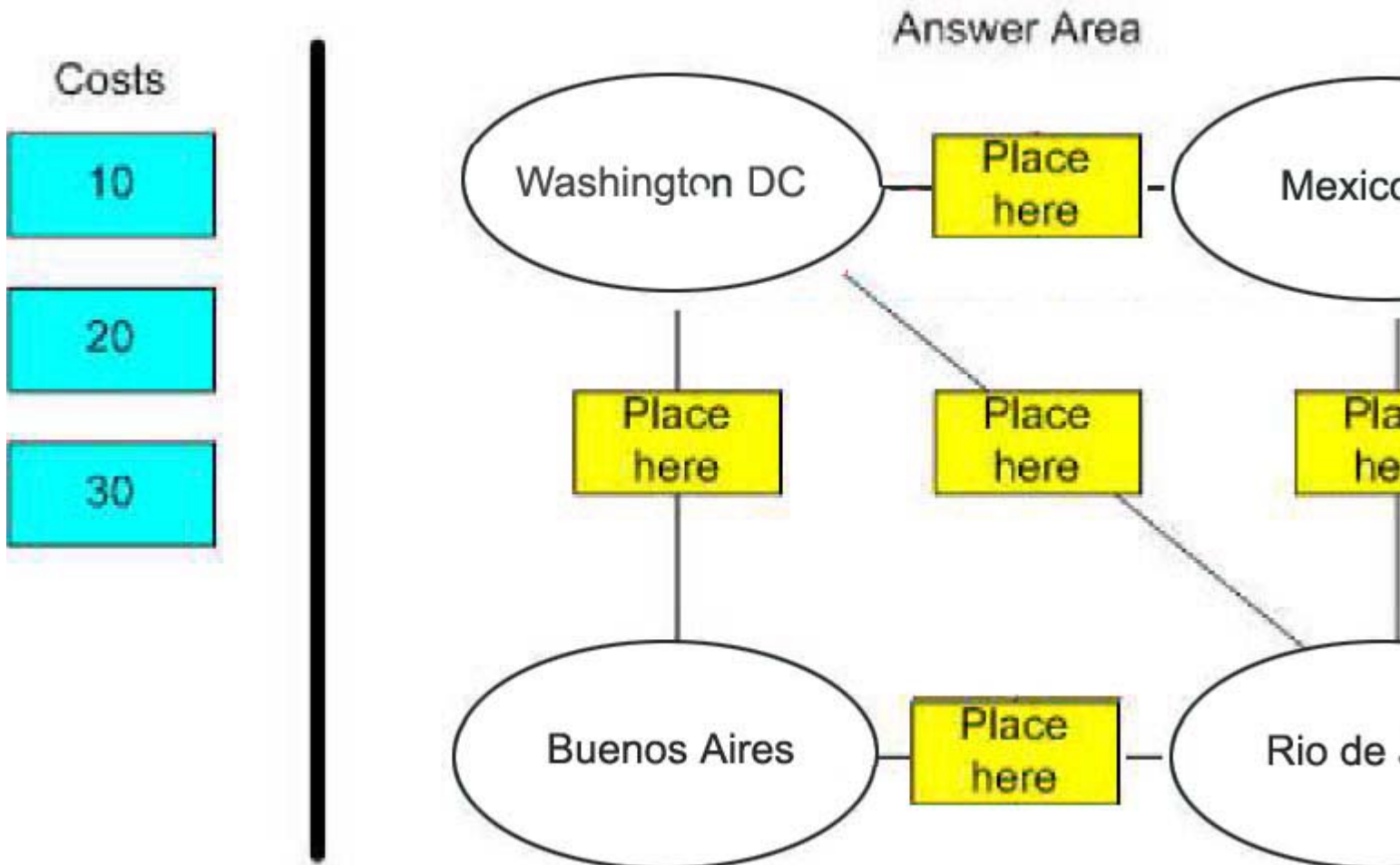
The logical order to upgrade would be : Certkiller 6 and Certkiller 1 (5000 users), Certkiller 7 and Certkiller 2 (1500 users), Certkiller 8 and Certkiller 3 (1450 users), Certkiller 9, Certkiller 4 (400 users).

QUESTION 36

You design a routing topology as shown in the answer area. You need to assign a cost to each connector.

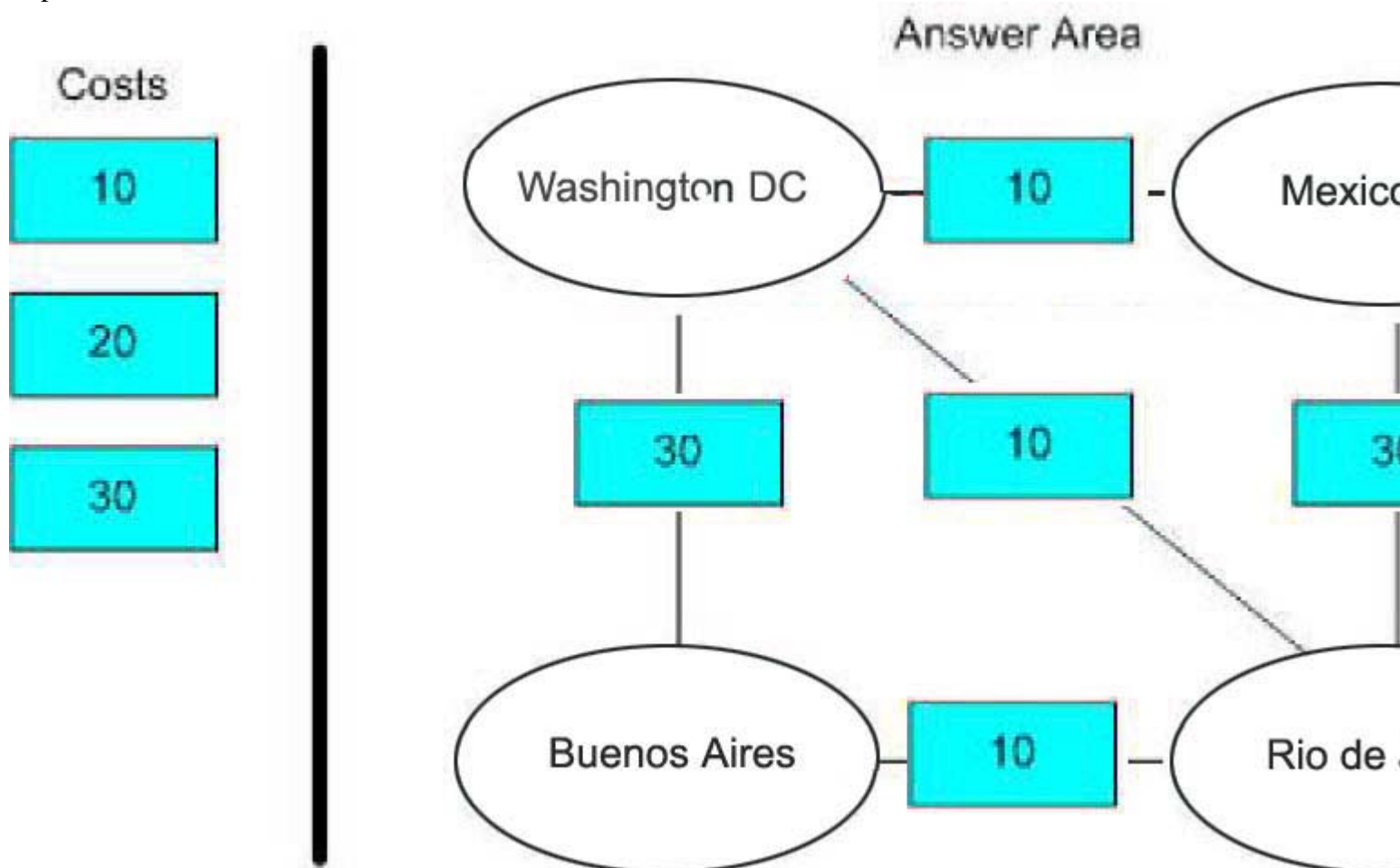
How should you configure the connector costs?

To answer, drag the appropriate costs to the correct locations in the answer area.



Answer:

Explanation:



Routing describes how Exchange Server transfers messages from one server to another. When multiple routing groups exist, messages are routed between routing groups using routing group connectors. When planning your routing topology, you need to plan for the most efficient transfer of messages. Your plan must include which connector will be used to connect routing groups as well as the locations of connectors to messaging systems outside your Exchange Server organization. Careful planning can reduce the volume of network traffic and optimize Exchange Server and Windows services.

Connectors between routing groups are ways to funnel mail. In situations where you have multiple connections to a possible destination, you can define connectors between routing groups to control message flow. Within a routing group, communication between servers is point-to-point, so you cannot determine paths and costs to ensure that the least expensive route between two servers is chosen. However, by creating routing groups, you can assign costs to various paths to ensure the most efficient route is used. Cost is the variable Exchange Server uses to determine the most efficient messaging route.

Exchange Server considers the lowest cost route the most efficient. Exchange Server uses

a more expensive route only if a server or connector is unavailable on the route with the lowest cost. You should assign the lowest costs to the most preferred routes, such as those with the highest available network bandwidth.

T1 connections are set at a lower cost of 10. 56 Kbps links are set to a higher cost of 30. This make the distance of two T1 connections to be preferred to the distance of a single 56 Kbps connection.

Topic 7, Coho Vineyard, Scenario

Time Case until final review 40 minutes

BACKGROUND

1. Over view

Coho Vineyard is an international winery and wine distribution company.

1. Physical locations

Coho Vineyard has vineyards in France, Italy, and Australia. The main office is located in Paris, and the branch offices are located in Paris, Rome, and Sydney. Coho Vineyard has recently purchased a subsidiary location that manufactures oak barrels. This subsidiary is located just outside Paris.

The number of users in each location is shown in the following table.

Location	Number of Users
Paris main office	1,500
Paris branch office	500
Rome branch office	500
Sydney branch office	500
Total users in vineyard locations	100
Mobile sales personnel	50
Subsidiary	20

1. Planned Changes

Coho Vineyard is migrating from Exchange 2000 Server to Exchange Server 2003.

PROBLEM STATEMENTS

Problem Statements

1. The Mobile users at Coho Vineyard need enhanced functionality without compromising security.
2. The subsidiary location needs to be integrated with the Coho Vineyard infrastructure.

EXISTING MESSAGING ENVIRONMENT

1. Administrative structure

1. The administration of the domain and the Exchange organization are configured as shown in the following table.

Group Name	Enlarge Permission	Active Directory Permissions	Comments
MOAdmins	Full Exchange Administrator for the organization	Domain Admins	The members are located at the main office
CityBranchAdmins	Exchange Administrator for the city's administration group	Domain Admins group	Administrator Exchange servers and all user and group accounts in the city's branch office
MOUserAdmins	Exchange View Only Administrator for the organization	Is delegated full control of users and groups in the domain	Administers all user and group accounts in the company

2. All Windows security groups are located in the main office organizational unit (OU).

1. Messaging infrastructure

1. There is one Exchange 2000 back-end server in the main office and one in each of the branch offices.

2. Each office is configured as a separate routing group and administrative group.

3. All routing groups are connected with Routing Group connectors.

4. All of the Exchange 2000 servers run on hardware that is on the hardware compatibility list for Windows 2000 Server and Windows Server 2003.

5. The Exchange organization at the subsidiary includes a single administrative group in a different Exchange organization.

6. The new subsidiary location has a single Exchange 2000 server.

7. The subsidiary location has a 56-Kbps dial-up connection to the Internet.

8. The Exchange server uses this connection for sending and receiving Internet e-mail messages.

9. Coho Vineyard has deployed an Exchange 2000 front-end server at the main office that is configured to support all the required Internet protocols.

10. All users who connect to Exchange from the Internet connect to the front-end server.

1. E-mail Clients

1. Users at the main office and in the branch offices use Microsoft Outlook 2000.

2. The sales personnel travel throughout the world. Each salesperson carries a company portable computer.

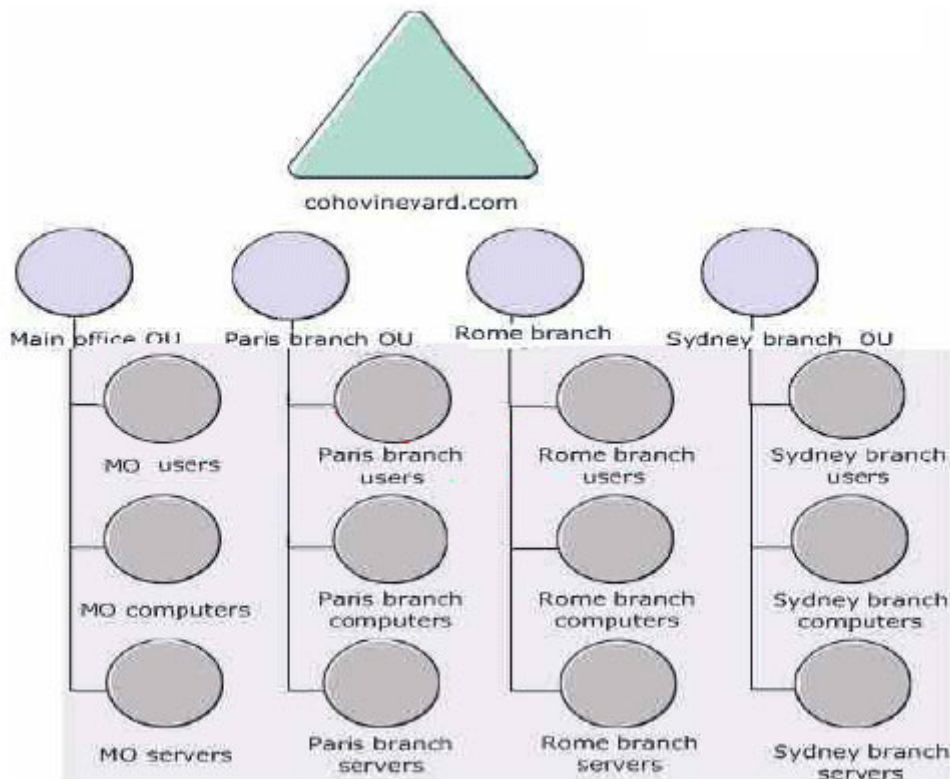
3. Sales personnel and users at vineyard locations use Microsoft Outlook Web Access.

4. The mailboxes for all Outlook Web Access users are located on the Exchange server at the main office. All users run Microsoft Internet Explorer 5.0 or later.

SUPPORTING INFRASTRUCTURE

1. Directory Services

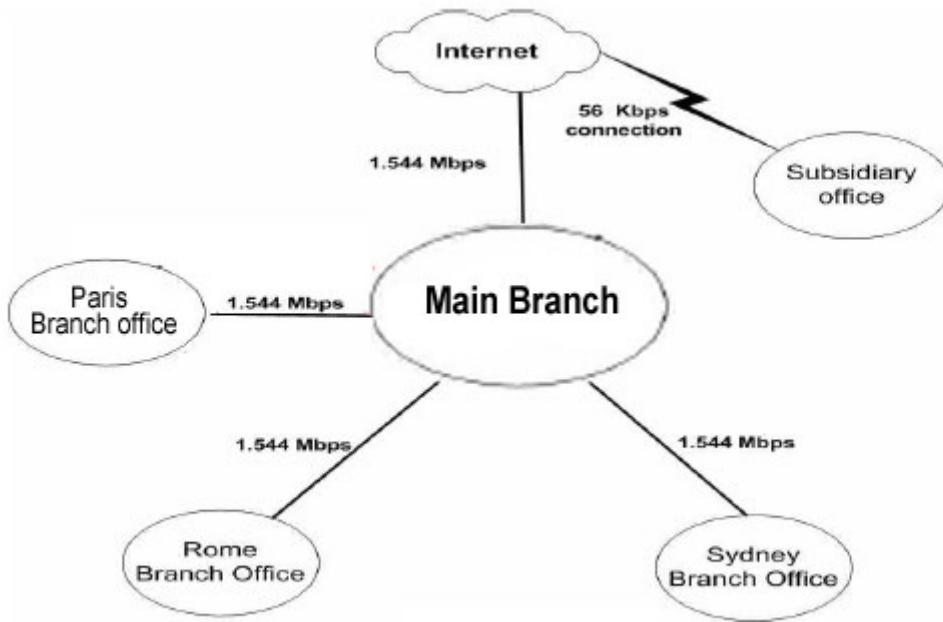
1. Coho Vineyard has deployed a single Windows Server 2003 Active Directory domain named cohovineyard.com. The active Directory configuration is shown in the following diagram.



2. Each branch office contains a single Windows 2000 Server domain controller that is configured as a global catalog server.
3. The main office contains two Windows Server 2003 domain controllers.
4. Both of these domain controllers are configured as global catalog servers.
5. The domain functional level is set to Windows 2000 native.

1. Network Infrastructure

1. The WAN connections have been upgraded recently, and no new upgrades are planned.
2. The company locations and WAN connections are shown in the following diagram.



BUSINESS REQUIREMENTS

1. Security

1. The Exchange 2000 front-end server needs to be upgraded to Exchange 2003 without modifying the way client computers connect to Exchange or the way Internet e-mail is delivered.
2. All client computer connections from the Internet must be as secure as possible.

1. Interviews

Chief Information Officer:

1. We recently bought a new application that we will use to track our wine production.
2. This application is messaging based. It uses several public folders on the Exchange servers to store information.
3. All of the users at the vineyard locations, as well as about 20 users in each branch office, must have access to the application.
4. We need to be able to back up and restore the data used by this application separately from our regular public folders.
5. Our sales personnel are critical to our continued growth.
6. We need to do whatever we can to make them as efficient as possible.

