QUESTION 1

You are the Exchange administrator for Certkiller .

The network consists of a single Active Directory forest.

The forest root domain is named domain.root.

The domain structure is shown in the work area.

You plan to implement Exchange Server 2003 as the companywide messaging system.

Exchange servers must be deployed only in the Certkiller .com and beijing. Certkiller .com domains.

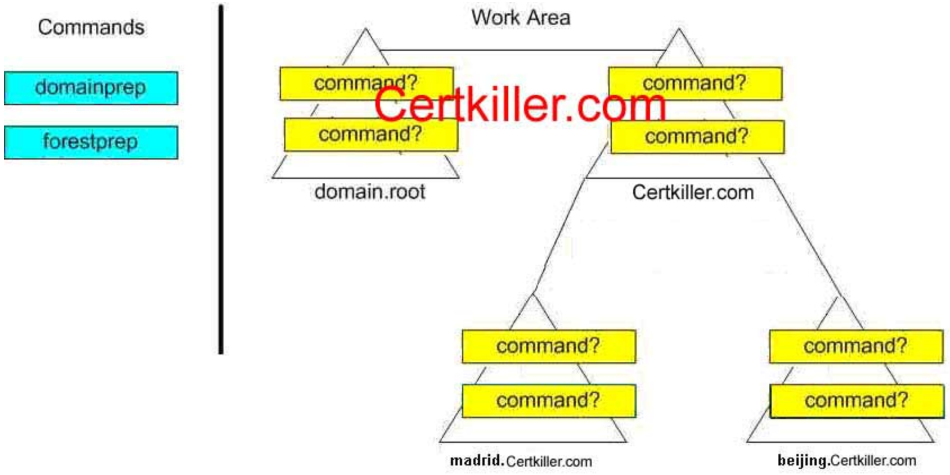
Each domain in the Certkiller .com tree must contain mailbox-enabled users and mail-enabled groups.

You need to run the appropriate command or commands to ensure that the Active Directory infrastructure is prepared to support this implementation.

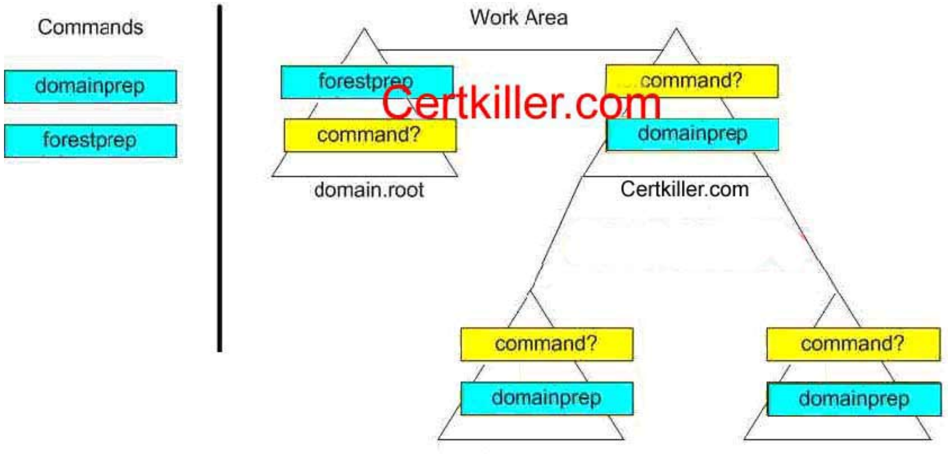
Your solution must require the minimum amount of administrative effort.

Which setup command or commands should you run, and in which domains?

To answer, drag the appropriate setup command or commands to the correct domain or domains in the work area.

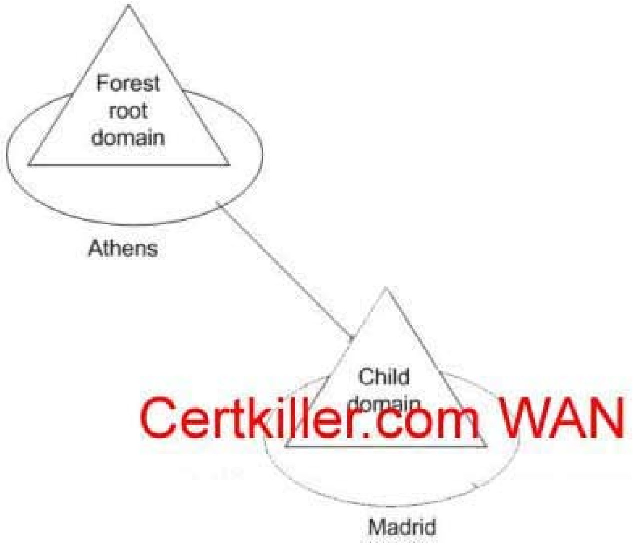


Answer:



Explanation:
The network consists of a single Active Directory forest.
You plan to implement Exchange Server 2003 as the companywide messaging system. They are telling you that they are going to deploy Exchange servers in the Certkiller .com and beijing. Certkiller .com domains but they also tell you that Each domain in the Certkiller .com tree must contain mailbox-enabled users and mailenabled groups.
Each domain in the Certkiller .com tree must contain mailbox-enabled users and mail-enabled groups.
In this case, it does not matter how many child domains are down, you must domainprep for each domain that hosts exchange users.
Reference
Exchange Server 2003 Deploy Tools

QUESTION 2
You are the Exchange administrator for Certkiller .
The company operates offices in Athens and Madrid.
The network consists of a single Active Directory forest, as shown in the exhibit.



Each office consists of a single Active Directory site and contains domain controllers for only the local domain.
You plan to implement Exchange Server 2003 as the companywide messaging system.
You plan to deploy Exchange servers in both sites.
You need to ensure that the Active Directory infrastructure is prepared is prepared to support this implementation.
What should you do?

A. Run the setup /forestprep command in the forest root domain.
Run the setup /domainprep command in both domains.
B. Run the setup /forestprep command in the forest root domain.
Install the Exchange system management tools.
Delegate the role of Exchange Full Administrator at the Exchange organization level to the Domain Admins group in both domains.
C. In the Madrid site, configure at least one domain controller as a global catalog server.

D. In the Madrid site, enable universal group membership caching and configure the Madrid site to refresh the cache from the Athens site.

Answer: A
Explanation
You plan to deploy Exchange servers in both sites. The DomianPrep option creates the groups and permissions necessary for Exhange Server to read and modify user attributes. You must run DomainPrep once in each domain that contains an Exchange Server 2003 server, and any domain that hosts Exchange users. This means both the Madrid site, and the Athens site.
Reference
Exchange Server 2003 Deploy Tools

QUESTION 3
You are the Exchange administrator for Certkiller .
The network consists of a single Active Directory domain named Certkiller .com.
All network servers run Microsoft Windows Server 2003.
The company operates five offices worldwide.
Management plans to install Exchange Server 2003 on one member server in each office.
Users will use HTTPS, WAP devices, MAPI, IMAP, and SMTP/POP3 to connect to the Exchange servers.
You create a script to automate the installation.
IT administrators in each office will prepare the servers to support the scripted installation.
You need to specify any additional Windows Server 2003 components that will be required.
Which component or components should you specify? (Choose all that apply)

A. World Wide Web Service
B. NNTP service
C. SMTP service
D. POP3 service
E. ASP.NET

Answer: A, B, C, E
Explanation
Installing and Enabling Windows 2000 or Windows Server 2003 Services
Exchange 2003 Setup requires that the following components and services be installed and enabled on the server:
• .NET Framework
• ASP.NET
• Internet Information Services (IIS)
• World Wide Web Publishing Service
• Simple Mail Transfer Protocol (SMTP) service
• Network News Transfer Protocol (NNTP) service
If you are installing Exchange 2003 on a server running Windows 2000, Exchange Setup installs and enables the Microsoft .NET Framework and ASP.NET automatically. You must install the World Wide Web Publishing Service, the SMTP service, and the NNTP service manually before running Exchange Server 2003 Installation Wizard.
If you are installing Exchange 2003 in a native Windows Server 2003 forest or domain, none of these services is

enabled by default. You must enable the services manually before running Exchange Server 2003 Installation Wizard.
Reference
Exchange Server 2003 Deployment Guide

QUESTION 4
You are the Exchange administrator for Certkiller .
The network consists of a single Active Directory domain named Certkiller .com.
All network servers run Microsoft Windows Server 2003.
You plan to install Exchange Server 2003 on a member server named Exch1.
You use a domain user account named ExchAdmin to run the setup /forestprep command.
However, you receive an error message stating that the account does not have the necessary permissions to perform this task.
You need to ensure that the ExchAdmin account can be used to run the setup /forestprep command.
To which two groups should you add ExchAdmin? (Each correct answer presents part of the solution. Choose two)

A. Administrators on Exch1
B. Enterprise Admins in the domain
C. DnsAdmins in the domain
D. Schema Admins in the domain
E. Administrators in the domain

Answer: B, D
Explanation
ForestPrep extends the Active Directory schema for Exchange Server 2003. You must rin ForestPrep in the domain where the schema master resides. To run ForestPrep, your account must be a member of the Enterprise Admins group, and the Schema Admins group.
Reference
Exchange Server 2003 Deploy Tools

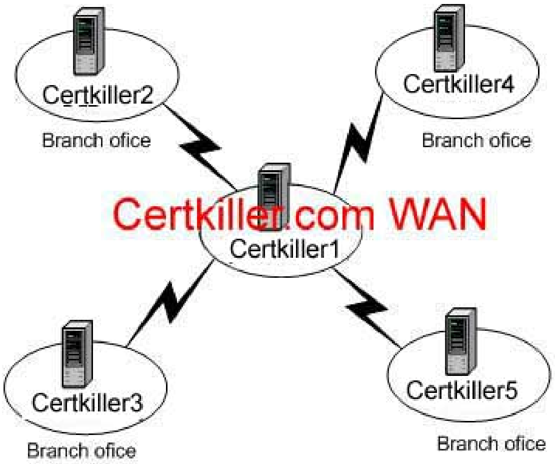
QUESTION 5
You are the Exchange administrator for Certkiller .
The network consists of a single Active Directory forest.
The forest contains the forest root domain Certkiller ,com and one child domain japan. Certkiller .com.
User accounts and group accounts are contained in the child domain.
Management decides to deploy Exchange Server 2003 as the companywide messaging system.
You prepare the forest to support a new Exchange Server 2003 organization.
Replication completes normally.
You install the first Exchange Server 2003 system in the forest root domain.
You need to ensure that all user accounts can be mailbox-enabled.
What should you do?