IT Manager:

1. Our IT administrators at the main office are very busy.
2. Ideally we need to make sure that we do not add too much to their workload during the implementation of Exchange 2003.
3. We need to assign as much work as possible to lower level administrators like the MOUserAdmins group.
4. This group of users is not as skilled as our IT administrators, but they do a great job if they are given a procedure and they use familiar tools.
5. We also need to minimize the growth of the Exchange databases during the migration.

Exchange Administrator:

1. Existing hardware can support up to 2,500 mailboxes per server.
2. We have about 20 public folders in active uses in the company.
3. All 20 public folders are replicated to all the Exchange servers in the company.
4. There are two additional public folders named Sales Data and production Data.
5. Both folders are updated two or three times a week.
6. These updates are about 5 MB in size.
7. At least 20 uses in each office access the reports in the Sales Data folder every day.
8. The Production Data folder is accessed primarily by users at the main office.
9. Users from the other offices do not access this folder more than once every two weeks.
10. The only replica of both public folders in on the Exchange server at the main office.

Network Administrator:

1. You need to make sure that you do not create additional network traffic across any of the network connections outside Paris. If possible, you should decrease e-mail related traffic.

Server Administrator:

1. All of our Exchange servers are running Windows 2000 Advanced Server with the latest service packs.
2. Our server management policy states that we do not upgrade from one version of Windows to another.
3. If we need to install Windows Server 2003 on any computers, we will buy new hardware and install a clear version of Windows Server 2003.

TECHNICAL REQUIREMENTS

1. Supporting Infrastructure

1. Only the MOAdmins group should be able to modify the routing configuration for the Exchange organization.
2. The branch office administrators should be able to administer all users, groups, and computers-including Exchange servers-in their respective offices.
3. The branch office administrators must not be able to grant themselves additional the main office.

1. E-mail Client Infrastructure

1. All of the users at the vineyard locations will continue to use Outlook Web Access to access the Exchange servers.
2. The company has not decided which e-mail client they will deploy on the portable computers that are used by the sales personnel.
3. Many of the sales personnel need to be able to read and respond to e-mail and schedule meetings when they are not connected to the Internet.
4. Their messages should be delivered automatically when they connect to the Exchange servers.

Topic 7, Coho Vineyard (5 Questions)

QUESTION 37

You need to design a public folder strategy for the Sales Data and Production Data public folders. What should you do?

To answer, drag the appropriate option or options to the correct location or

locations in the answer area.

Public Folder Replica

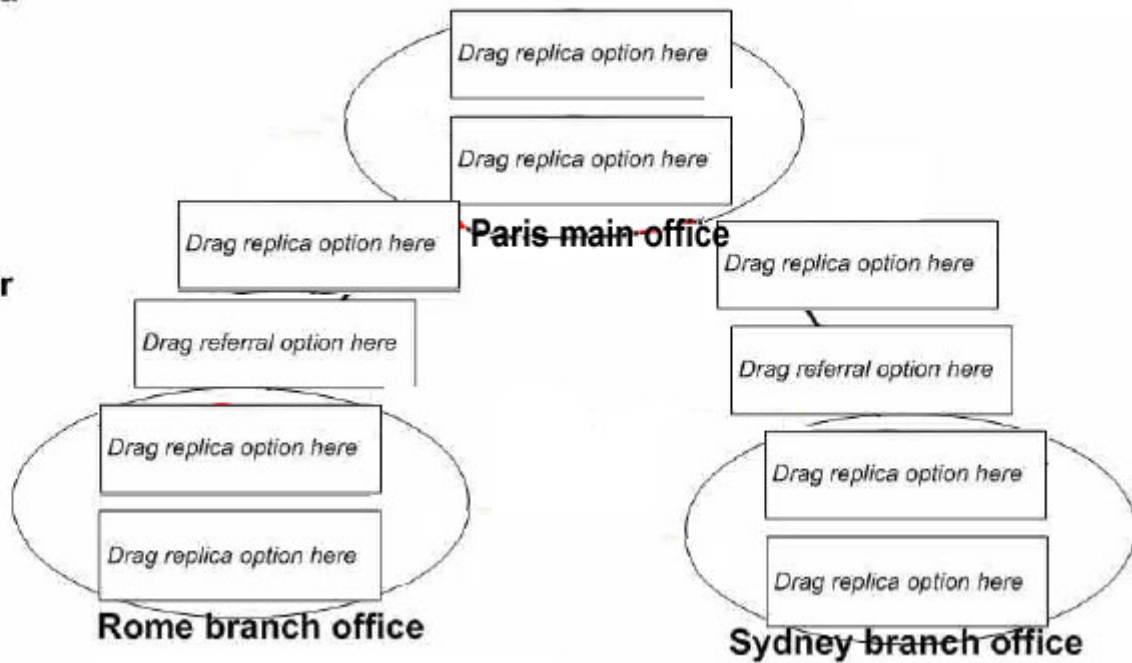
Sales Data
Public Folder Replica

Production Data
Public Folder Replica

Access Public Folder by Referral

Sales Data
Access By Referral

Production Data
Access By Referral



Answer:

Explanation:

Public Folder Replica

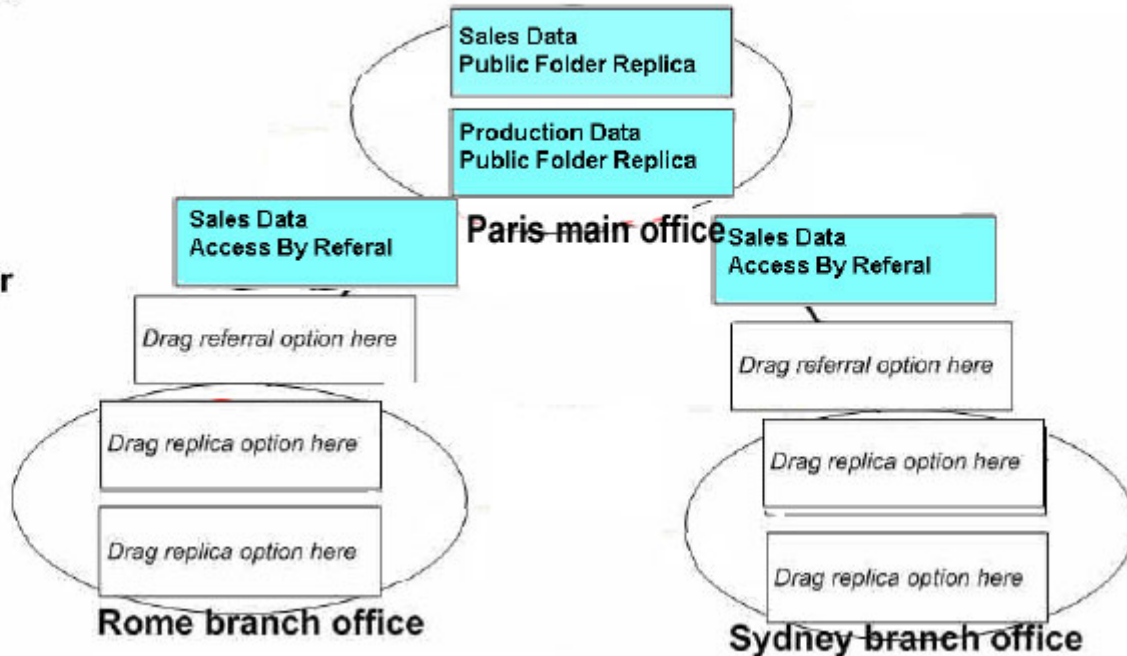
Sales Data
Public Folder Replica

Production Data
Public Folder Replica

Access Public Folder by Referral

Sales Data
Access By Referral

Production Data
Access By Referral



By default, when you create a public folder, only one copy of the public folder exists within the Exchange organization. A public folder can exist in an Exchange organization either as a single copy or as multiple copies. Multiple copies of a public folder are known as replicas. You do not need to create a public folder replica to access public folders across multiple Exchange servers. However, replicas allow users to access a public folder on their local Exchange server, rather than a distant server located on another location. There are several reasons for why you should replicate public folders in your environment:

- * Public folder replication provides fault tolerance for your public folders.
- * Public folder replication provides load balancing to your network.
- * Public folder replication minimizes client traffic across the wide area network (WAN)

For a client to be able to access a public folder on an Exchange server in a routing group that is different from the one to which the client belongs, the connector between the routing groups must be configured to allow public folder referrals. You can enable public folder referrals by using either one of the following methods:

- * Implement and configure a connector between two routing groups.
- * Configure a public folder referral list on the Exchange Server properties.

They tell us that the only replica of Sales Data and Production Data Public folders, are in on the Exchange server at the main office. According with the use of public folders, at least 20 users in each office access the reports in the Sales Data folder every day. Apart from them, other users do not access this folder more than once every two weeks and the Production Data folder is accessed primarily by users at the main office. They can use referrals instead replicas because they tell us that you need to make sure that you do not create additional network traffic across any of the network connections outside Paris. If

possible, you should decrease e-mail related traffic.

Reference

Exchange Server2003 Administration Guide

<http://www.microsoft.com/technet/prodtechnol/exchange/2003/library/admingde.mspx>

Understanding Public Folder Replication and Referrals

<http://support.microsoft.com/default.aspx?kbid=273479>

Exchange Server2003 and Exchange2000 Server Front-End and Back-End

Topology

<http://www.microsoft.com/technet/prodtechnol/exchange/2003/library/febetop.mspx>

QUESTION 38

You need to design a solution for deploying the custom wine production application. Your solution must make as few configuration changes as possible. Which three actions should you perform? (Each correct answer presents part of the solution. Choose three.)

- A. Create a new public folder named ProdData in the default public folder tree on the Exchange back-end server at the main office.
- B. Create a general purpose public folder tree named ProdData on the Exchange back-end server at the main office.
- C. Configure an additional IMAP4 virtual server on the Exchange front-end server at the main office. Associate the IMAP4 virtual server with ProdData.
- D. Configure an additional IMAP4 virtual server on the Exchange back-end server at the main office. Associate the IMAP4 virtual server with ProdData.
- E. Configure an HTTP virtual server on the Exchange front-end server at the main office. Associate the HTTP virtual server with ProdData.
- F. Configure an HTTP virtual server on the Exchange back-end server at the main office. Associate the HTTP virtual server with ProdData.

Answer: B, C, E

Explanation

There are two types of public folder trees: the default public folder tree and the general-purpose public folder trees.

The default public folder tree, also known as the MAPI public folder tree, is the public folder tree that is automatically created by the Setup program when you install the first Exchange server in your organization. The default public folder tree is listed in Exchange System Manager as Public Folders, and it is displayed in Outlook as All Public Folders. The default public folder tree contains the list of all public folders that are within the tree. However, the default public folder tree does not contain the content of the folders themselves.

The default public folder tree is replicated to each Exchange server that contains a public folder store that is associated with that tree. As a result, users can easily browse the public folder hierarchy. By default, this public folder tree exists on every public folder server in an Exchange organization. There can be only one MAPI public folder tree in an Exchange organization.

General-purpose public folder trees are the additional public folder trees that you can

create. A general-purpose public folder tree is replicated only to servers that are running Exchange 2000 Server and later that contain a public folder store associated with that tree. As a result, you can create additional public folder trees that are replicated to selected public folder servers in the Exchange organization.

You use a general-purpose public folder tree when you want to store custom applications data in public folder and you want to maintain the data in a store separate from the other public folder data. For example, you can use one tree to store personnel department applications and use another tree to store accounting applications or research and development applications. You can also use general public folder trees if you want to have the public folder hierarchy replicated to only selected servers.

They are replicating 20 public folders to all the Exchange servers in the company that are in the root hierarchy.

They need to create a general purpose public folder three named ProdData to control the replication to be able to back up and restore the data used by this application separately from our regular public folders and they need to be able to back up and restore the data used by this application separately from our regular public folders.

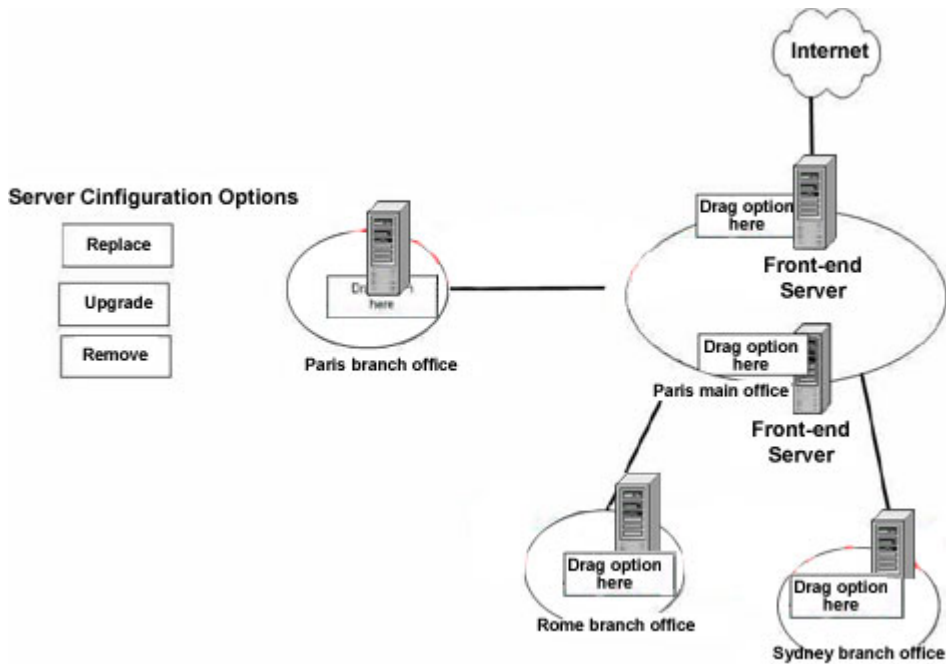
The Front-end server at the main office is already configured to support all the required Internet protocols.

They configure a new an additional IMAP virtual server on the Exchange front-end server at the main office this can be used by the remote locations to access this public folder using a better protocol than https for public folder access One of the main advantages of IMAP is that it makes your e-mail easily accessible from multiple locations and computers. With IMAP, all mail is stored on the IMAP server, but they tell us that all of the users at the vineyard locations will continue to use Outlook Web Access to access the Exchange servers.

QUESTION 39

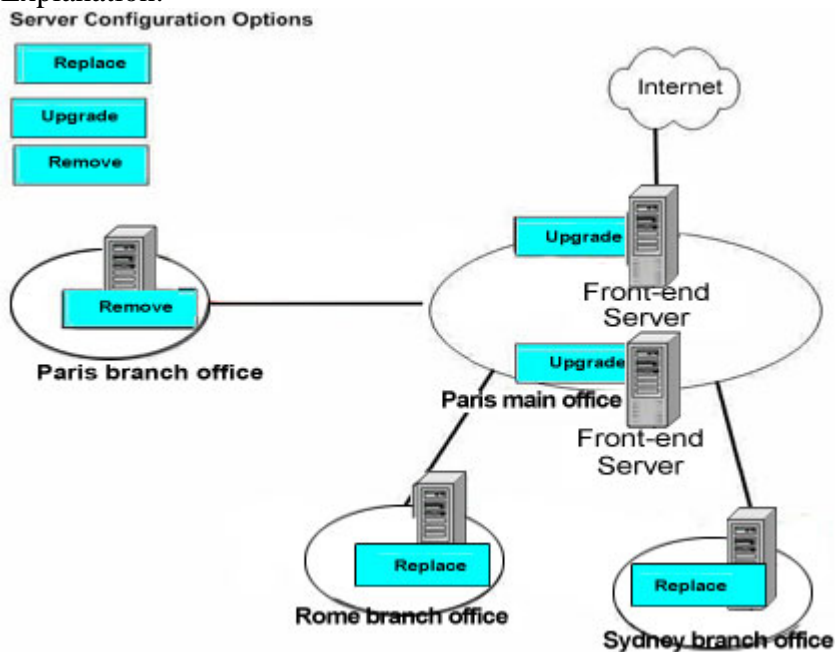
You need to design a strategy for migrating the Exchange servers from Exchange 2000 to Exchange 2003. What should you do?

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



Answer:

Explanation:



The supporting network infrastructure shows us that the Paris Main Office and the Paris Branch Office are connected with a 10 Mbps WAN link. So it would be good thing to remove the servers from the Branch Office and integrate them in the Main Office.

The Security Business Requirements tell us that : "1. The Exchange 2000 front-end server needs to be upgraded to Exchange 2003 without modifying the way client computers connect to Exchange or the way Internet e-mail is delivered." and "2. All client computer connections from the Internet must be as secure as possible." We know

that the remote users are connecting with RPC over HTTPS to access their mail in the Main Office. If we want to implement RPC over HTTPS we will need Exchange 2003 front-end and back-end servers that are running on windows 2003 OS. Therefore we need to replace the frontend and back servers in the Main Office to fulfill this requirement since the Server Administrator told us that : "3. If we need to install Windows Server 2003 on any computers, we will buy new hardware and install a clear version of Windows Server 2003." Exchange 2003 will run nicely if the OS is Windows 2000, so we can upgrade the Exchange 2000 servers to Exchange 2003 since they will not require RPC over HTTP.

QUESTION 40

You need to design a strategy for remote client computer access that meets all business and technical requirements. What should you do?

- A. Configure the HTTP virtual server on the Exchange front-end server to require a secure connection. Instruct the sales personnel to use Microsoft Outlook Web Access to connect to the Exchange front-end server.
- B. Configure the back-end Exchange servers to use static ports for RPC connections. Open the required ports on the firewall. Install Microsoft Outlook 2003 on the portable computers and configure it to connect to the Exchange back-end server using a MAPI connection.
- C. Configure the Exchange front-end server to require secure connections from IMAP4 client computers. Install Microsoft Outlook 2003 on the portable computers and configure it to use a secure IMAP4 connection.
- D. Configure the Exchange servers to support RPC over HTTPS. Install Microsoft outlook 2003 on the portable computers and configure it to use RPC over HTTPS.