A. Run the setup /domainprep command in the forest root domain.
B. Run the setup /domainprep command in the child domain.
C. Install Active Directory Connector (ADC) on a domain controller in the forest root domain.

D. Install Active Connector (ADC) on a domain controller in the child domain.

Answer: A, B
Explanation
Management decides to deploy Exchange Server 2003 as the company wide messaging system. This means Certkiller .com and one child domain japan. Certkiller .com. The DomianPrep option creates the groups and permissions necessary for Exhange Server to read and modify user attributes. You must run DomainPrep once in each domain that contains an Exchange Server 2003 server, and any domain that hosts Exchange users. This means both Certkiller .com and japan. Certkiller .com.
Reference
Exchange Server 2003 Deploy Tools

QUESTION 6
You are the Exchange administrator for Certkiller . The network consists of a single Active Directory domain Certkiller .com. All network servers run Microsoft Windows Server 2003. The relevant portion of the network configuration is shown in the exhibit.

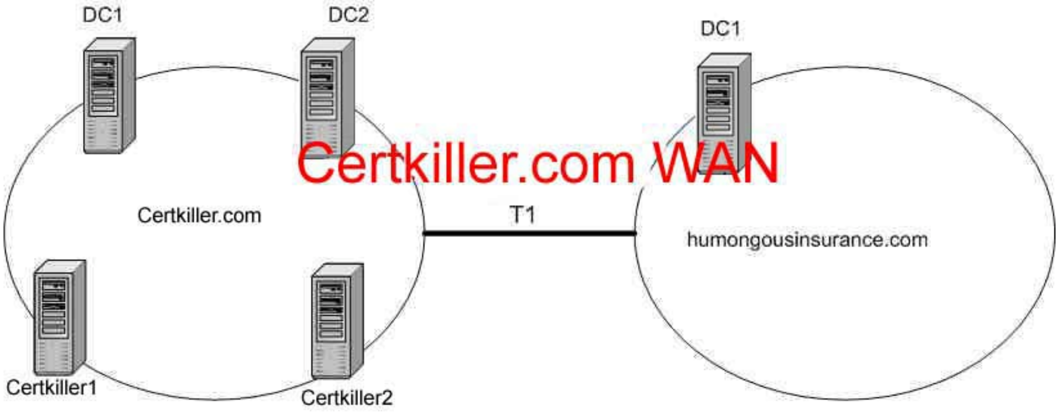


Each of the five offices is defined as a separate Active Directory site. Each site contains one global catalog server, which also provides DNS services for all local computers. The global catalog servers are named Certkiller 1 through Certkiller 5.
Active Directory replication is managed by the company's networking group. The server in each branch office replicates with the main office once a day after regular business hours. To avoid saturating the WAN connections or overloading Certkiller 1, the starting times for replication are staggered by one hour. Active Directory replication cannot be forced to occur at any time other than the regularly scheduled replication interval.
Management decides to implement Exchange Server 2003 as the companywide messaging system. Each office requires its own Exchange server, which must be located in a separate routing group. Necessary hardware is purchased. All appropriate software is installed in each office to prepare for the installation of Exchange. You install Exchange on a new server in the main office and create all of the routing groups. Then you immediately begin to remotely install Exchange on a new server in one of the branch offices. However, you are unable to select a routing group in which to place the server. You cancel the installation.
You need to ensure that you can complete the installation of the branch office Exchange servers before the end o the business day.
What should you do?

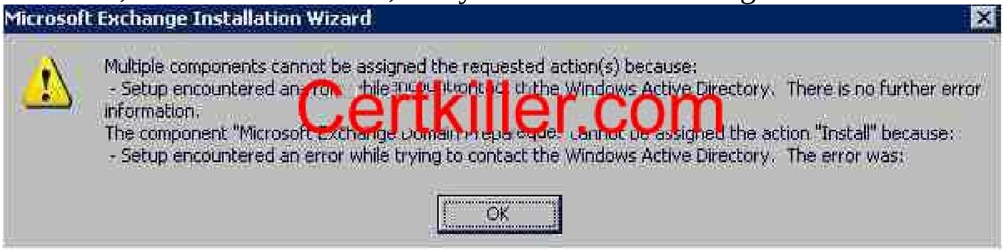
A. First configure the new server in each branch office to point to Certkiller 1 as its primary DNS server.
Then install Exchange Server 2003 on the new server.
B. First configure the new server in each branch office to point to the local global catalog server as its primary DNS server.
Then install Exchange Server 2003 on the new server.
C. On the new server in each branch office, install Exchange by running setup /choosedc and specify Certkiller 1.
D. On the new server in each branch office, install Exchange by running setup /choosedc and specify the local global catalog server.