Answer: D

Explanation

To use RPC over HTTP, you must install Windows Server 2003 on the computers that are running Exchange Server 2003 and you need Windows 2003 DC running Global catalog role. They tell us that Coho Vineyard has deployed a single Windows Server 2003 Active Directory domain named cohovineyard.com and that the main office contains two Window Server 2003 domain controllers that are also global catalog servers. Because you need to design a strategy for remote client computer access that meets all business and technical requirements, you can think that you can deploy https over RPC, but their users at the main office and in the branch offices use Microsoft Outlook 2000. So, for them to access with https over RPC, they need to run Outlook 2003.

They tell us that we can configure the Exchange servers to support RPC over HTTPS and Install Microsoft outlook 2003 on the portable computers, as is required to access an Exchange 2003 Server using RPC over HTTPS.

Reference

Exchange Server2003 RPC over HTTP Deployment Scenario

<http://www.microsoft.com/technet/prodtechnol/exchange/2003/library/ex2k3rpc.msp>

QUESTION 41

You need to design a strategy for moving the mailboxes from the Exchange server at the Paris branch office to the Exchange server at the main office. What should you do?

- A. Use the Exchange Task Wizard to migrate all the mailboxes to the Exchange 2003 server.
- B. Use the Exchange Mailbox Merge Wizard (Exmerge) to migrate all the mailboxes to the Exchange 2003 server.
- C. Use the Exchange Server Migration Wizard to migrate all the mailboxes to the Exchange 2003 server.
- D. Export the contents of each mailbox to a .pst file. Create a new mailbox on the Exchange 2003 servers for each existing mailbox. Import the .pst file contents into each new mailbox.

Answer: A

Explanation

If Exchange Server 2003 was deployed into an existing Exchange Server 5.5 organization, you can move mailboxes between servers using the Exchange Task Wizard. You can then migrate public folders using the Microsoft Exchange Public Folder Migration Tool (pfMigrate). This tool allows you to migrate both system folders and public folders by creating replicas on the new server and removing the replicas from the source server once replication is complete.

Incorrect Answers

- B. Exmerge is normally used in recovery procedures.
- C. If Exchange Server 2003 was deployed into a new Exchange Server organization instead of joining the existing Exchange Server 5.5 organization, you must use the Exchange Server Migration Wizard to move mailboxes, and then use the Inter-Organization Replication Tool to migrate public folders and free and busy information between the Exchange organizations.
- D. Export the contents of each mailbox to a .pst file. Create a new mailbox on the Exchange 2003 servers for each existing mailbox. Import the .pst file contents into each new mailbox. This will work but require more administrative effort.

Reference

Appendix A - Tools Used with Exchange

Exchange 2003 Deployment Guide Chapter 5 - Inter-Organizational Migration

Topic 8, Prosaware Inc, Scenario

BACKGROUND

1. Overview

Prosaware, Inc. produced manuscripts that are published by other companies.

The company provides e-mail access to employees during business hours only, Monday through Friday from 9:00 A.M. to 5:00 P.M.

1. Physical Locations

The company has one main office and three branch offices in North America. Each office has 600 users. Users work from the office, and they use their own Internet connections to

work from home.

1. Planned Changes

The company will provide after-hours e-mail access to users when they are working from home.

EXISTING MESSAGING ENVIRONMENT

1. E-mail Clients

1. All users run Microsoft Windows XP Professional and Microsoft Outlook in the office and at home.
2. The company uses in an in-house POP3 server for e-mail. This server will be replaced with Exchange Server 2003. Mail will not be migrated from the old server.

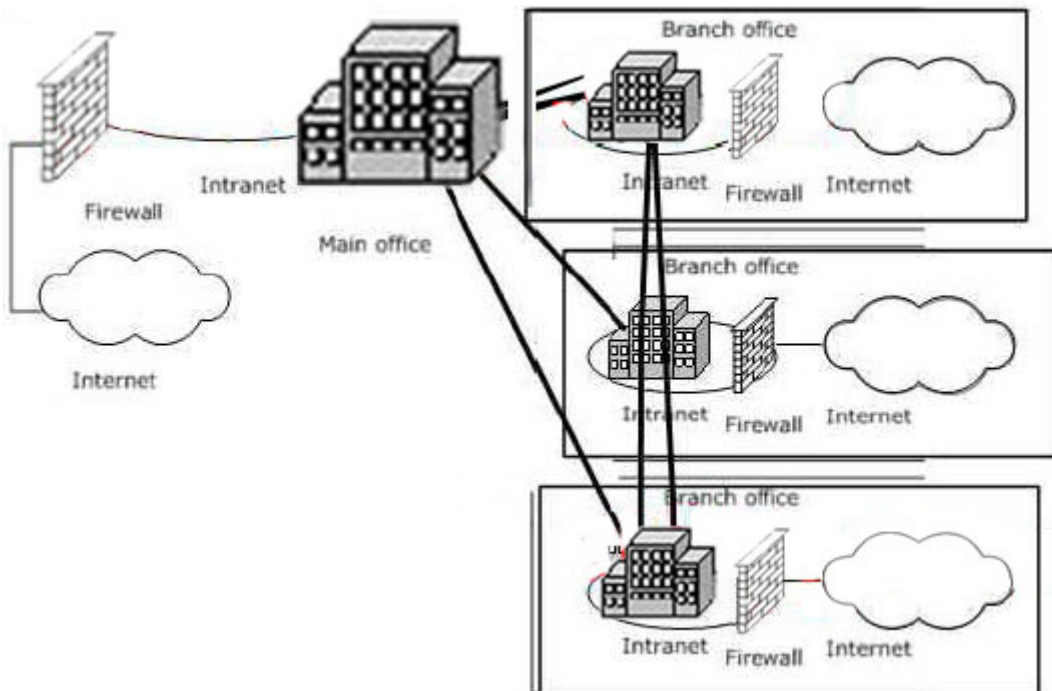
SUPPORTING INFRASTRUCTURE

1. Directory Services

1. The company has a single Active Directory domain with one domain controller at each office.
2. The domain controller at the main office is a global catalog server.

1. Network Infrastructure

1. Each office has an internal network, which is connected to the Internet by a firewall.
2. Each office also has a 128-Kbps WAN connection to the other offices.
3. The relevant portion of the network is shown in the following diagram.



BUSINESS REQUIREMENTS

1. Security

1. Branch office technicians will manage Exchange backup and recovery operations, including single-mailbox recovery, on all servers located in their offices.
2. The central information Technology (IT) group will manage all other aspects of all

servers.

3. The branch office technicians may occasionally manager other aspects of the Exchange servers, under the direction of the central IT group.
4. Branch office technicians must not have permissions on any servers located in other offices.

1. Interviews

Chief Executive Officer:

1. I want all users to have full access to all Exchange e-mail features - including calendars, client-side messaging rules, contacts, and journal entries - at all times.
2. In addition, I want all users to use Microsoft Outlook 2003. I want all users to have a 250-MB limit on their mailboxes. This limit will encourage users to manage their e-mail messages more effectively than they have in the past.
3. We must minimize additional hardware purchase other than the four new servers we bought to run Exchange.

Chief Information Officer:

- 1 We need to ensure that e-mail servers are protected from denial of service attacks.
2. We do not want to manage the technology resources that would be required to allow all users to connect to the company network through a VPN.
3. However, all access to e-mail by remote users must be encrypted.
4. We need to ensure that users have the best e-mail performance possible while minimizing the use of our WAN connections, which have very low bandwidth.

Network Administrator:

1. We need to minimize our backup requirements for the new e-mail system.
2. Each office has the capacity to back up an additional 73 GB of data each weekday.
3. We also need to minimize the complexity of backup and recovery operations, because the office technicians are not well trained.
4. Most importantly, we must be able to restore from a complete mailbox store failure as quickly as possible.
5. We want all aspects of the server configuration to be as simple as possible while meeting our business and technical requirements.

TECHNICAL REQUIREMENTS

1. Message Infrastructure

1. The company will add four Exchange Server 2003 computers. The company wants to spread the messaging workload equally across the four servers. Each server will contain seven 120-GB hard disks.
2. The Exchange server hard disks must be configured to provide the best possible performance. Also, neither the operating system, the Exchange log files, nor the Exchange data must be affected by the failure of a single hard disk.

1. E-mail Client Infrastructure

1. Each user that works from home will connect to his or her local office through that office's Internet connectdion.
2. All users will use remote e-mail capabilities only when they work from home.

Topic 8, Prosaware Inc, (4 Questions)

QUESTION 42

You need to design an administrative model for Exchange Server 2003. What should you?

A. Create an administrative group for each office.

Place each Exchange server that is managed by an office technician into that Office's administrative group.

Assign the central IT group full control over all administrative groups.

Assign each office technician control over his or her office's administrative groups.

B. Create one administrative group.

Place all Exchange servers in the administrative group.

Assign the central IT group full control over the administrative group.

Make each office technician a member of the local Backup Operators group on each group they manage.

C. Create an administrative group for each office.

Place one Exchange server in each group.

Assign the central IT group and each office technician full control over each administrative group.

D. Create one administrative group for all Exchange front-end servers.

Assign each office technician control over this administrative group.

Create another administrative group for all Exchange back-end servers.

Assign the central IT group control over this administrative group.

Answer: A

Explanation

First, let's summon up the things we already know from the Security topic :

1. Branch office technicians will manage Exchange backup and recovery operations, including single-mailbox recovery, on all servers located in their offices.

2. The central information Technology (IT) group will manage all other aspects of all servers.

3. The branch office technicians may occasionally manage other aspects of the Exchange servers, under the direction of the central IT group.

4. Branch office technicians must not have permissions on any servers located in other offices.

Now we already know that we need an administrative group per location, because the branch office technicians will only manage their own servers and the Central IT Admins must be able to manage all servers.

After this we can assign permissions to the branch office users, so that they can manage their own servers. We also assign permissions to the Central IT Admins so that they can manage all servers if necessary.

Incorrect Answers :

B. This conflicts with the security requirement point 4 : "Branch office technicians must not have permissions on any servers located in other offices." The Office technicians will get backup permissions on every exchange server.

C. This conflicts with the security requirement point 4 : "Branch office technicians must not have permissions on any servers located in other offices." The Office technicians will

get Full Control permissions on every exchange server.

D. In this scenario we will not use Front-end Servers. Only Back-end servers with the RPC Proxy software installed.

QUESTION 43

You need to design an e-mail access strategy for remote users. What should you do?

- A. Instruct remote users to connect to their e-mail by using RPC.
- B. Instruct remote users to connect to Outlook Web Access by using only HTTPS.
- C. Instruct remote users to connect to the company network by using PPTP connections.
- D. Instruct remote users to connect to their e-mail by using RPC over HTTP.

Configure the HTTP servers to require encryption.

Answer: D

Explanation

Microsoft Exchange Server 2003 and Microsoft Office Outlook 2003, combined with Windows Server 2003, support the use of RPC over HTTP to access Exchange servers. Using the Microsoft Windows RPC over HTTP feature to enable your users to connect to their Exchange mailbox eliminates the need for remote office users to use a virtual private network (VPN) to connect to their Exchange servers. Users running Outlook 2003 on client computers can securely connect directly to an Exchange server within a corporate environment from the Internet.

To use RPC over HTTP, you must run Windows Server 2003 on the following computers:

All Exchange Server 2003 Servers That Microsoft Office Outlook 2003 Clients Will access using RPC over HTTP, such as mailbox servers and public folder servers.

All Exchange Server 2003 front-end Servers that act as RPC proxy servers.

All global catalog servers that Outlook 2003 Clients and Exchange Server 2003 Servers (that are configured to use RPC over HTTP) use.

Incorrect Answers :

- A. RPC over HTTP must be used. Not RPC only.
- B. We know due to the interview with the Chief Executive Officer that all users (remote and internal) will use the outlook 2003 client. Therefore we also know that Outlook Web Access will not be used.
- C. We know due to the interview with the Chief Information Officer that a VPN technology cannot be used. Therefore we cannot use a PPTP technology.

Reference :

<http://www.microsoft.com/technet/prodtechnol/exchange/2003/library/ex2k3rpc.mspx>

QUESTION 44

You need to designate Exchange server roles and locations. What should you do?



Main office



Branch Office

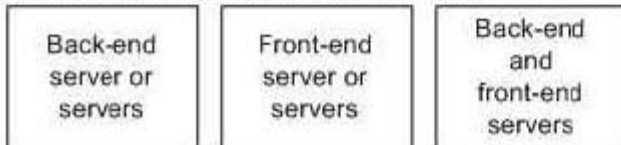


Branch Office



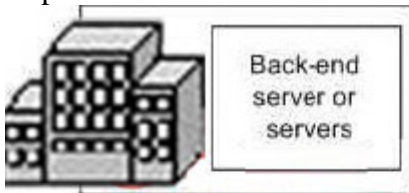
Branch Office

Server roles, select from these

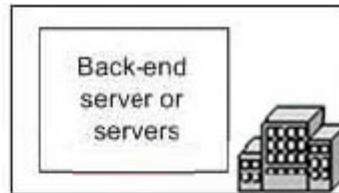


Answer:

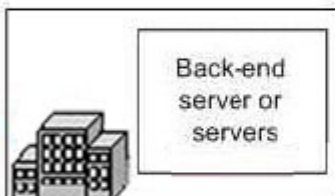
Explanation:



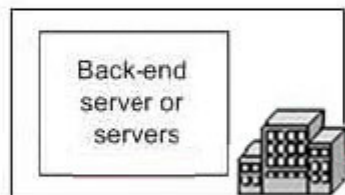
Main office



Branch Office

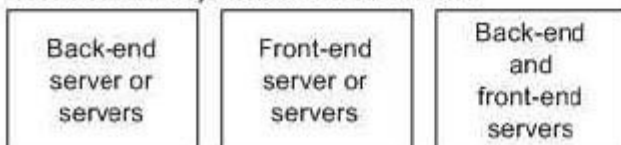


Branch Office



Branch Office

Server roles, select from these



Explanation

Microsoft Exchange Server 2003 and Microsoft Office Outlook 2003, combined with Windows Server 2003, support the use of RPC over HTTP to access Exchange servers. Using the Microsoft Windows RPC over HTTP feature to enable your users to connect to their Exchange mailbox eliminates the need for remote office users to use a virtual private network (VPN) to connect to their Exchange servers. Users running Outlook 2003 on client computers can connect directly to an Exchange server within a corporate environment from the Internet.

It is possible to implement only back-end servers that also have the RPC Proxy installed. This way you can reduce costs but still provide RPC over HTTP access the the outlook 2003 clients.

We know due to the technical requirements, that users will connect to their nearest branch office. Therefore we need to have at least a backend server with the RPC proxy software installed in every location.

We also know due to the interview with the Chief Executive Officer point 3 that : "We must minimize additional hardware purchase other than the four new servers we bought to run Exchange." Therefore it is not allowed to purchase four extra exchange servers to install separate Frond-end Servers.

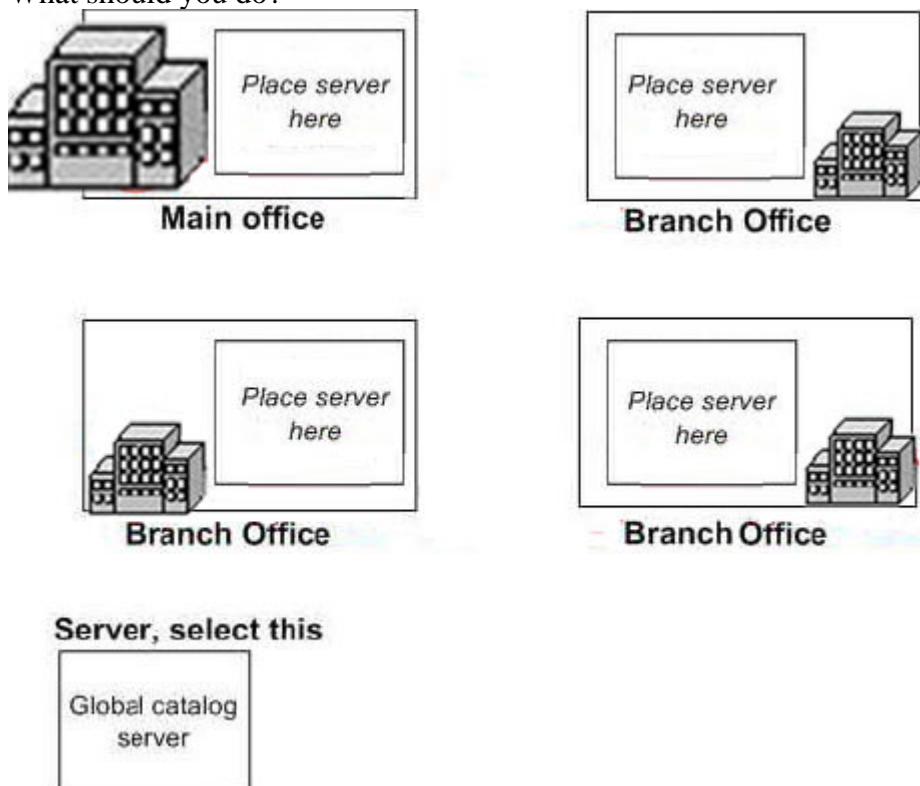
Reference :

<http://www.microsoft.com/technet/prodtechnol/exchange/guides/E2k3RPCHTTPDep/48d6d03d-64c2-470f-9561>

QUESTION 45

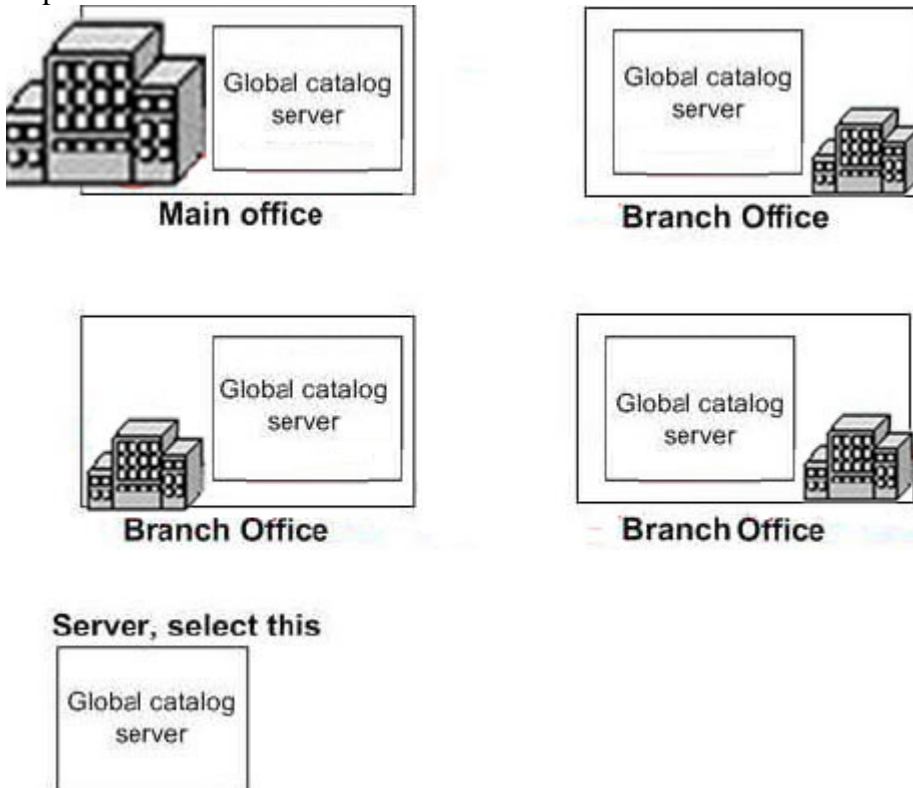
You need to design the replacement of global catalog servers for the new environment.

What should you do?



Answer:

Explanation:



The function of a global catalog server in Active Directory is to maintain a partial attribute set for user objects across all domains in the forest. You may need to make changes in the placement of these servers to provide better support for your Exchange servers.

- * Both Exchange Server and Outlook need a local global catalog server. The global catalog server is critical for Exchange Server services, including log on, group membership, store services, and access to the global address list (GAL).

- * Deploying global catalog servers locally to both servers and users can, with proper configuration, make address lookups more efficient.

- * Contacting a global catalog server across a slow connection increases network traffic and impairs the user experience.

Regarding due to point 4 of the interview with the Chief Information Officer : " We need to ensure that users have the best e-mail performance possible while minimizing the use of our WAN connections, which have very low bandwidth." Therefore we need to reduce WAN traffic between the offices. A good idea will be by placing Global Catalog Servers in every location.

Topic 9, A. Datum Corporation, Scenario

BACKGROUND

1. Overview

A. Datum Corporation is a company that has a wholly owned subsidiary named Certkiller .com.

1. Physical Locations

A. Datum Corporation has an office in New Delhi that includes 500 users.
Certkiller .com has an office in Mumbai that includes 1,000 users.

1. Planned Changes

The company plans to migrate its messaging environment from Exchange Server 5.5 to Exchange Server 2003.

PROBLEM STATEMENTS

1. Administrators report that there is a lack of server capacity for future growth in the number and size of mailboxes.
2. The messaging infrastructure for Certkiller .com will be partitioned into a separate Exchange organization to facilitate the future sale of the company.

EXISTING MESSAGING ENVIRONMENT

1. Administrative Structure

1. Administration is centralized in the New Delhi office. All Exchange Server computers are managed by a single group of messaging administrators.
2. These administrators are responsible for server maintenance, desing and implementation of GPOs, installation of antivirus software, and the design and implementation procedures for the backup and restoration of data.
3. One employee named Certkiller is responsible for maintaining the availability of all conference rooms in adatum.com. Her user account is the primary account for the conference room mailboxes in addition to her personal mailbox.

1. Messaging Infrastructure

1. The network contains a single Exchange Server 5.5 organization for both companies. An Exchange Server named EX1 contains mailboxes for all users.
2. EX1 runs Microsoft Windows 2000 Server SP1 and Exchange Server 5.5 SP3.

1. E-mail clients

1. When working at the office, users connect to their mailboxes by using Microsoft Outlook 2000.
2. All users have portable computers and periodically connect to their mailboxes from remote locations such as a home office by using Outlook 2000 and a MAPI connection over a virtual private network (VPN).
3. All home users report that they use Microsoft Internet Explorer 5.01 or later.

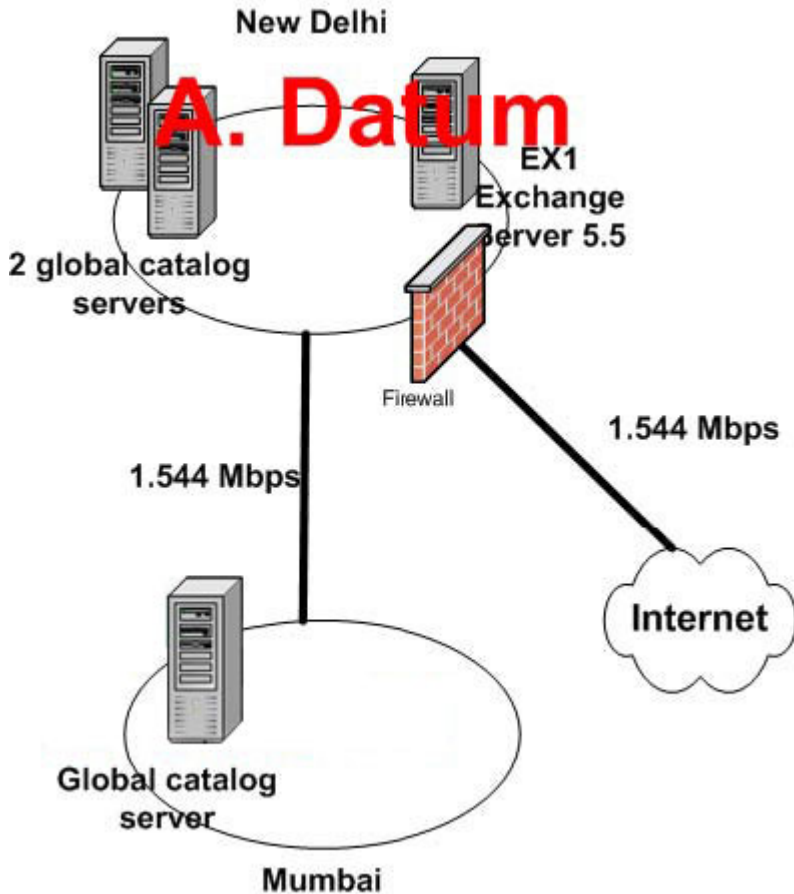
SUPPORTING INFRASTRUCTURE

1. Directory Services

1. The network consists of a single-domain Active Directory forest named adatum.com. The functional level of the forest is Windows Server 2003.

1. Network Infrastructure

1. The company registered adatum.com and Certkiller .com for use as the external DNS Internet domains.
2. The network configuration is shown in the following diagram.



3. A Windows Server 2003 computer named DNS1 hosts the internal adatum.com and Certkiller .com DNS zones.
4. A Windows Server 2003 computer named DNS2 hosts the external adatum.com and Certkiller .com DNS zones.
5. The company has a third-party X.500 directory that contains person objects. For security reasons, these objects must not be located in the adatum.com forest.
6. Mail-enabled InetOrgPerson objects exist in Active Directory for the objects in the third-party directory.
7. A member server named Server1.adatum.com will be available to host Active Directory Connector (ADC).

BUSINESS REQUIREMENTS

1. Security

1. The company's written security policy requires the minimum number of ports possible to be opened on the firewall to allow home users to access their e-mail messages.
2. The written policy also requires that user passwords for company user accounts must not be stored permanently in the Web browsers of home users.
3. You need to ensure that the user account that will install ADC has only minimum necessary permissions.

1. Interviews

Chief Information Officer

1. You need to minimize the disruption to the users during the migration.

2. Users are required to enable the out-of-office notification when they are on vacation.
3. Free/Busy information in the Outlook Calender is used extensively in the company.
4. You need to minimize the disruption to the users at Certkiller .com in the event of a single Exchange server failure.
5. users at Certkiller .com must maintain access to resources in adatum.com during te migration.

TECHNICAL REQUIREMENTS

1. Messaging Infrastructure

1. The company plans to implement adatum.com and Certkiller .com as separate Exchange organizations with separate identities.
2. You purchase three new server computers for the New Delhi office. The servers are shown in the following table.

Server name	Server type	External IP address
EX2	Single server	131.107.0.1
EX3	Single server	Not available
EX4	Single server	131.107.0.2

3. There is no budget for additional hardware during the migration.
4. The company wants EX4 to be used for incoming Internet e-mail messages only when EX2 is unavailable. You need to ensure that internal e-mail messages are sent only to servers in the current environment until the migration is complete.
5. The new servers will be installed in the Mumbai office as a two-node cluster named EX5, and the cluster will belong to the new Exchange Server 2003 organization for Certkiller .com.
6. You plan to install Windows Server 2003 and Exchange Server 2003 on each server.
7. You plan to perform a one-time migration of mailboxes for Certkiller .com users to EX5. The global address list must be available for all users during and after the migration.
8. To the maximum extent possible, you need to ensure that only the e-mail messages from the last six months are migrated.

Topic 9, A. Datum Corporation (5 Questions)

QUESTION 46

You need to implement an e-mail client that can be used by all home users at A. Datum Corporation. You want to minimize the amount of additional configuration that users need to do to their e-mail clients.
What should you do?

- A. Enable forms based authentication. Instruct the users on the use of Outlook Web Access.
- B. Enable ports 110 and 995 on the firewall. Create and configure a POP3 virtual server to enable ports 110 and 995. Instruct users to install a POP3 client.
- C. Enable ports 143 and 993 on the firewall. Create and configure a IMAP4 virtual server to enable ports 143 and 993. Instruct users to install an IMPAT4 client.
- D. Configure EX2 to use RPC over HTTP and configure an RPC virtual directory in IIS. Configure EX2 to act as an RPC proxy server. Instruct users to obtain and install Outlook 2003.
- E. Configure EX2 to use RPC over HTTP and configure an RPC virtual directory in IIS. Instruct users on the use of Outlook Web Access.

Answer: A

Explanation

The existing messaging environment told us that : "1. When working at the office, users connect to their mailboxes by using Microsoft Outlook 2000. and 2. All users have portable computers and periodically connect to their mailboxes from remote locations such as a home office by using Outlook 2000 and a MAPI connection over a virtual private network (VPN)."

The security business requirements told us that : "1. The company's written security policy requires the minimum number of ports possible to be opened on the firewall to allow home users to access their e-mail messages. and 2. The written policy also requires that user passwords for company user accounts must not be stored permanently in the Web browsers of home users."

We know know that the existing remote client connections via outlook 2000 and VPN must be replaced by a simpler solution since the firewall should be configured with a minimum of open ports. Outlook Web Access with form-based authentication will be a simpler setup for this scenario. Enabling forms-based authentication (Cookie-auth) lets you enable a new logon page for Outlook Web Access that stores the user's name and password in a cookie instead of in the browser. When a user closes the browser, the cookie is cleared. Additionally, after a period of inactivity, the cookie is cleared automatically. To access e-mail, the new logon page requires the user to enter a domain, a user name, and a password, or a full user principal name (UPN) e-mail address and password.

QUESTION 47

You need to configure the mail exchanger (MX) resource records for EX2 and EX4 on the external DNS adatum.com zone. How should you configure the MX records for the adatum.com zone?

Server	Preference	Mail Exchanger
EX2	<input type="text" value="Place preference here"/>	<input type="text" value="Place Mail Exchanger here"/>
EX4	<input type="text" value="Place preference here"/>	<input type="text" value="Place Mail Exchanger here"/>

Select from these

Preference

<input type="text" value="5"/>	<input type="text" value="10"/>
--------------------------------	---------------------------------

Mail Exchanger

<input type="text" value="ex2.adatum.com"/>	<input type="text" value="ex4.adatum.com"/>
<input type="text" value="207.46.245.222"/>	<input type="text" value="207.46.245.214"/>

Answer:

Explanation:

Server	Preference	Mail Exchanger
EX2	<input type="text" value="5"/>	<input type="text" value="ex2.adatum.com"/>
EX4	<input type="text" value="10"/>	<input type="text" value="ex4.adatum.com"/>

Select from these

Preference

<input type="text" value="5"/>	<input type="text" value="10"/>
--------------------------------	---------------------------------

Mail Exchanger

<input type="text" value="ex2.adatum.com"/>	<input type="text" value="ex4.adatum.com"/>
<input type="text" value="207.46.245.222"/>	<input type="text" value="207.46.245.214"/>

A mail exchanger record is a DNS record that the e-mail server names for your domain so that you can receive SMTP e-mail from Internet hosts. Transferring messages between SMTP hosts is dependent on DNS. When an SMTP host sends an e-mail message to another SMTP host, DNS resolves the domain name of the receiving host to its name and

then the Transmission Control Protocol/Internet Protocol (TCP/IP) address by first using MX records.

To receive e-mail from the Internet, you must configure MX records for all SMTP mail domains hosted on your network. Remote SMTP hosts use the MX records in external DNS servers to locate the messaging servers for your domain name. You must configure the MX records for all your SMTP address spaces. Secondly, to be able to recognize what host matches with your MX record, you will need two A records, one for each host. The interview with the Messaging Infrastructure Technician told us that : "The company wants EX4.adatum.com to be used for incoming Internet e-mail messages only when EX2.adatum.com is unavailable. You need to ensure that internal e-mail messages are sent only to servers in the current environment until the migration is complete." In case your mail server fails you'd like to still be able to receive incoming e-mail messages. For that to happen we need to configure two MX records with two different priorities. One for EX1.adatum.com with a priority of 5, and one for EX4.adatum.com with a priority of 10.

QUESTION 48

You need to be able to delegate responsibility for administration of the Exchange servers. Where should you place the Exchange servers?

- A. in a new subdomain named exchange.adatum.com
- B. in a new Active Directory forest exchange local
- C. in a new OU named ExchangeServers in adatum.com
- D. in the default Domain Controllers OU in adatum.com

Answer: C

Explanation

Companies that use the centralized administrative model allocate the administrative tasks of the entire Exchange Server organization to a single group or department. In Exchange Server 2003, a company organized around a centralized model can implement a small number of administrative groups or a single administrative group to contain all Exchange Server objects, whether you have a single data center or a large number of branch offices. Doing so enables you to delegate control over the entire organization to your centralized group of administrators by assigning permissions on the Exchange Server organization object.

The existing messaging environment tells us that : "1. Administration is centralized in the New Delhi office. All Exchange Server computers are managed by a single group of messaging administrators."

Therefore we can create an OU and place all exchange server in that OU. After this we can delegate permissions to that OU for the messaging administrators.

QUESTION 49

You need to ensure that Certkiller's user account is associated with only her mailbox during and after the migration. You want to achieve this goal by using the minimum amount of administrative effort.

What should you do?

- A. Run the Resource Mailbox Wizard to mark the conference room mailboxes as resource mailboxes.
- B. The the Migration Wizard to migrate the conference room mailboxes to the new server.
- C. Create a comma-seperated value (CSV) file that assigns Certkiller's user account to the obj-users hidden attribute.
- D. Create a comma-separated value (CSV) file that sets a custom attribute with the NTDSNoMatch value on each conference room mailbox.

Answer: A

Explanation

The Resource Mailbox Wizard resolves multiple Exchange mailboxes to one NT account by letting you specify one mailbox as the primary and setting the other mailboxes as resource mailboxes. Using this wizard, you can match the appropriate primary mailbox to the Active Directory account and stamp other mailboxes with the NTDSNoMatch attribute, which designates the mailboxes as resource mailboxes. You can either make these changes online or export a commaseparated value (.csv) file that you can update and import into the Exchange 5.5 directory.

QUESTION 50

You need to add your user account to the appropriate groups sot aht you can install ADC on Server1. To which two groups should you add your user account? (Each correct answer persents part of the solution. Choose two.)

- A. Domain Admins for adatum.com
- B. Enterprise Admins for adatum.com
- C. Schema Admins for adatum.com
- D. Exchange Full Administrator for the organization
- E. Exchange Services
- F. Exchange Administrators
- G. Local Administrators for EX1
- H. Local Administrators for Server1

Answer: B, C

Explanation

To successfully install the Active Directory Connector (ADC) and configure a Connection Agreement, you must be able to log on to Windows 2000 Server with an account that carries distinctive credentials.

When you first install an ADC in a Windows 2000 forest, the ADC Setup program extends the Active Directory schema with the Exchange 2000 schema extensions. To do this, the account that you are running Setup from must belong to a member of the Schema Administrators group or otherwise have permissions to extend the schema.

Additionally, ADC Setup creates objects in the Active Directory Configuration container. This requires that the account running Setup belong to the Enterprise Administrators group. This permission is a prerequisite of the ADC installation process

and Setup cannot succeed without it.