Answer: C
The question tells us that the Active Directory replication schedule cannot be modified nor can replication be forced to occur outside of the schedule. Exchange server 2003 installation needs to lookup for the CG attributes for Exchange, the new server site can't been installed until the replication occurs. However, you can use the new Exchange Server 2003 switch /chooseDC and select Certkiller 1 as the GC to successfully install Exchange.
This switch can be used to specify the domain controller that Setup must use during installation to read and to write Microsoft Active Directory service information. You can use the /chooseDC switch in combination with other Exchange 2003 Setup switches, including /domainprep.
Reference
Description of the /ChooseDC Switch in Exchange Server 2003 822593
Setup Options for Exchange Server 2003 822893

QUESTION 7
You are the Exchange administrator for Certkiller .
The network consists of a single Active Directory domain named Certkiller .com.
The domain contains two domain controllers named DC1 and DC2, which are also configured as DNS servers.
The Exchange organization contains two servers, named Certkiller 1 and Certkiller 2 that run Exchange Server 2003.
Certkiller acquires a subsidiary named Humongous Insurance and opens a new office for the subsidiary.
You deploy a new domain controller named DC1 in a new domain tree at the new office. You configure DC1 as a DNS server.
The relevant portion of the resulting network configuration is shown in the Network exhibit.



You install Windows Server 2003 on a new computer in the new office.
You name the new server Exch3 and join it to the humongousinsurance.com domain.
You begin to install Exchange Server 2003 on Exch3.humongousinsurance.com.
However, the installation fails, and you receive the message shown in the Error Message exhibit.



Multiple components cannot be assigned the requested action(s) because:
- Setup encountered an error while trying to contact the Windows Active Directory. There is no further error information.
The component "Microsoft Exchange Domain Preparation" cannot be assigned the action "Install" because:
- Setup encountered an error while trying to contact the Windows Active Directory. The error was:

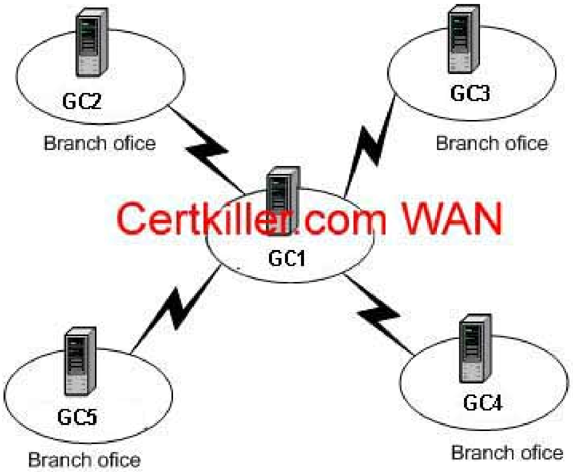
You need to ensure that you can successfully complete the installation of Exch3.humongousinsurance.com.
What should you do?

A. Configure DC1.humongousinsurance.com as a global catalog server.
B. Configure Exch3.humongousinsurance.com to use one of the DNS servers at Woodgrove Bank for DNS services.
C. Configure a secondary zone for Certkiller .com on the DNS server at Humongous Insurance.
D. Configure a conditional forwarder for the humongousinsurance.com zone at the DNS servers at Certkiller so that all queries for humongousinsurance.com are forwarded to DC1.humongousinsurance.com.

Answer: A

Explanation:
This error occurs when Setup cannot locate a qualifying Global Catalog server to connect to. Exchange needs at least one domain that contains a Global Catalog server that belongs to the local or an adjacent Windows site.
References
"Multiple Components Cannot Be Assigned the Requested Action" Error Message During Exchange 2003 Installation KB 822439
http://support.microsoft.com/default.aspx?scid=kb;en-us;822439
"Setup Encountered an Error While Trying to Contact the Windows Active Directory" Error Message When You Try to Install Exchange Server 2003 to an Existing Windows 2000 Domain KB 822452
http://support.microsoft.com/default.aspx?scid=kb;en-us;822452
Cannot Install Exchange Server 2003 in a Child Domain after You Run SETUP /DOMAINPREP KB 817378
http://support.microsoft.com/default.aspx?scid=kb;en-us;817378

QUESTION 8
You are the Exchange administrator for Certkiller .
The network consists of a single Active Directory domain named Certkiller .com.
All network servers run Microsoft Windows Server 2003.
The relevant portion of the network configuration is shown in the exhibit.



Each of the five offices is defined as a separate Active Directory site.
Each site contains one global catalog server, which also provides DNS services for all local computers.
The global catalog servers are named GC1 through GC5.
Active Directory replication is managed by the Certkiller 's networking group.
The server in each branch office replicated with the main office once a day after regular business hours.
To avoid saturating the WAN connections or overloading GC1, the starting times for replication are staggered by one hour.
Active Directory replication cannot be forced to occur at any time other than the regularly scheduled replication interval.
Management decides to implement Exchange Server 2003 as the companywide messaging system.
Each office requires its own Exchange server, which must be located in a separate routing group.
Necessary hardware is purchased.
All appropriate software is installed on each office to prepare for the installation of Exchange.
You install Exchange on a new server in the main office and create all the routing groups.
Then you immediately begin to remotely install Exchange on a new server in one of the branch offices.
However, you are unable to select a routing group in which to place the server.
You cancel the installation.
You need to ensure that you can complete the installation of the branch office Exchange servers before the end o the business day.
What should you do?