Finally, ADC Setup creates a security group in the local domain called "Exchange Services." This requires that the account you are running Setup from belongs to a member of the Domain Administrators Group or otherwise has permissions to create objects in the Users container. If this group is inadvertently deleted, a reinstallation of the ADC over the existing installation will re-create this group without adverse effects to Exchange or the AD.

Topic 10, Baldwin Museum of Science, Scenario

BACKGROUND

1. Overview

Baldwin Museum of Science is a network of four research centers that are open to the public and employ field researches and senior research staff from many disciplines.

1. Physical Locations

The main office of the museum is located in Toronto. The three branch offices are located in Montreal, Ottawa, and Quebec.

1. Planned Changes

The museum is planning to upgrade its Exchange Server 5.5 messaging environment to Exchange Server 2003. The company plans to consolidate administration of the Exchange Server 2003 environment as soon as possible.

PROBLEM STATEMENTS

The museum is merging with a research firm named Certkiller .com. The only office of Certkiller .com is in Moscow.

The Montreal, Ottawa, and Quebec offices lack a secure server room and administrative resources. The message stores and the administration of messaging for the museum must be consolidated in the Toronto office as soon as possible.

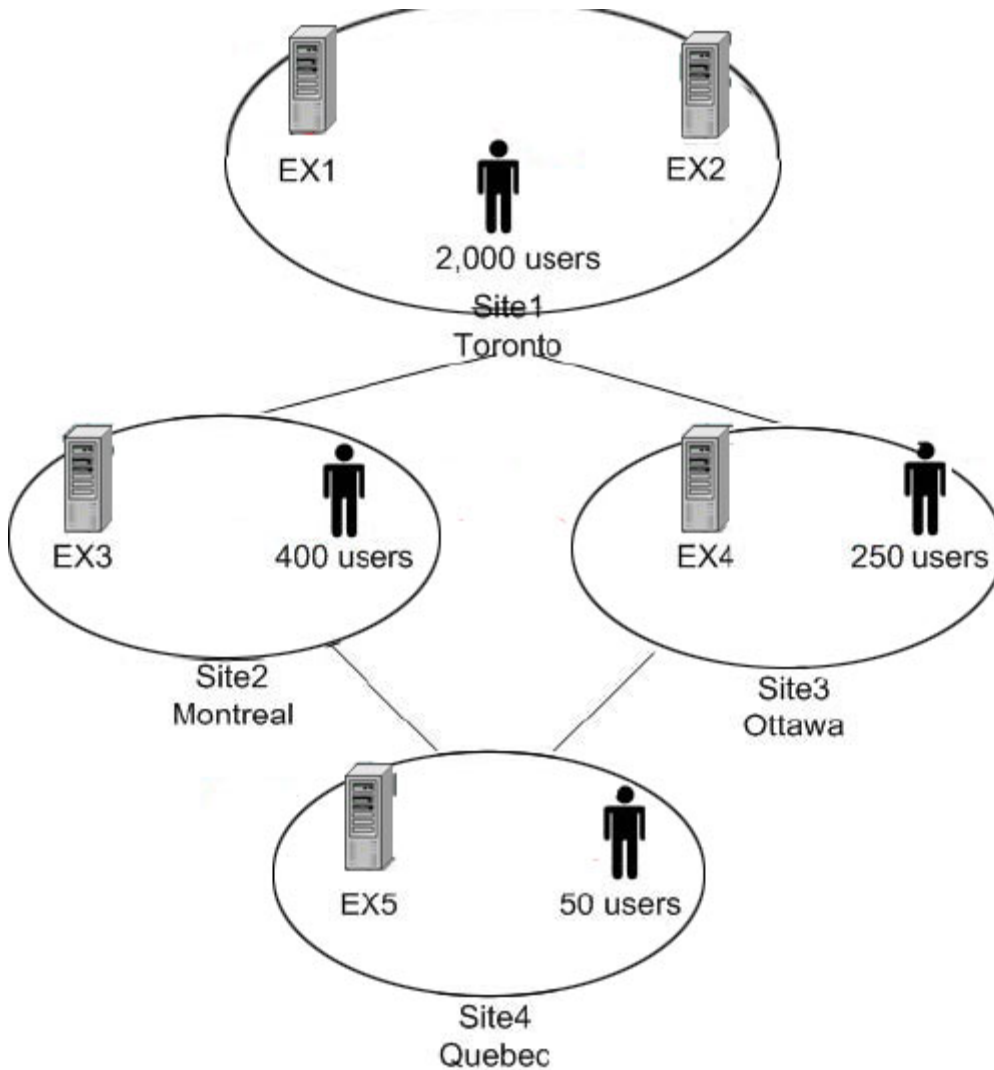
EXISTING MESSAGING ENVIRONMENT

1. Administrative Structure

1. The museum currently has a distributed administrative structure.
2. The Exchange Server 5.5 organization is named BaldwinMuseum(ofScience)

1. Messaging infrastructure

1. The Exchange Server 5.5 routing topology for the museum is shown in the following diagram.



1. E-mail Clients

1. All current users at the museum use Microsoft Outlook 2000 as their e-mail client.
2. Many users at the museum have server-side and client-side Inbox rules.
3. Users at the museum do not access any public folders by using their e-mail clients.
4. All users at Litware, Inc., use a POP3 client on their portable computers to connect to an ISP-hosted e-mail system both from the office and from remote locations.

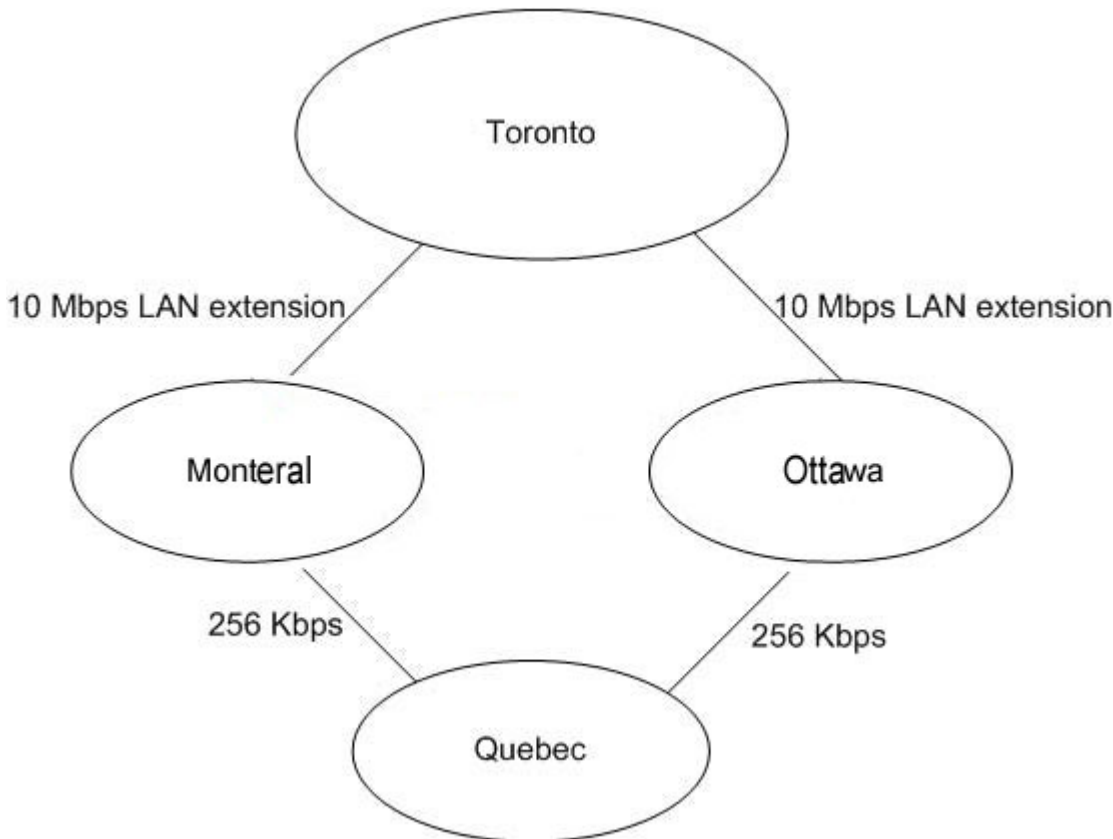
SUPPORTING INFRASTRUCTURE

1. Directory Services

1. The network for the museum consists of a single-domain Active Directory forest named baldwinmuseumofscience.com.
2. The domain currently contains a single Microsoft Windows Server 2003 domain controller that acts as a global catalog server in the Toronto office.

1. Network Infrastructure - Baldwin Museum of Science

1. The museum network is shown in the following diagram.



2. Routing costs for all WAN connections are set to the same value.
3. The global catalog server in the Toronto office acts as an DNS server for the internal baldwinmuseumofscience.com zone.
4. A Windows Server 2003 member server named DNS1 in the Toronto office is configured to host the external baldwinmuseumofscience.com zone.
5. In addition, member servers are distributed as shown in the following table.

Server Name	Operating System	Location
Server1	Windows Server 2003 with most recent pack	Toronto
Server2	Windows NT Server 4.0 SP6a	Montreal
Server3	Windows 2000 Server SP3	Ottawa

1. Network Infrastructure - Litware, Inc.
1. The Litware, Inc., network consists of a LAN in the Amsterdam office that supports 800 users.
2. Litware Inc. relies on a ISP for DNS name resolution services. Litware Inc. has an independent connection to the Internet.
3. The Toronto office of the Baldwin Museum of Science and the Amsterdam office of Litware, Inc., are connected by using a VPN connection over the Internet.

BUSINESS REQUIREMENTS

1. Business Factors
 1. You need to perform the migration to Exchange Server 2003 at the Baldwin Museum of Science by using the minimum amount of administrative effort.
 2. You also need to ensure that users experience the minimum amount of disruption to

their messaging capabilities during the migration.

3. Messages that have large attachments, such as research documents, must be scheduled to use the VPN connection between the Toronto office and the Litware, Inc., office only during off-peak hours whenever possible.

4. Costs for the deployments of e-mail clients for Litware Inc. must be minimized as much as possible.

5. Administrative assistants for Litware, Inc., must be able to send messages and respond to messages from research staff on behalf of senior staff members.

6. The Field Researchers in the Litware, Inc., office must digitally encrypt messages that they send to their colleagues in the field.

1. Security

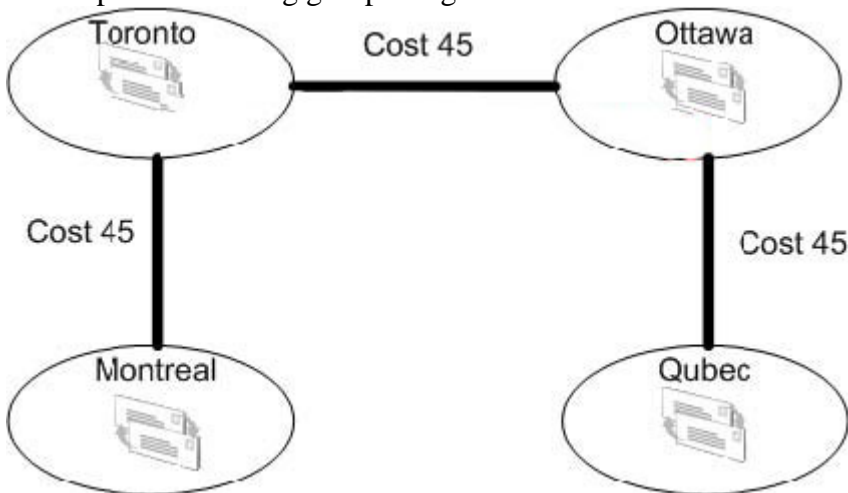
1. The Active Directory database must be physically secured and protected against the failure of a single domain controller.

TECHNICAL REQUIREMENTS

1. Messaging Infrastructure

1. When the migration to Exchange Server 2003 at the Baldwin Museum of Science is complete, additional Windows Server 2003 and Exchange Sever 2003 computers will be deployed as necessary for Litware, Inc., as part of a separate Exchange Server 2003 organization named Litware.

2. The planned routing group design for the museum is shown in the following diagram



3. You need to ensure that e-mail messages will be delivered to the Quebec office even if the physical connection between the Ottawa and Quebec offices fails.

4. Remote bridgehead servers will be installed in the Amsterdam and Toronto offices to route e-mail messages between the two Exchange organizations over the Internet.

5. You need to ensure that all e-mail messages from Baldwin Museum of Science users in Canada to Litware, Inc., users are routed through the bridgehead server for Litware, Inc.

6. You want any new Exchange Server 5.5 mailboxes for the museum to be created on the servers in the Toronto office only.

7. You need to ensure that Single Instance Store (SIS) is maintained on the Exchange Server 5.5 information stores for as long as possible during the migration.

8. Two additional servers are available to act as back-end Exchange Server 2003 mail servers in the Toronto office. You plan to name these servers EX11 and EX12. No

additional servers are available to assist with the migration.

1. Supporting Infrastructure

1. During the period of coexistence of Active Directory and Exchange Server 5.5, user accounts and their mailboxes will be created from Active Directory.
2. You need to ensure that replication between Active Directory and the Exchange Server 5.5 directory has the minimum possible effect on the network traffic between offices.
3. You need to ensure that duplicate mailboxes are not created during the period of coexistence.

1. E-mail Client Infrastructure

1. You need to ensure that Field Researchers at Litware, Inc., have the minimum possible effect on network traffic when accessing their mailboxes from remote locations.

Topic 10, Baldwin Museum of Science (4 Questions)

QUESTION 51

You need to implement EX11 as an Exchange 2003 mailbox server and move mailboxes to EX11. What should you do?

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

Actions	Steps, place here
Install Exchange Server 2003 on EX11 and join EX11 to the same site as the Exchange 5.5 servers in the main office.	Place first step here
Use the Exchange Task Wizard to move mailboxes from the Exchange 5.5 servers to EX11.	Place second step, if any, here
Use the Migration Wizard to migrate mailboxes from the Exchange 5.5 servers to EX11.	Place third step, if any, here

Answer:

Explanation:

Steps, place here

Install Exchange Server 2003 on EX11 and join EX11 to the same site as the Exchange 5.5 servers in the main office.

Use the Exchange Task Wizard to move mailboxes from the Exchange 5.5 servers to EX11.

Use the Migration Wizard to migrate mailboxes from the Exchange 5.5 servers to EX11.

Place third step, if any, here

If Exchange Server 2003 was deployed into an existing Exchange Server 5.5 organization, you can move mailboxes between servers using the Exchange Task Wizard. You can then migrate public folders using the Microsoft Exchange Public Folder Migration Tool (pfMigrate). This tool allows you to migrate both system folders and public folders by creating replicas on the new server and removing the replicas from the source server once replication is complete. If Exchange Server 2003 was deployed into a new Exchange Server organization instead of joining the existing Exchange Server 5.5 organization, you must use the Exchange Server Migration Wizard to move mailboxes, and then use the Inter-Organization Replication Tool to migrate public folders and free and busy information between the Exchange organizations.

The business requirements tell us that : "1. You need to perform the migration to Exchange Server 2003 at the Baldwin Museum of Science by using the minimum amount of administrative effort." and the Technical requirements tell us that : "1. When the migration to Exchange Server 2003 at the Baldwin Museum of Science is complete, additional Windows Server 2003 and Exchange Sever 2003 computers will be deployed as necessary for Litware, Inc., as part of a separate Exchange Server 2003 organization named Litware."

Now we know that Baldwin Museum of Science will not change their Exchange Server 2003 organization and Litware, Inc will use a seperate Exchange organization. Therefore we need to install Exchange 2003 on the EX11 server and join it to the existing site as the exchange 5.5 servers. After that we can use the Exchange Task Wizard to move the maiboxes.

QUESTION 52

You need to design a routing configuration between the Toronto office and the Litware, Inc., office. You need to ensure that the configuration requires the minimum amount of administrative effort to create and maintain.
What should you do?

- A. Install an X.400 connector to connect the two offices.
- B. Install an SMTP connector to connect the two offices.
- C. Configure the appropriate mail exchange (MX) resource records to route e-mail messages between the two offices.
- D. Configure the appropriate name server (NS) resource record to route e-mail messages between the two offices.

Answer: B

Explanation

The Technical Requirements tell us that : "4. Remote bridgehead servers will be installed in the Amsterdam and Toronto offices to route e-mail messages between the two Exchange organizations over the Internet. AND 5. You need to ensure that all e-mail messages from Baldwin Museum of Science users in Canada to Litware, Inc., users are routed through the bridgehead server for Litware, Inc."

Exchange 2000 and Exchange 2003 work differently than Exchange Server 5.5. SMTP is an add-on to Exchange Server 5.5 through Internet Mail Service. SMTP is native to Exchange 2000 and Exchange 2003. Everything is SMTP-based. The default SMTP virtual server, by itself, can handle all Internet traffic (inbound and outbound).

Typically, the main reason for an SMTP connector is either to send mail a certain way to a certain domain (for example, to forward messages to a specific smart host for that domain only or to send HELO instead of EHLO) or to take the place of an IMS in an environment that includes Exchange Server 5.5.

To create and securely configure the SMTP connector follow these steps: 1. Start Exchange System Manager.

2. Expand the Administrative Groups container. To do so, click the plus sign (+) to the left of the container.

3. Click the administrative group that you want to work with, and then expand it.

4. Expand the Routing Groups container.

5. Click the routing group that you want to work with, and then expand it.

6. Click the Connectors container. Right-click the Connectors container, and then click New.

7. Click SMTP Connector.

8. On the General tab, provide an appropriate identifying name for the connector.

9. Choose to use DNS or forward to a smart host (if you are relaying through an Internet service provider send-mail server). If you are forwarding to a smart host, use the IP address of the smart host in square brackets.