A. Run setup /choosedc GC1
B. **MISSING**

A. **MISSING**
C. **MISSING**

Answer: A

Explanation:
They have already have installed Exchange on a new server in the main office and create all the routing groups.
To avoid saturating the WAN connections or overloading GC1, the starting times for replication are staggered by one hour in this way they need to wait a least one hour because replication can't be forced and they need to

wait replication from GC1 to GC2, GC3, GC4 and GC5.
They basically can do two things: Wait for replication al least 5 hours until the full mesh replication finish and use repadmin or replmon to check that all the objects have been replicated from GC1 until to begin to install the next Exchange. Or they can use the option setup /choosedc GC1. In this way they setup will query to CG1 for Exchange objects info.

QUESTION 9
You are the Exchange administrator for Certkiller .
The company operates three offices.
The network consists of a single Active Directory domain named Certkiller .com.
Each office has one domain controller that runs Microsoft Windows Server 2003.
You plan to deploy one Exchange Server 2003 computer in each office.
Each Exchange server must be placed in a separate administrative group.
The forest and the domain are already prepared to support Exchange Server 2003.
When you try to install the first Exchange server, you discover that you cannot choose an administrative group in which to place the server.
You cancel the installation.
You need to ensure that you can choose an administrative group during installation.
What should you do?

A. Install Exchange Server 2003 by running the setup /choosedc command and specify the local domain controller.
B. Install Exchange System Manager. Create the administrative groups.
C. Install Exchange System Manager. At the Exchange organization level, assign the Exchange Full Administrator permissions to the account used to install Exchange Server 2003.
D. At the Administrative Groups container level, use Active Directory Sites and Services to assign the Full Control permission to the account used to install Exchange Server 2003.

Answer: B
Explanation
If the administrative group or routing group already exists, a server only can be assigned to a routing group or to an administrative group during the installation phase.
By default, if one Exchange server has been installed only one administrative group, the First Administrative Group exists. To be able to install the FIRST Exchange server in a different administrative Group than the default, the required administrative group must be created prior to the installation.
The forest and the domain are already prepared to support Exchange Server 2003.
You must install the Exchange System Manager tool choosing a custom action during the setup.
Incorrect Answers

A. Exchange Setup includes the new /ChooseDC switch. You can now enter the fully qualified domain name (FQDN) of a Windows domain controller to force Setup to read and write all data from the specified domain controller (the specified domain controller must reside in the domain where you install your Exchange 2003 server). When installing multiple Exchange 2003 servers simultaneously, forcing each server to communicate with the same Active Directory(r) directory service domain controller ensures that replication latencies do not interfere with Setup and cause installation failures.
"setup.exe" /ChooseDC "Your FQDN Server name here"

The principal reason to use this switch is to avoid errors during multiple Exchange setup running to same time
C, D. Exchange System Manager by default is installed when you install the first Exchange server
Also is required to permit administrators who are assigned the Exchange Full Administrator administrative role at the administrative group level to install and to remove Exchange Server 2003, to upgrade servers, and to perform disaster recovery on servers that are in that administrative group. They already have and account that is able to perform this task, same account that they have used to run ForestPrep and DomainPrep switch's
Reference
Exchange Server 2003 Deployment Guide

QUESTION 10
You are the Exchange administrator for Certkiller .
The network consists of a single Active Directory domain named Certkiller .com.
The network contains an Exchange Server 2003 active/passive server cluster that contains nodes named Exchange1 and Exchange2.
The NetBIOS name of the cluster is Cluster1.
The cluster contains one Exchange Virtual Server (EVS) named EVS1.
The configuration of the cluster is shown in the following table.

Name	**Fully qualified domain name**
Exchange1	Exchange1. Certkiller .com
Exchange2	Exchange2. Certkiller .com
CLUSTER1	CLUSTER1. Certkiller .com
EVS1	EVS1. Certkiller .com

Users attempt to connect to Exchange1. Certkiller .com by HTTP, but fail.
You need to ensure that users can connect to their e-mail servers by using Microsoft Outlook Web Access.
What should you do?

A. Create an HTTP virtual Web site for Exchange1. Certkiller .com.
B. Create an HTTP virtual Web site for CLUSTER1. Certkiller .com.
C. Instruct users to connect to CLUSTER1. Certkiller .com.
D. Instruct users to connect to EVS1. Certkiller .com

Answer: D

Explanation:
The client connection name to connect form clients need to be called as is Exchange virtual instance
Cluster1 is suppose to be cluster name, no the virtual instance Exchange Virtual Server (EVS) is named EVS1

http access provides access to an Exchange mailbox and public folders through HTTP (for example, using Outlook Web Access) and is Created automatically after the creation of the Exchange System Attendant resource.
The client should use a NetBIOS name to connect to the cluster. The configuration information is completely irrelevant. The NetBIOS name is the only name that will be understood outside of the cluster set.
Incorrect answers:

A. Creating an HTTP virtual web site is unnecessary. Users should be able to connect to the default virtual site and make the connection.
B. Users need to connect to the cluster, not to the cluster resource name. The name cluster1. Certkiller .com is the internal name; not an external one.
C. CLUSTER1. Certkiller .com is the name of the Cluster. It is not used externally for clients.