10. Under Local Bridgeheads, click Add. Add the server that becomes the bridgehead server for the routing group. Designate an SMTP virtual server as a bridgehead server for the SMTP connector. This can be either the server that you are working on or another server in the same routing group. Alternatively, this duty can be shared by multiple servers.

11. Click the Address Space tab. Under Connector Scope, click either Entire Organization or Routing Group. As in earlier versions of Exchange Server, when you configure the Internet Mail Service, click Add, click SMTP, and then click OK. Accept the default (*) unless you require outbound e-mail domain restriction, and leave the cost

as 1. If you have accepted the default of (*), you should never click to select the Allow messages to be relayed to these domains check box. Clicking to select the Allow messages to be relayed to these domains check box would open your server for relay to the world. The Allow messages to be relayed to these domains check box should be for secure domain to domain connections only.

12. If you have chosen forward all mail to a smart host, click the Advanced tab. Click the Outbound Security option, and then select an appropriate authentication method for your relay host. The default is Anonymous Access. Anonymous is the method that must be used if you are forwarding to an ISP, unless you have made prior arrangements with the ISP for another security level. If you are forwarding to your own server or to another server outside your environment, work with the administrator of that server to select the appropriate security level for both servers. You can add more than one smart host in this box by using the following format: [IP];[IP];[IP];[IP]

13. Click OK to exit Outbound Security.

14. Click OK to exit the Advanced tab.

15. Click OK to exit the SMTP connector.

16. You must restart the Microsoft Exchange Routing Engine service and the SMTP service for these changes to take effect.

QUESTION 53

You need to configure the messaging environment to route e-mail messages from users at the Baldwin Museum of Science to users at Litware, Inc.

What should you do?

A. On DNS1, configure mail exchanger (MX) resource records for the Exchange servers in the litwareinc.com domain.

B. On DNS1, configure host (A) resource records for the designated bridgehead server at the Litware, Inc., office.

C. Configure a bridgehead server in the Toronto office to route e-mail messages to the litwareinc.com domain by using a smart host.

D. Configure a bridgehead server at the Litware, Inc., office to route e-mail messages to the baldwinmuseumofscience.com domain by using a smart host.

E. Install and configure a DNS server at the Litware, Inc., office by using the appropriate mail exchanger (MX) resource records for Exchange servers that host the litwareinc.com domain.

Answer: C

Explanation

The Technical Requirements tell us that : "4. Remote bridgehead servers will be installed in the Amsterdam and Toronto offices to route e-mail messages between the two Exchange organizations over the Internet. AND 5. You need to ensure that all e-mail messages from Baldwin Museum of Science users in Canada to Litware, Inc., users are routed through the bridgehead server for Litware, Inc."

Although the Routing Group connector is the preferred connector to connect routing groups in a single Exchange Server organization, it cannot be used to connect routing groups in separate Exchange Server organizations. To connect separate Exchange Server

organizations you must use either the SMTP connector or the X.400 connector depending on your company's messaging requirements.

To connect two independent Exchange Server organizations instead of routing groups within the same organization, you must know the server in the remote organization that e-mail will be forwarded to, the secondary proxy address of recipients in the remote organization to configure address space on the connector, and any additional options that your company will require for communication between the organizations.

To configure an SMTP connector, you must:

1. Create a new SMTP connector.
2. Configure the Internet Protocol (IP) address of a server in the remote Exchange Server organization as the smart host for that connector.
3. Define an address space with the e-mail domain of the remote Exchange Server organization.
4. Configure other options such as outbound security or delivery restrictions that may be a requirement for your company.

To configure an X.400 connector, you must:

1. Create a new X.400 connector.
2. Configure the name of a server in the remote Exchange Server organization that you are connecting to and the password that will be used for the connector.
3. Configure the remote server name or IP address of the remote server.
4. Define an address space with the e-mail domain of the remote Exchange Server organization.
5. Configure other options such as delivery restrictions that may be a requirement for your company.

So we must create an SMTP connector on the bridgehead server in the toronto office. On this SMTP connector we configure the remote bridgehead server at Litware Inc. as a smarthost.

QUESTION 54

You need to deploy new e-mail clients to users at Litware, Inc. Which e-mail client or clients should you use for each type of users?

To answer, drag the appropriate e-mail client type or types to the correct location or locations in the answer area.

E-mail Client Types	Answer Area
Outlook 2003	Senior staff members Drag e-mail client type here
Outlook Web Access	Drag e-mail client type here
POP3 client	
	Administrative assistants Drag e-mail client type here
	Drag e-mail client type here
	Field researches Drag e-mail client type here
	Drag e-mail client type here

Answer:

Explanation:

E-mail Client Types	Answer Area
Outlook 2003	Senior staff members Outlook 2003 Drag e-mail client type here
Outlook Web Access	Administrative assistants Drag e-mail client type here
POP3 client	Outlook 2003
	Field researches Outlook Web Access Drag e-mail client type here

From the Technical Requirements we know that : "1. You need to ensure that Field Researchers at Litware, Inc., have the minimum possible effect on network traffic when accessing their mailboxes from remote locations." and from the Business Requirements we know that : "5. Administrative assistants for Litware, Inc., must be able to send messages and respond to messages from research staff on behalf of senior staff members." Outlook Web Access cannot does not support send on behalf email sending, therefore we must configure Outlook 2003 for all Senior staff members and Administrative assistants.

The Files researchers will use Outlook Web Access to reduce traffic from remote locations to the main office.

Topic 11, Southridge Video, Scenario

BACKGROUND

1. Overview

Southridge Video is one of the fastest growing retailers of moves in videocassette and DVD in the southern United States. The company offers moves for sale and rental. The retail outlets are open seven days per week from 10:00 A.M. through 10:00 P.M.

1. Physical Locations

The company's main office is in Dallas. The company also has 10 branch offices that operate as distribution centers to 100 retail outlets across the southern United States. There are 3,000 users at the main office, 600 users at each branch office, and between 90 and 100 users at each retail outlet.

1. Planned Changes

The company plans to upgrade from Exchange 2000 Server to Exchange Server 2003 within the next three months. Microsoft Outlook 2003 will be deployed to all client computers as part of this project.

PROBLEM STATEMENTS

1. A previous migration from Exchange Server 5.5 to Exchange 2000 Server resulted in the existing administrative group structure that makes administration difficult.
2. A recent estimate is that almost 50 percent of e-mail messages received by users at the company are unsolicited commercial e-mail messages. The amount of unsolicited commercial e-mail messages received by users is growing.

EXISTING MESSAGING ENVIRONMENT

1. Administrative Structure

1. There are currently 111 administrative groups, with one group for each physical location.
2. The administrative group at the main office is named MO Admins. This group is responsible for all servers and users located in the main office.
3. All main office servers have a mailbox storage policy to limit users' mailboxes to 50 megabytes. Some users have an exemption to this limitation.
4. The administrative group at each branch office is named Branchname Admins.
5. Each Branchname Admins group is responsible for all servers and users located in the branch office and its associated retail outlets. No branch office or retail outlet servers have mailbox storage policies in place.
6. Group membership and permissions are shown in the following table.

Group	Exchange 2000 Server Permissions	Active Directory Permissions	Member Of
MO Admins	Full administrative rights to all Exchange servers in the main office and branch offices	Full Control	Local Administrators Group of all Exchange servers
Branchname Admins	Full administrative rights to branch office Exchange servers and associated retail outlet servers	Full Control	Local Administrators Group of all Exchange servers

1. Messaging Infrastructure

1. Southridge Video currently uses Exchange 2000 Server. An in-place upgrade was

performed from Exchange Server 5.5 two years ago.

2. The network includes 11 Internet SMTP connectors.
3. At the main office, there are separate mailbox stores created for each department.
4. Each branch office Exchange server has a single mailbox store.
5. Two Exchange 2000 servers at the main office contain all 200 MB of the public folders.
6. Public folders are widely used throughout the environment.
7. Tape backups are performed locally on each Exchange server. A full backup is performed every Sunday, and a daily incremental backup is performed every Monday through Friday

1. E-mail Clients

1. Outlook 2000 and Outlook 2002 are supported.
2. Some users upgraded to Outlook 2003 on their own.
3. Microsoft Outlook Web Access is used by a few users at their homes.
4. Some users use Microsoft Outlook Express. No other e-mail clients are supported.
5. The MAPI, IMAP4, and POP3 protocols are currently enabled.
6. Each user at the main office, branch offices, and retail outlets used Outlook configured with a MAPI connection to access the user's mailbox located on the Exchange 2000 server at the user's location.

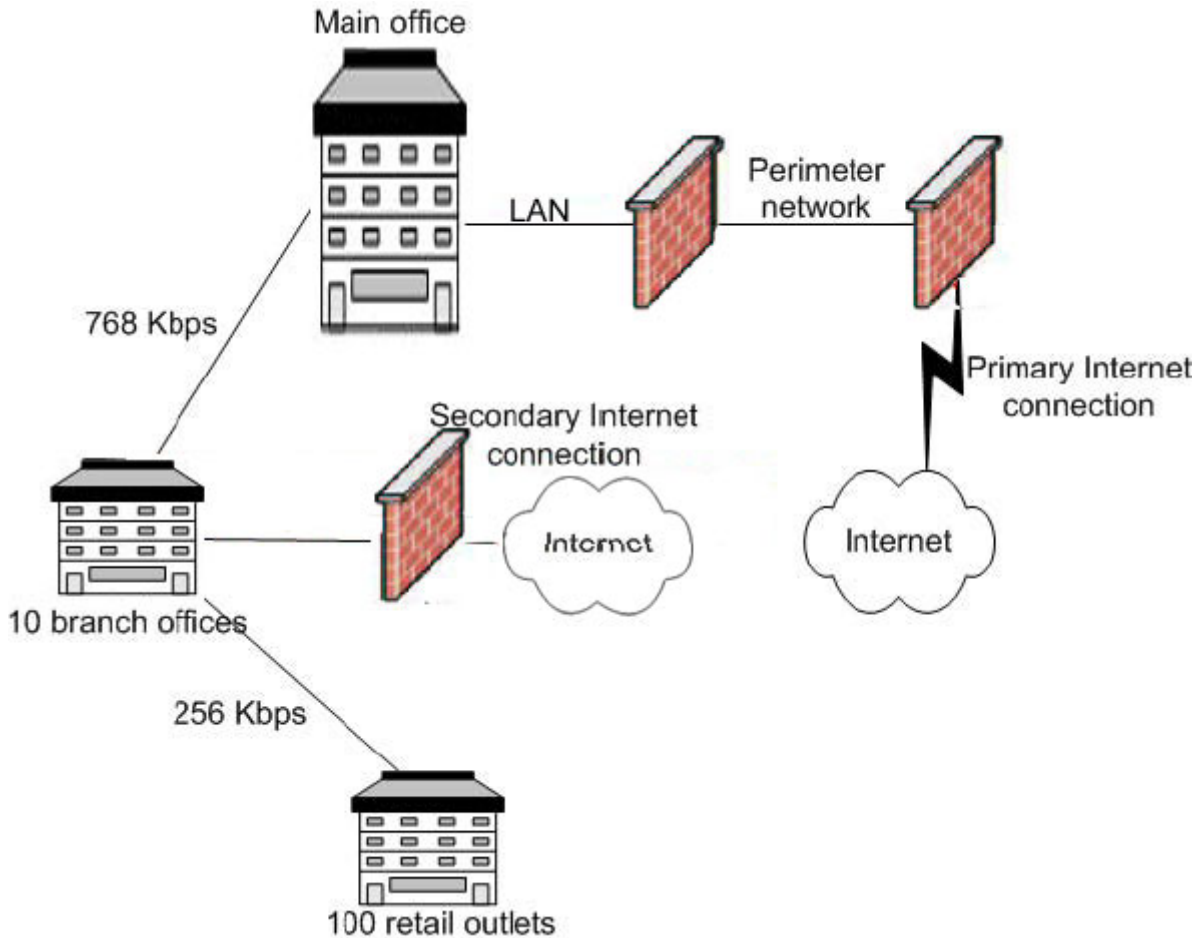
SUPPORTING INFRASTRUCTURE

1. Directory Services

1. Active Directory is deployed in a single-domain forest named southridgevideo.com.
2. All user accounts are located in a single organizational unit (OU) named Company Users.
3. There are 12 global catalog servers, with two at the main office and one at each branch office. There are no additional domain controllers within the environment.

1. Network Infrastructure

1. The network infrastructure is shown in the following diagram.



1. Administration

1. The IT administrative functions are distributed between the main office and the branch office. Each branch office IT group is also responsible for the administration of 10 retail outlets.
2. Currently, all Active Directory user administration is performed by each Exchange administrative group.

BUSINESS REQUIREMENTS

1. Security

1. External access to user mailboxes needs to be allowed only for users who use Outlook Web Access. In addition, access to e-mail messages must be encrypted.
2. Efforts to stop unsolicited commercial e-mail messages must be implemented.
3. An antivirus solution needs to be implemented to protect the network from Internet e-mail messages that are potentially harmful.
4. Files that pose a virus risk need to be blocked.

1. Interviews

Chief Executive Officer:

1. We need to improve our electronic messaging environment.
2. It takes too long for our retail outlets to receive some mailings. This is not acceptable.

3. We have been spending too many IT resources cleaning viruses that have entered our network through our e-mail system.

Chief Information Officer:

1. Our current e-mail infrastructure is based on an in-place upgrade that was performed over two years ago. As we grew, we did not adapt to our current needs. There seem to be too many security risks.

2. We need to minimize the permissions that the Exchange administrators have.

3. Currently, Exchange administrators can create a user account with a mailbox on any Exchange 2000 server. This needs to be restricted to allowing administrators to create mailboxes on only the servers they support and manage.

4. We need to be able to recover a single mailbox without effecting other user's mailboxes.

Messaging Expert:

1. I notice that almost every marketing person in the main office has an exemption to the mailbox storage limits. Rather than having exemptions, we need to manage mailbox storage limits by using policies.

End Users:

1. I work in a retail outlet. Sometimes when I send an e-mail message, it seems to take a long time to send, especially if I am sending it to a distribution group.

2. Also. Sometimes when I click a public folder, I receive a pop-up message that tells me that my computer is trying to connect to the server and that I have to wait.

TECHNICAL REQUIREMENTS

1. Messaging Infrastructure

1. You need to ensure that a single mailbox can be recovered without adding additional hardware.

2. Each new Exchange 2003 server will have seven 72-GB hard disks.

1. Supporting Infrastructure

1. You need to ensure that Active Directory supports the current Exchange administrative model. No changes will be made to the network topology

1. E-mail Client Infrastructure

1. The company wants Outlook 2003 to be used as the e-mail client for users who are connected to the LAN.

2. The company wants Outlook Web Access to be used as the e-mail client on computers that are not members of the southridgevideo.com domain.

3. All network segments must allow HTTPS, MAPI, and IMAP4. POP3 will no longer be allowed.

4. Microsoft Internet Explorer 5.0 and later is the only supported Web browser.

Topic 11, Southridge Video (6 Questions)

QUESTION 55

You need to design a mailbox store policy for all mailboxes.

What should you do?

A. Create and apply one mailbox store policy for users in all offices.

B. Create and apply one mailbox store policy for the users at the main office.

- Create and apply a second mailbox store policy for the users at all the branch offices.
- C. Create and apply one mailbox policy for all users who are not in the marketing department. Create and apply a second mailbox store policy for the users at all the branch offices.
- D. Create and apply one mailbox store policy for the users in the marketing department. Create and apply a second mailbox store policy for users in all other departments.

Answer: D

Explanation

Storage limits can be configured for individual mailboxes or can be set in the properties of a mailbox store or by using a mailbox store policy. By default, mailboxes inherit their storage limits from their corresponding mailbox stores.