QUESTION 11
You are the Exchange administrator for Certkiller .
The network contains a single Active Directory domain named Certkiller .com.
The functional level of the domain is Windows Server 2003.
The network is configured in a two-node Exchange Server 2003 cluster.
The cluster nodes are named Exchange1 and Exchange2.
The cluster includes a single Exchange Virtual Server (EVS) named Exch1.
All mailboxes are on Exch1.
The cluster node receives its IP addresses from a DHCP server.
The Exchange1 node is the preferred owner of Exch1.
Users report that they cannot access the Exchange server.
You open Cluster Administrator.
You notice that all the cluster resources in the Exchange cluster group are offline except for the disk resources.
You attempt to bring the Exch1 cluster group online, but the attempt fails and you receive the following error message: "This IP address is already in use".
You need to bring the Exch1 cluster group back online and ensure that it remains accessible.
What should you do?

A. Run the ipconfig /registerDNS command from one of the cluster nodes.
B. Run the ipconfig /release command and then run the ipconfig /renew command from one of the cluster nodes.
C. Change the IP address of the cluster IP address resource to a fixed IP address that is reserve for the cluster node.
D. In Cluster Administrator, create a new cluster group. Move the existing Exch1 resources to this new cluster group. Configure the cluster IP address resource with a reserved DHCP address.

Answer: C

Explanation:
Cluster servers require a static IP address to function correctly. The DHCP server attempted to renew the address on the inactive node and failed, then released the address to another client. When the node then needed

the address, it was not available even though the node was using it. This resulted in the problem noted in the question. To permanently resolve this issue, use a static IP address.
Incorrect answers:

A. Running the Registerdns command will attempt to register the server's address with DNS. However, since the address is in use, the command will fail, and the problem will still exist.
B. Releasing and renewing the address will resolve the problem. However, this is not the best answer since some time in the future, the problem will reoccur as the situation described in the explanation happens again.
D. Creating a new cluster group is not required. Although creating the cluster IP address with a reserved address will work, it is much more work than is required to resolve the problem. Therefore, this is not the best answer.

QUESTION 12
You are the Exchange administrator for Certkiller .
The network currently consists of a two-node Exchange Server 2003 active/passive cluster.
Three hundred HTTP client computers connect to the Exchange servers by using SSL.
Users report that the response time of their Microsoft Outlook Web Access screen refreshed is unacceptably slow.
You add two more servers to the existing Exchange environment.
You need to ensure that your HTTP client computers have redundancy and acceptable client response times.
Which two actions should you perform? (Each correct answer presents part of the solution. Choose two)

A. Join the new servers to the existing cluster.
B. Select the option to configure the new servers as front-end servers.
C. Configure the new servers so that they use Network Load Balancing.
D. Create an Exchange System Attendant cluster resource for each front-end server on the existing cluster.

Answer: B, D
Explanation
To configure a clustered back-end server, you must map each front-end server to the nodes of your cluster, so that either node can accept proxy requests from any front-end server in your organization. Proxy requests are requests for messaging services from client computers running Microsoft Outlook(r) Web Access, Outlook Mobile Access, Microsoft Exchange ActiveSync(r), POP3, or IMAP4. These proxy requests are sent to the cluster through the front-end servers. All communication between front-end and back-end servers goes through TCP port 80, regardless of the port used for communication between the client and front-end server.
Incorrect Answers:

A. Joining the servers to the existing cluster would resolve the problem, as processing power is disturbed among three servers as opposed to one. (Remember that one server in active/passive is unused.)
However, if this were done, it would not conform to Microsoft Best Practices. In addition, there would be no second answer, and as the question specifically calls for two answers, this answer can't be correct.
C. This is not an option when the back-end is a Cluster

QUESTION 13
You are the Exchange administrator for Certkiller .
All network servers run Microsoft Windows Server 2003.
The network contains a two-node server cluster.
Another administrator installs Exchange Server 2003 on the cluster in an active/passive configuration.
When you test the installation, you discover that Exchange is not running on the cluster. Exchange services are set to manual startup and are not running on either node.
You need to ensure that Exchange is running on the cluster.
What should you do?

A. Configure all Exchange services to start automatically on the active node.
Reboot the active node.
B. Configure all Exchange services to start automatically on both nodes.
Reboot both nodes.
C. Create a new cluster resource group for the Exchange server and create a System Attendant resource.
D. In Exchange Server 2003, run the setup /disasterrecovery command to reinstall Exchange Server 2003 on the active node.

Answer: C
Explanation
It is only stated that Exchange has been installed in a Cluster. However, to permit an active passive configuration, we need to perform two additional tasks. We need to create a new cluster resource group for the Exchange server and create a System Attendant resource for the active/passive configuration.

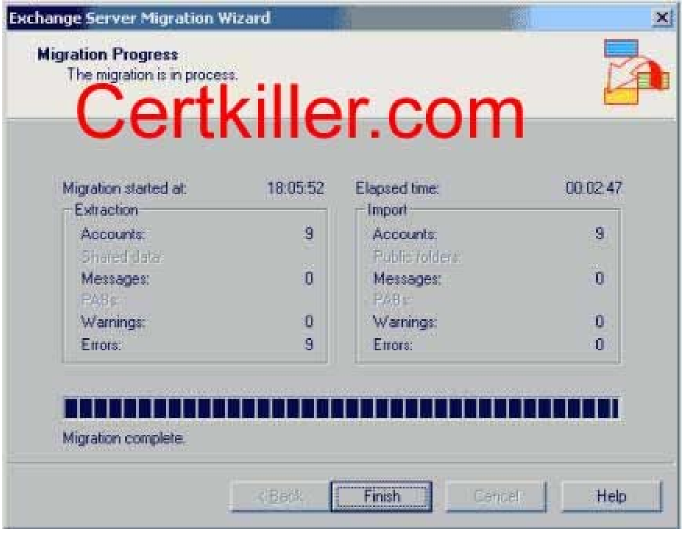
QUESTION 14
You are the Exchange administrator for Certkiller .
The company's network consists of a single Active Directory domain named Certkiller .com.
You attempt to install Exchange Server 2003 on your existing Exchange Server 5.5 computer. Setup fails, and you receive the following error message: "This version of Microsoft Exchange does not support upgrading from Exchange Server 5.5."
You need to ensure that Exchange Server 2003 can be installed on the existing exchange 5.5 server.
What should you do?

A. Install the Exchange Sever 2003 Active Directory Connector (ADC).
B. Upgrade the Exchange 5.5 server to Exchange 2000 Server.
C. Upgrade the operating system of the Exchange 5.5 server to Microsoft Windows Server 2003.
D. Run the commands to clean and prepare the forest and to prepare the domain for Exchange Server 2003.

Answer: B
Explanation
An in-place upgrade from Exchange Server 5.5 to Exchange 2003 is not supported. Because they ask to us for an in-place upgrade, an upgrade to Exchange 2000 is required. After migrate to Exchange 2000 migrate from Exchange 2000 to Exchange 2003.
References
Considerations When You Upgrade to Exchange Server 2003 822942

Overview of Operating System and Active Directory Requirements for Exchange Server 2003 822179
XADM: Description of Exchange Server Migration Methods 327928

QUESTION 15
You are the Exchange administrator for Certkiller . The network consists of a single Active Directory domain Certkiller .com. Currently, companywide messaging services are provided by an IMAP4 mail server.
You create a new Exchange organization to replace the existing messaging system. Exchange Server 2003 is installed on all Exchange servers. All IMAP4 mailbox data must now be migrated to an Exchange server named Certkiller 1. IMAP4 users already have user accounts in the domain. You manually create a migration file that lists all IMAP4 users. Then you perform a one-step migration of the IMAP4 mailbox data. The migration completed with errors. The migration summary is shown in the exhibit.



Migration Progress
The migration is in process.

Migration started at: 18:05:52
Elapsed time: 00:02:47

Extraction
Accounts: 9
Shared data:
Messages: 0
PABs:
Warnings: 0
Errors: 9

Import
Accounts: 9
Public folders:
Messages: 0
PABs:
Warnings: 0
Errors: 0

Migration complete.

You verify that the Active Directory user accounts for the IMAP4 users have Exchange mailboxes on Certkiller 1. However, the mailboxes are empty.
You need to ensure that all IMAP4 mailbox data is migrated to the new Exchange mailboxes.
What should you do?

A. Enable and start the Exchange IMAP4 service on Certkiller 1 and return the one-step migration.
B. Create an Active Directory user account that has the same user name and password as the IMAP4 mail administrator.
Assign the Send As permission on Certkiller 1 to the new account.
Use the new account to log on to Certkiller 1 and rerun the one-step migration.
C. Collect the Exchange alias name of each new Exchange mailbox.
Use this information to update the migration file and rerun the one-step migration.
D. Collect the IMAP4 mailbox password of each IMAP4 user.
Use this information to update the migration file and rerun the one-step migration.

Answer: B
Explanation
IMAP4 users already have user accounts in the target domain and you manually create a migration file that lists all IMAP4 users. Exchange Migration Wizard must have appropriate permissions in the original mail account and in the destination to be able to access. In order to do that you will need to give the account the send as

permission to the Migration wizard account
The Migration Wizard is a stand-alone application that is installed on your computer during Exchange setup.
The Migration Wizard consists of two types of components: source extractors and a migration file importer.
Source extractors copy directory information, messages, and calendar information from various messaging systems. They save the data in and intermediate file format that can be read by the migration file importer.
After the information is in an intermediate file format, the migration file importer imports directory information to Active Directory and then adds messaging data to Information Store.
You can perform both steps in this two-step process (extract and then import) the same time or in separate steps.

QUESTION 16
You are the Exchange administrator for Certkiller .
Certkiller acquires a company named Tailspin Toys.
Certkiller has a single Active Directory forest named Certkiller .com.
Tailspin Toys has a single Active Directory forest named tailspintoys.com.
Certkiller uses a directory synchronization tool to synchronize identity information between the directory services.
For business reasons, you cannot decommission either of the two forests.
Users will continue to use either Certkiller .com or tailspintoys.com as their primary logon domain.
Users in each forest have mailboxes on servers in their local Exchange organization.
When users in both forests search the global address list (GAL), they must be able to see recipients from both forests.
You need to create the required directory objects on the two forests. For security reasons, you must create objects that have only the minimum necessary rights and permissions.
What should you do?