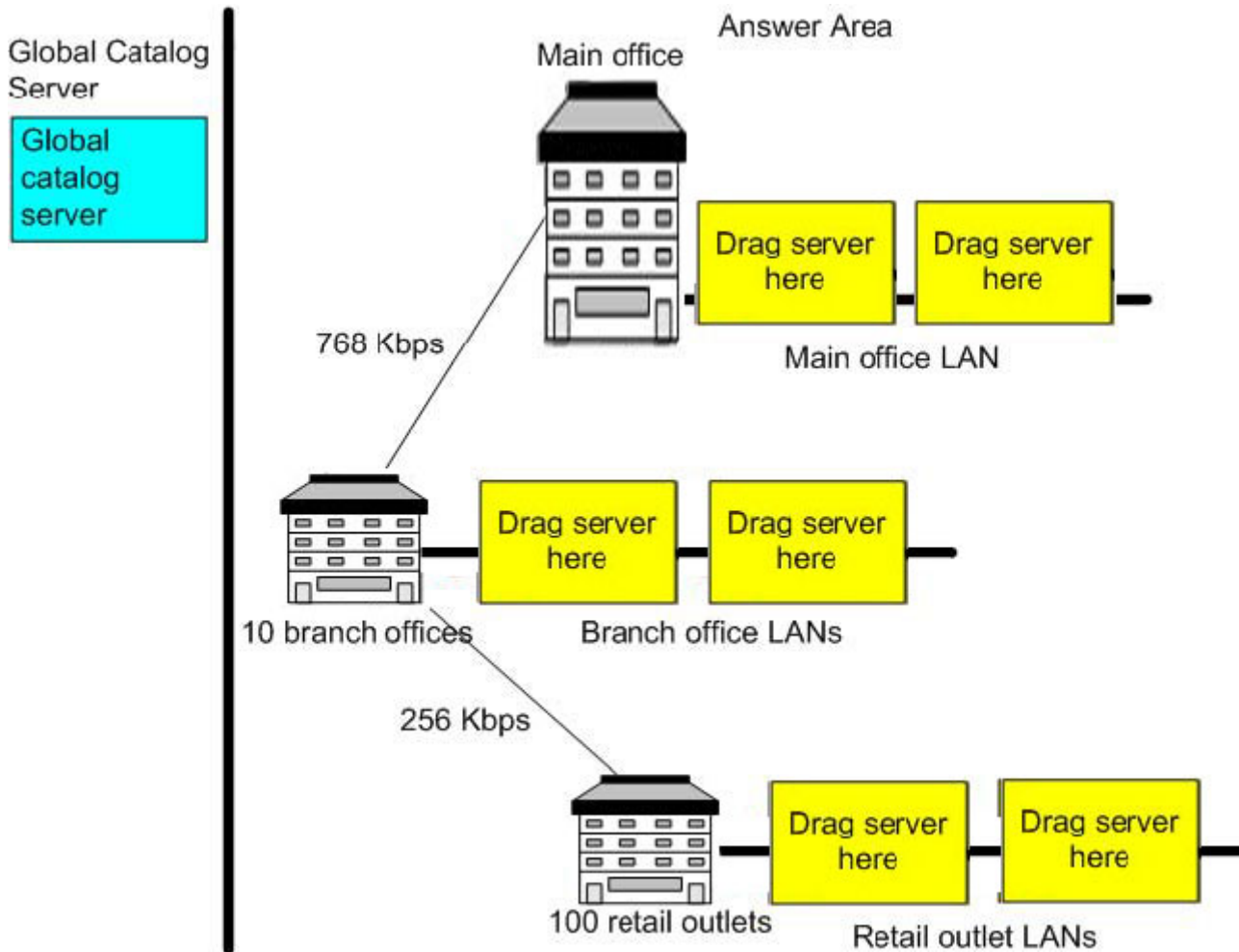
However, you can configure individual mailbox limits to override the limits that you set for the mailbox store. This is useful if you have a specific user or group of users, such as managers, who require larger mailboxes. This is also useful if you want to set a more restrictive storage limit for certain users, such as contract employees.

The messaging expert told us that : "1. I notice that almost every marketing person in the main office has an exemption to the mailbox storage limits. Rather than having exemptions, we need to manage mailbox storage limits by using policies."

Now we know we need to create a separate mailbox policy for the marketing department and one for all other users.

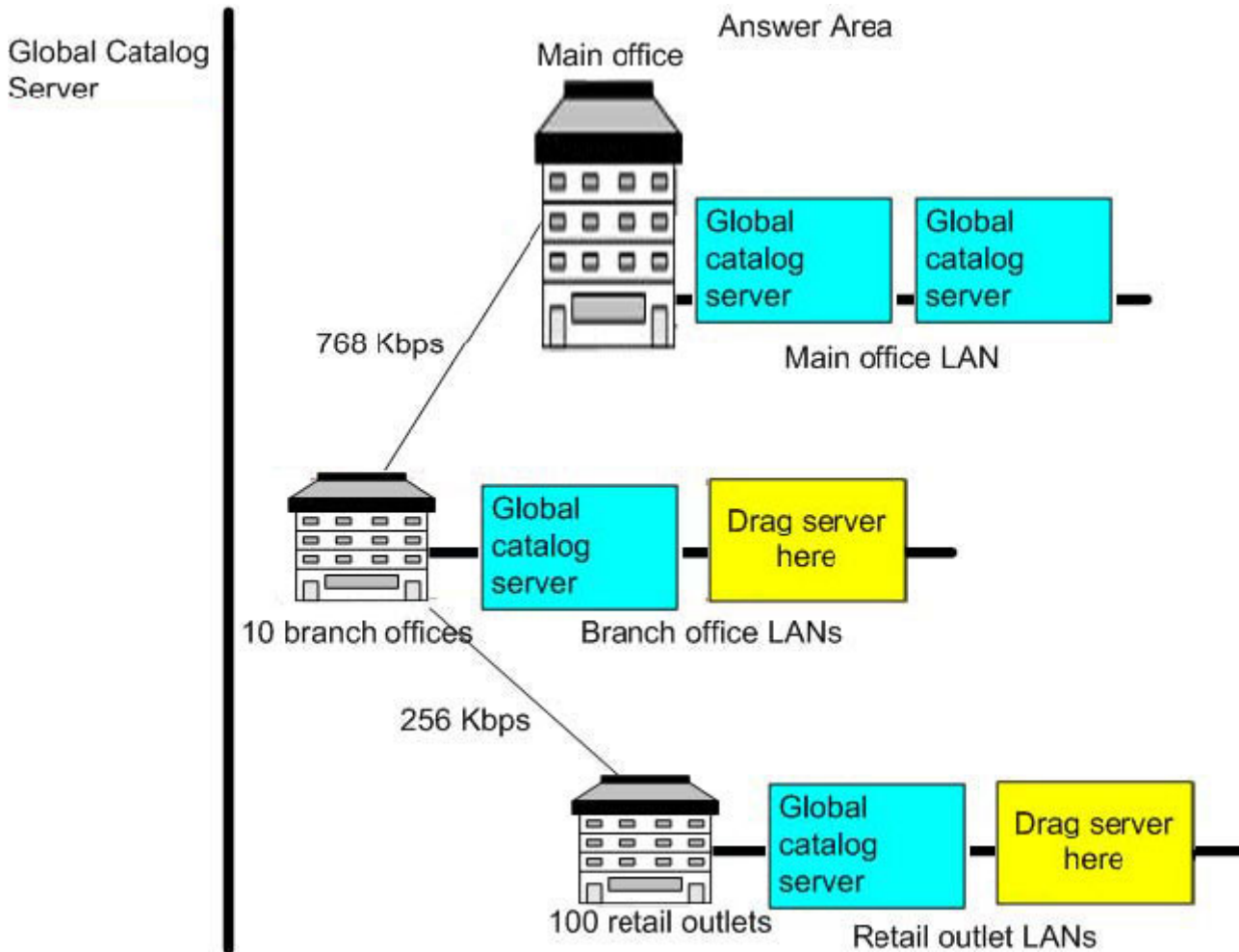
QUESTION 56

You need to design the placement of global catalog servers in the new environment. Where should you place global catalog servers?



Answer:

Explanation:



Exchange Server 2003 must access global catalog servers to obtain complete address information for all recipient objects in the forest. Only global catalog servers contain a complete replica of all objects in the domain and a partial replica of all objects in the forest.

Global catalog servers that an Exchange server currently uses are called working global catalog servers.

A global address list (GAL) is a list that contains all Exchange recipients in the organization. The GAL is retrieved from the global catalog servers in Active Directory and used by Exchange Server clients to address e-mail messages or find information about recipients in the organization. When you first install Exchange Server, a default GAL is created automatically. The GAL is the default address list that users will use in their address book.

The recommended ratio is a 4:1 ratio of Exchange Server processors to global catalog server processors, assuming the processors are similar models and speeds. However, depending on your situation, higher global catalog server usage, a large Active Directory, or large distribution lists can necessitate more global catalog servers.

The end-users told us that : "1. I work in a retail outlet. Sometimes when I send an e-mail message, it seems to take a long time to send, especially if I am sending it to a distribution group. and 2. Also. Sometimes when I click a public folder, I receive a pop-up message that tells me that my computer is trying to connect to the server and that

I have to wait."

This is due to misplacement of Global Catalog Servers. We can speed this up by placing a GC in the retail offices.

(Nonetheless this increases replication traffic). The Main Offices already had 2 GC's and the Branch Offices already had 1 GC. There were no complaints by using that setup, so no changes are necessary there.

QUESTION 57

You need to reduce the number of unsolicited commercial e-mail messages that are received.

What should you do?

- A. Require Basic authentication on all SMTP virtual servers.
- B. Require Integrated Windows authentication on all SMTP virtual servers.
- C. Create a block list of IP addresses and apply the block list to each SMTP virtual server.
- D. Subscribe to a real-time list service and use the appropriate Block List Service Configuration Settings.

Answer: D

Explanation

E-mail is an essential service for nearly all organizations. Therefore, it is crucial that administrators provide their users with secure and reliable e-mail services. A malicious attack on the messaging system, in the form of a virus, worm, or denial of service, is a prominent area of risk in daily Exchange 2003 operations. Similarly, unsolicited commercial e-mail (spam) has become intrusive and sophisticated enough to be considered a threat to e-mail operations.

Exchange Server 2003 includes a number of security features that can be used to reduce the amount of unwanted e-mail, including:

- * Support for Realtime Block Lists (RBLs). Allows Exchange Server to subscribe to Internet listing services identifying servers that are sources of spam on the Internet. Exchange Server blocks all messages from servers that are listed by the RBL provider.
- * Intelligent Message Filtering (IMF). IMF is used by Exchange Server 2003 to perform server-side and client-side junk e-mail filtering by using Microsoft SmartScreen technology. Filtered messages can be archived so that they can be viewed by Exchange administrators or sent to the Outlook client's Junk E-Mail folder. IMF can be installed as a separate installation on Exchange servers that are not running SP2. IMF is installed by default when Service Pack 2 is installed.
- * Restricted relaying and submission. Allows administrators to restrict message relaying and message submission to a list of security principals, thereby protecting your organization against address spoofing.
- * Secure Web Client connection using Secure Sockets Layer (SSL). Exchange Server administrators can enforce certificate authentication for clients connecting to their mailboxes by using Outlook Web Access. Hypertext Transfer Protocol Secure (HTTPS) can also be used to secure connections from mobile clients such as mobile phones or

wireless Microsoft
ActiveSync(r) clients.

* Support for Sender ID. Exchange Server 2003 SP2 supports Sender ID as an additional layer of message filtering. Sender ID verifies that every e-mail message originates from the Internet domain from which it claims to have been sent. This is accomplished by checking the address of the server sending the mail against a registered list of servers that the domain owner has authorized to send e-mail.

QUESTION 58

You need to design a plan for recovering mailboxes.
What should you do?

- A. Configure a recovery storage group on each Exchange 2003 server.
- B. Configure a new empty storage group on each Exchange 2003 server.
- C. Configure a recovery storage group on one Exchange 2003 server at the main office.
- D. Install Exchange Server 2003 on a separate server at each location. Configure these servers to perform mailbox recoveries.
- E. Install Exchange Server 2003 on a separate server at the main office. Configure this server to perform mailbox recoveries.

Answer: A

Explanation

The Chief Information Officer told us : "4. We need to be able to recover a single mailbox without effecting other user's mailboxes." and the Technical Requirements tell us that : "1. You need to ensure that a single mailbox can be recovered without adding additional hardware."

The Recovery Storage Group (RSG) is a new type of storage group in Exchange 2003 that essentially allows you to mount a copy of a mailbox store onto a production Exchange 2003 server. You can then recover data within the restored mailbox store whilst the current store is still running. Use of the RSG on a production server won't interfere with the users as the RSG is logically isolated; users cannot log into it, and mail cannot be delivered to it. As you can probably guess, the main benefit here is that you don't necessarily need a spare disaster recovery server in its own Active Directory forest to recover a single mailbox or single mailbox store, as was required in Exchange 2000. Therefore we need to configure a recovery storage group on each Exchange 2003 server.

QUESTION 59

You need to protect the messaging environment from potentially harmful attachments to e-mail messages.
What should you do?

- A. Configure block list in the global settings for the Exchange organization.
- B. Configure a receipt filter in the global settings for *@southridgevideo.com.
- C. Configure Outlook 2003 so that it does not allow users to access potentially harmful file types.
- D. Configure Outlook 2003 rules to move all potentially harmful attachments to a

quarantine folder.

Answer: C

Explanation

The Microsoft Outlook 2003 e-mail security features provide additional levels of protection against malicious e-mail messages. The security features included with Outlook 2003 can be divided into the following three distinct parts:

- * Blocking of potentially unsafe attachments.
- * Confirmation of programmatic access to e-mail addresses.
- * Confirmation of automatic sending of e-mail messages.

If you use Outlook in a Microsoft Exchange environment, you can configure the server to block certain attachment file name extensions by using the Outlook E-mail Security Administrator Package.

After you configure the security features on Exchange Server, you must enable the customized settings for your users. To enable the changed settings, you may need to deploy a new registry key to the client computers, depending upon whether or not Microsoft Office was initially deployed with system policies.

Incorrect Answers :

A. A block list will block IP Addresses or domain names. It will not block certain attachment types.

B. You cannot configure attachment blocking in receipt filters.

D. You cannot configure attachment blocking by using a rule in outlook 2003.

Reference:

<http://support.microsoft.com/kb/290499/en-us>

<http://support.microsoft.com/kb/837388/en-us>

<http://office.microsoft.com/en-gb/assistance/HA011364471033.aspx>

QUESTION 60

You need to design a security strategy for Outlook Web Access. Which three actions should you perform? (Each correct answer presents part of the solution. Choose three)

- A. Install an SSL client certificate.
- B. Install an SSL server certificate.
- C. Require only Basic authentication.
- D. Require SSL for access to each Outlook Web Access server that is accessible from the Internet.
- E. Allow only Integrated Windows authentication.
- F. Allow SSL connections for access to each Outlook Web Access server that is accessible from the Internet.

Answer: B, C, D

Explanation

OWA enables users to access their Exchange Server 2003 mailbox by using a Web browser such as Microsoft Internet Explorer. OWA can also provide access to mailbox

data from UNIX, Macintosh, and Microsoft Windows(r)-based computers without the installation of any messaging client. These users can view and work with any public folder, mailbox, global address list, or calendar from the Web interface.

By default, OWA is configured to use HTTP. This means that all user logon information is passed in clear text to the computer running Exchange Server 2003. This issue can be easily addressed by using SSL to encrypt all user sessions. However, some clients may cache the user logon credentials so that if the user does not close all Web browser sessions,

another user may be able to access the user's e-mail without logging on. This security concern is addressed by reducing the timeout for cached credentials with forms-based authentication.

The steps for securing OWA communications by using SSL are as follows:

1. Install a Web Server certificate on an Exchange server.
2. Enable SSL listening ports on the Exchange server.
3. Configure SSL in the e-mail applications.

A number of authentication methods are available for Outlook Web Access. You must select an authentication method depending on the capabilities of the client operating system and the specific security policies. You can enable or disable these authentication methods by using the IIS Manager and modifying the properties of the virtual directories that are used by OW

A. Anonymous access is disabled by default on the Exchange Server virtual directories that provide access to mailbox or public folder contents. You can enable anonymous access to provide limited access for specific public folders and directory information. Anonymous authentication is supported by all clients, and it is an easy way to allow access to unsecured content in public folders. Basic authentication uses clear text to perform a simple challenge and response authentication. Basic authentication requires users to specify their user name, domain, and password to gain access to mailbox data. If you are going to enable basic authentication to provide access to OWA, you must implement SSL to encrypt the user name and password. Integrated Windows authentication provides the highest level of security for clients running Internet Explorer 5.0 or later because it uses Kerberos protocol version 5 to authenticate users. If you deploy OWA in a front-end and back-end server topology, only anonymous and basic authentication are supported on the front-end server. You cannot use Integrated Windows authentication. The only option for securing authentication traffic between the OWA client and the front-end server is to deploy SSL.

Topic 12, The School of Fine Art, Scenario

BACKGROUND

1. Overview

The School of Fine Art is a creative learning school that specializes in modern art. Primary hours of operation are 8:00 A.M. to 5 P.M. Users include faculty members, students, and employees. All users must be able to access their e-mail messages at all hours

1. Physical Locations

The school's main office is in Chicago. There are 150 campuses located throughout the United States.

The main office includes 2,500 users. Each campus has approximately 30 faculty members who are network users.

1. Planned Changes

Users must be able to retrieve their e-mail messages from any supported device that is connected to the Internet. Both wired and wireless connectivity must be supported.

PROBLEM STATEMENTS

Users cannot currently access their e-mail messages remotely by using Microsoft Outlook.

EXISTING MESSAGING ENVIRONMENT

1. Administrative Structure

1. There is one Exchange 2000 Server administrative group for the Exchange servers in the main office. There are 150 additional Exchange 2000 Server administrative groups, with one group for each campus. These groups were created when the company upgraded from Exchange Server 5.5.

2. All Information Technology (IT) administrative roles are centralized in the main office.

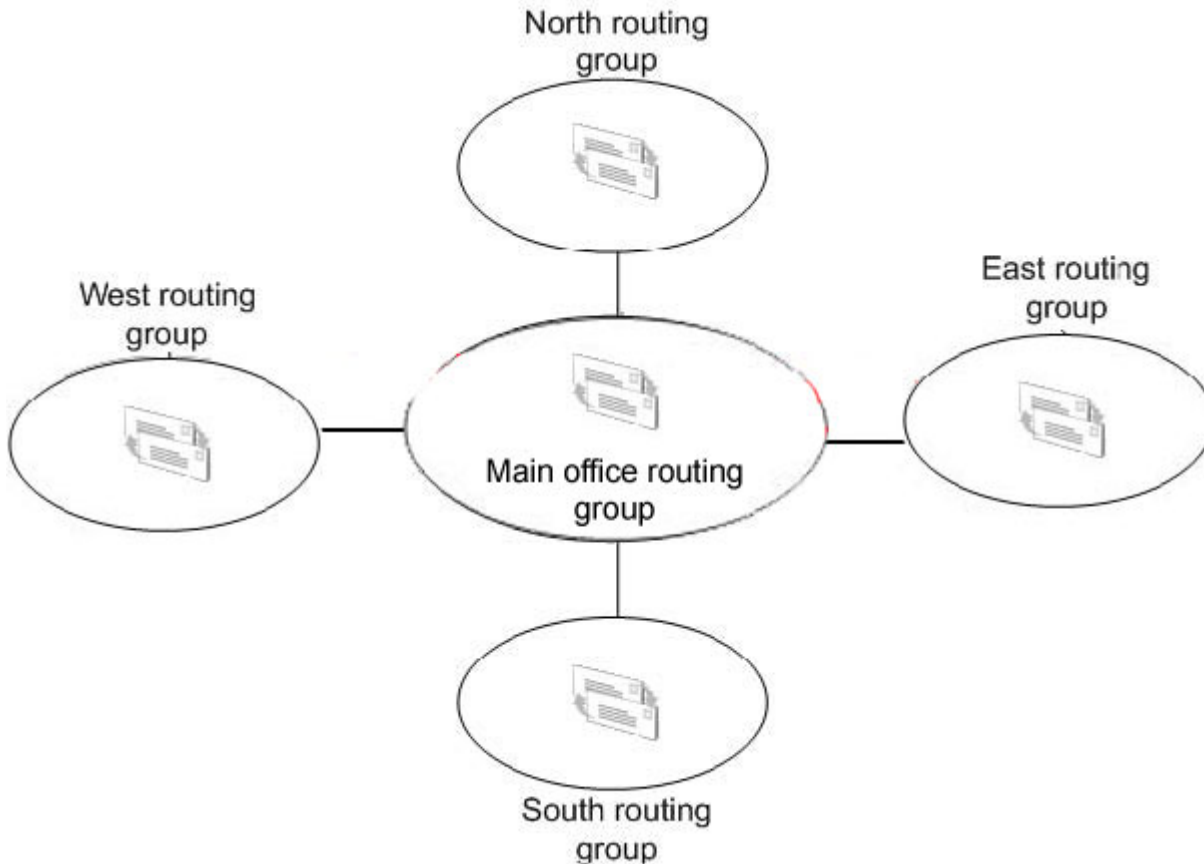
3. The campus office are administered by a team named Campus Admin, which is also located in the main office. The Campus Admin team has Exchange Full Administrator permission for the 150 Campus administrative groups.

4. The main office servers are administered by a team named Main Office Admin. The Main Office Admin team has Exchange Full Administrator permission for all administrative groups.

1. Messaging Infrastructure

1. Currently, the School of Fine Art is using Exchange 2000 Server as its messaging platform. The Exchange servers are grouped into five main routing groups. The main office routing group contains all of the servers in the main office. The servers for the 150 campus locations are in routing groups based on regions of the country.

2. The routing group topology is shown in the following diagram.



3. All campus Exchange servers have a single mailbox store for all users in that campus location.

4. The Exchange servers at the main office have two mailbox stores that have the users divided equally based on the first letter of their last name. Both stores are in a single storage group.

5. Exchange servers at all campus locations are backed up daily by performing a local backup. A centralized network backup tool is used for the Exchange servers at the main office. The current backup solution can back up and restore at a rate of 14 GB per hour.

6. There is one public folder server that is widely used.

1. E-mail Clients

1. Users access their e-mail messages by using Outlook 2000 and Microsoft Outlook Web Access.

2. E-mail clients access Outlook Web Access by using SSL from the Internet and while using the company network.

3. Outlook Web Access is deployed on the front-end servers located in the perimeter network.

4. There are no mailbox size limits.

SUPPORTING INFRASTRUCTURE

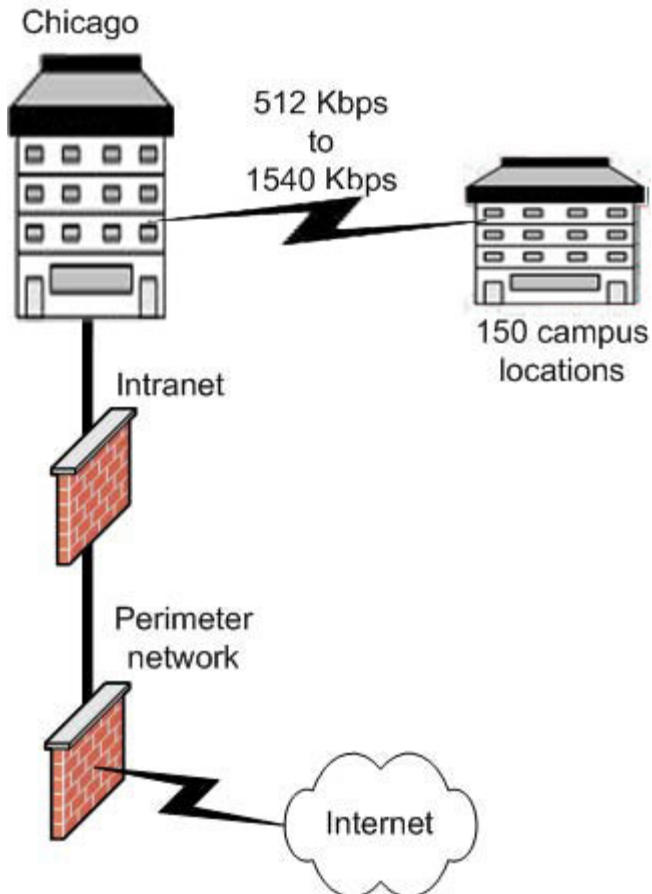
1. Directory Services

1. Active Directory is deployed in a single domain named corp.fineartschool.net.

2. Each campus office is considered a single site and has a site connector back into the main office site.

1. Network Infrastructure

1. Each campus office is connected directly to the main office. Connection speeds vary from 512 Kbps to 1540 Kbps. All LAN connections are 100 Mbps.
2. Each campus office has a single multifunction server that is the Exchange 2000 server and a global catalog server.
3. The relevant portion of the network is shown in the following diagram.



BUSINESS REQUIREMENTS

1. Business Factors

1. The company requires end users to be able to access to their e-mail messages from any supported device.
2. Sales personnel need to be able to read and send e-mail messages and schedule meetings while they are offline. The company wants e-mail messages and meeting requests to be sent automatically when the sales personnel connect to the Exchange servers from remote locations.

1. Security

1. The Exchange environment includes mailboxes for only faculty members and no other users. The company requires security measures to be put into place to protect the messaging environment from external and internal users.
2. There are currently no message attachments being blocked. The company wants attachment types that can invoke a virus attack to be blocked at the SMTP gateway level.
3. The company wants viruses to be stopped before they reach the Exchange

environment.

4. All mailbox data that a user accesses from the Internet must be encrypted to ensure security.

1. Interview

Chief Information Officer:

1. We plan to implement new service level agreements that will require us to restore mailboxes within one hour of a request.
2. We currently cannot do this in regard to availability and recovery.
3. We need to make our internal network more secure by limiting the traffic into our internal network to secure Web traffic and SMTP traffic only.
4. We need to limit the cost of hardware and software while still achieving our technical goals.
5. We need to be able to apply service packs and security updates without affecting users' access to their mailboxes.

Messaging Expert:

1. We need to move all mail functions and servers into the main office data centers.
2. We must have redundant servers for all messaging functions.
3. We must design a solution that has the most flexibility for future growth without having to redesign mailbox servers.
4. We must also have dedicated servers for each mail function.
5. We also cannot afford to lose a single e-mail item if a database becomes corrupt.

Messaging Administrator:

1. The administrative model must be streamlined. Our current administrative group structure at times makes it difficult to find a server quickly.

TECHNICAL REQUIREMENTS

1. Messaging Infrastructure

1. Service-level agreements require mailboxes to be restored within one hour.
2. Users must be able to send and receive e-mail messages in the event of a single mailbox server failure.

1. Supporting Infrastructure

1. No changes are planned for the network topology.
2. As a part of the migration, the functional level of the Active Directory forest will be upgraded to Windows Server 2003.

1. E-mail Client Infrastructure

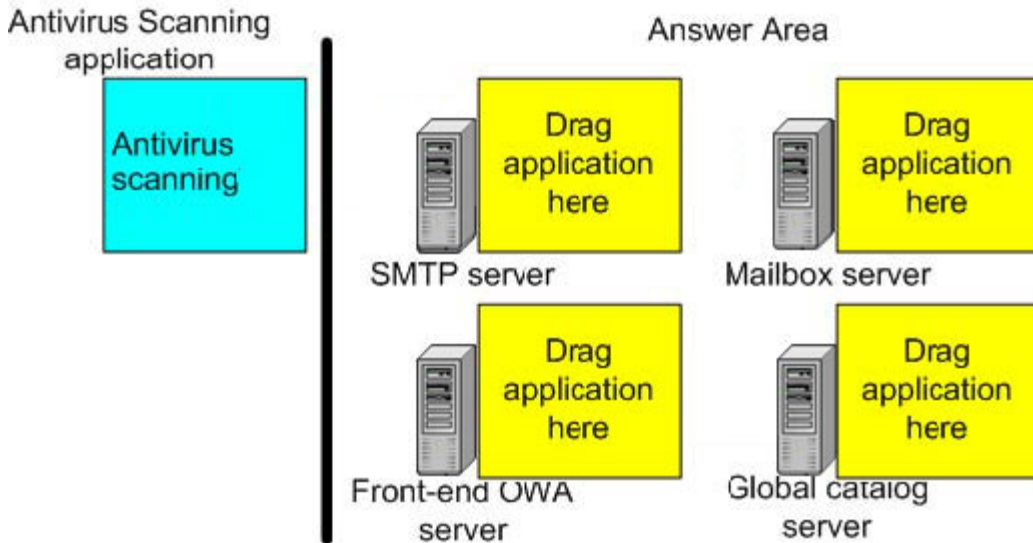
1. Outlook 2003 will be deployed to all client computers.
2. Outlook Web Access 2003 and Outlook Mobile Access will also be deployed.
3. Microsoft Outlook Express will not be a supported e-mail client.

Topic 12, The School of Fine Art (4 Questions)

QUESTION 61

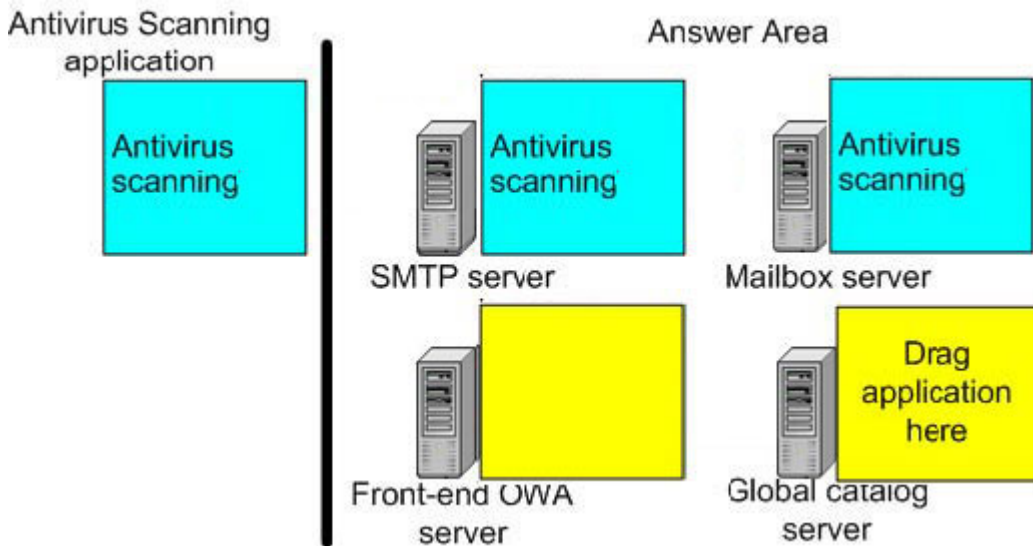
You need to design an antivirus solution for scanning e-mail messages- On which server or servers should you install an antivirus scanning application?

To answer, drag the antivirus scanning application to the appropriate server or servers in the answer area.



Answer:

Explanation:



To prevent viruses from spreading to users who are not using the current client-side antivirus software, you should install server-side antivirus software on every Exchange server that is in your company that has mailboxes installed. Server-side antivirus software scans mailbox and public folder stores for viruses (some server-side antivirus software can also scan transports) and removes viruses before they enter your network. Some server-side antivirus software products also search for a sudden increase in the amount of e-mail, such as the same message being sent from multiple accounts. The security requirements stated that we should protect the messaging environment from external and internal users, and that viruses should be blocked at SMTP gateway level. Therefore we need to enable antivirus software on the SMTP server and the mailbox servers.

Reference:

Overview of Exchange Server 2003 and Antivirus Software
(<http://support.microsoft.com/kb/823166>)

QUESTION 62

You need to design a fault tolerant Exchange Server 2003 solution for the main office users. What should you do?

- A. Design an active/active cluster that includes two back-end mailbox servers.
- B. Design an active/passive cluster that includes two back-end mailbox servers.
- C. Design a Network Load Balancing solution consisting of two front-end servers per load-balanced server group.
- D. Design front-end and back-end Exchange servers for mailbox access by using two front-end servers for each back-end mailbox server.

Answer: B

Explanation

Regarding to the interviews and requirements we know :

1. Interview with CIO Requirement 5 : " We need to be able to apply service packs and security updates without affecting users' access to their mailboxes."
2. Interview with the Messaging Expert point 2: "We must have redundant servers for all messaging functions."
3. Interview with the Messaging Expert point 4: "We must also have dedicated servers for each mail function."
4. Messaging Infrastructure Technical requirements point 2 : " Users must be able to send and receive e-mail messages in the event of a single mailbox server failure."

Therefore we need to design a redundant solution for The School of Fine Art.

A cluster hosts one or more virtual servers. Each virtual server has the same kind of resources you would expect to find in a regular server-such as a network name and an IP address-and drives and application services and so forth.

The servers that run the cluster service are called nodes. Each node hosts a virtual server and its resources.

In a two-node cluster, if you create a single Exchange virtual server and assign it to one of the nodes, the other node does nothing until the first node fails. This is an active/passive cluster.

If you create two or more Exchange virtual servers and host one on each of the nodes, then you have an active/active cluster.

In an active/active cluster, if one of the underlying servers goes down-a node failure-the virtual Exchange server hosted by that node rolls over to the good node. Now that node hosts two virtual Exchange servers. This is certainly supported, but it presents a challenge to the Exchange designers.

Microsoft did extensive improvements in the memory handling of both Windows Server 2003 and Exchange Server 2003 to improve cluster operations, but it's still possible to make too many demands on system memory to get a clean failover. In Exchange 2000, Microsoft recommended a maximum of 1900 concurrent connections when using active/active clustering, and it has not revised that number upward for Exchange 2003. In fact, its emphatic recommendation, is to avoid active/active clustering completely.

Incorrect Answers:

A. Microsoft always recommends to use an active/passive cluster solution, not an active/active cluster solution.

C,D. The question states that we need to design a fault tolerant solution for the main office users, not the remote users. The main office users are using outlook 2003 clients, not OWA.

QUESTION 63

You need to design an administrative group model that supports the IT administrative model. Which two actions should you perform? (Each correct answer presents part of the solution. Choose two)

- A. Create one administrative group for each campus location.
- B. Create one administrative group for each of the routing groups.
- C. Create one administrative group for each of the departments at the main office.
- D. Create one administrative group for all servers that store mailboxes for users at the main office.
- E. Create one administrative group for all servers that store mailboxes for users at the campus locations.

Answer: D, E

Explanation

Regarding the administrative structure we know that :

1. There is one Exchange 2000 Server administrative group for the Exchange servers in the main office. There are 150 additional Exchange 2000 Server administrative groups, with one group for each campus. These groups were created when the company upgraded from Exchange Server 5.5.
2. All Information Technology (IT) administrative roles are centralized in the main office.
3. The campus office are administered by a team named Campus Admin, which is also located in the main office. The Campus Admin team has Exchange Full Administrator permission for the 150 Campus administrative groups.
4. The main office servers are administered by a team named Main Office Admin. The Main Office Admin team has Exchange Full Administrator permission for all administrative groups.

Interview with the messaging Administrator :

1. The administrative model must be streamlined. Our current administrative group structure at times makes it difficult to find a server quickly.

Now we know that the existing administrative model is not functioning to well, we need to reduce the workload on the Campus Admins group. We can simplify the administrative model by creating one administrative group for all servers that store mailboxes for users at the main office and by creating one administrative group for all servers that store mailboxes for users at the campus locations.

Incorrect Answers :

A. We already have 150 administrative groups in the existing environment. This conflict with the messaging Administrator : "The administrative model must be streamlined. Our current administrative group structure at times makes it difficult to find a server quickly"
B,C. In the new situation, all servers that have mailboxes are located in the main office. We also know that the new model should be simplified. It will also be difficult to split up by departments or routing groups.

QUESTION 64

You need to design the public folder infrastructure. Which two solutions should you perform? (Each correct answer presents part of the solution. Choose two)

- A. Create one dedicated folder server.
- B. Create two dedicated public folder servers.
- C. Create five dedicated public folder servers.
- D. Replicate each public folder to all dedicated public folder servers.
- E. Replicate only the free and busy information to each public folder server.
- F. Replicate only the free and busy information to all Exchange 2003 servers.

Answer: B, D

Explanation

According to the testcase :

1. The Existing Messaging Infrastructure : "There is one public folder server that is widely used."
2. Interview with the Messaging Expert point 2 : "We must have redundant servers for all messaging functions."
3. Interview with the Messaging Expert point 4 : "We must also have dedicated servers for each mail function."

Now we know that we need at least two dedicated servers that will provide the public folders.

Public folder replication is an e-mail-based process for copying public folders from one Exchange Server to another. Replication messages are sent by using the same protocols and connectors as any other e-mail message that is sent on your network. We also need to setup replication for a solid redundant public folder infrastructure.