A. For every mailbox-enabled user object in the tailspintoys.com domain, create a mail-enabled inetOrgPerson object in the Certkiller .com domain.
For every mailbox-enabled user object in the Certkiller .com domain, create a mail-enabled inetOrgPerson object in the tailspintoys.com domain.
B. For every mailbox-enabled user object in the tailspintoys.com domain, create a mail-enabled disabled user object on the Certkiller .com domain.
For every mailbox-enabled user object in the Certkiller .com domain, create a mail-enabled disabled user object in the tailspintoys.com domain.
C. For every mailbox-enabled user object in the tailspintoys.com domain, create a mail-enabled enabled user object in the Certkiller .com domain.
For every mailbox-enabled user object in the Certkiller .com domain, create a mail enabled enabled user object in the tailspintoys.com domain.
D. For every mailbox-enabled user object in the tailspintoys.com domain, create a mail-enabled contact object in the Certkiller .com domain.
For every mailbox-enabled user object in the Certkiller .com domain, create a mail-enabled contact for object in the tailspintoys.com domain.

Answer: D
By creating contacts in each organization for the users in the other domain, the users can access any users' contact from their own GAL without requiring permissions.
Incorrect answers:

A. The InetOrgPerson object is designed to be used as an outward facing security context. Therefore, it is ideal for use as e-mail recipients for external users or for Internet access to mail in a hosting scenario Exchange Server mailboxes can be configured to have an associated Windows account (Primary Windows NT accounts) that are InetOrgPerson objects. The ADC may partially replicate these objects, however this is not a supported scenario as InetOrgPerson objects are not supported in scenarios with an ADC installed. The InetOrgPerson object class can be mailbox-enabled or mail-enabled but to be able to use the InetOrgPerson object Active Directory must be 2000 SP3 or Windows 2003 and Exchange 2003 must be in native mode they do not give us that information
B, C: Each of these answers give the tailspintoys users an account in Active Directory. This violates the requirement that the users not have any rights. (The users would at least have domain user rights, and this is not acceptable given the scope of the question.)
References:
InetOrgPerson Object Support in Exchange 2003 KB article 822591
Overview of the Differences Between Mixed Mode and Native Mode in Exchange Server 2003 KB article 822446

QUESTION 17
You are the Exchange administrator for Certkiller .
The network consists of a single Active Directory domain Certkiller .com.
A single Exchange organization contains servers that run Exchange Server 2003.
The domain contains 500 Contact objects that represent company customers.
The Contact objects are used by all users and updated infrequently. The domain also contains mailboxenabled users.
Certkiller acquires another company Acme.
The other company's network consists of a single Active Directory domain acme.com. A single Exchange organization contains servers that run Exchange Server 2003.
The other company's domain contains 200 Contact objects that represent company customers and are updated frequently.
Microsoft Outlook is the only e-mail client in use in both companies.
Written security polices state that users in one domain must no have any security permissions in the other domain, including the permission to read Active Directory information.
You need to enable users in both companies to send e-mail messages to the Contact objects from both domains.
What should you do?

A. Configure a two-way trust relationship between the domains.
Configure SID filtering so that SIDs in one domain cannot be used in the other domain.
B. Use Active Directory Users and Computers to export the Contact objects from each domain.
Then use an import utility to import the objects into the other domain.
C. Configure Outlook in each domain to make LDAP queries against the other company's domain.
D. Configure DNS in each domain to use DNS server in the other domain as a forwarder.

Answer: B
Explanation
Because of the tight integration between Exchange and Active Directory, the Active Directory forest structure

directly affects your Exchange planning. There is a one-to-one relationship between an Active Directory forest and an Exchange organization. An Exchange organization can span only a single Active Directory forest. Likewise, an Active Directory forest can host only a single Exchange organization.
Understanding your current forest structure and the reasoning behind those design decisions can help you to decide whether to use an existing forest to host Exchange or whether to create a new forest to host Exchange.
Although the recommended design for Active Directory consists of a single Active Directory forest for the entire organization. Your organization may contain multiple forests that represent separate business units. One reason this design may be necessary is if your organization needs strict security boundaries between the directories for each business unit.
In a multiple forest scenario, you need to determine which forest is to host Exchange. To reduce the administrative burden, you also need to implement a provisioning method so that changes made in one forest are propagated to the other forests, for example, by using Microsoft Identity Integration Manager (MIIS).
Another option is to create a separate forest dedicated to running Exchange. By default you can't access from one Exchange Organization GAL (Global Address Book), to another Exchange Organization GAL (Global Address Book), including if they have a trust relation between forests
You will need to use some as Microsoft Identity Integration Server to sync both directories.
So the only way that they can take is to import export the contacts
Incorrect Answers:

A. SID filtering ensures that any misuse of the SIDHistory attribute on security principals (including inetOrgPerson) in the trusted forest cannot pose a threat to the integrity of the trusting forest.
The SIDHistory attribute can be useful to domain administrators when they migrate user and group accounts from one domain to another. Domain administrators can add SIDs from an old user or group account to the SIDHistory attribute of the new, migrated account. By doing this, domain administrators give the new account the same level of access to resources as the old account.
B. You can't configure outlook in each domain to make LDAP queries against the other company's domain because the users have not any account or rights in the other forest.
C. Configure DNS in each domain to use DNS server in the other domain as a forwarder only will be useful to resolve names
References:
Windows 2003 Concepts: Securing External Trusts
Exchange Server Chapter 2 - Planning Your Active Directory and Administrative Model
Active Directory Chapter 2: Establishing Secure Active Directory Boundaries

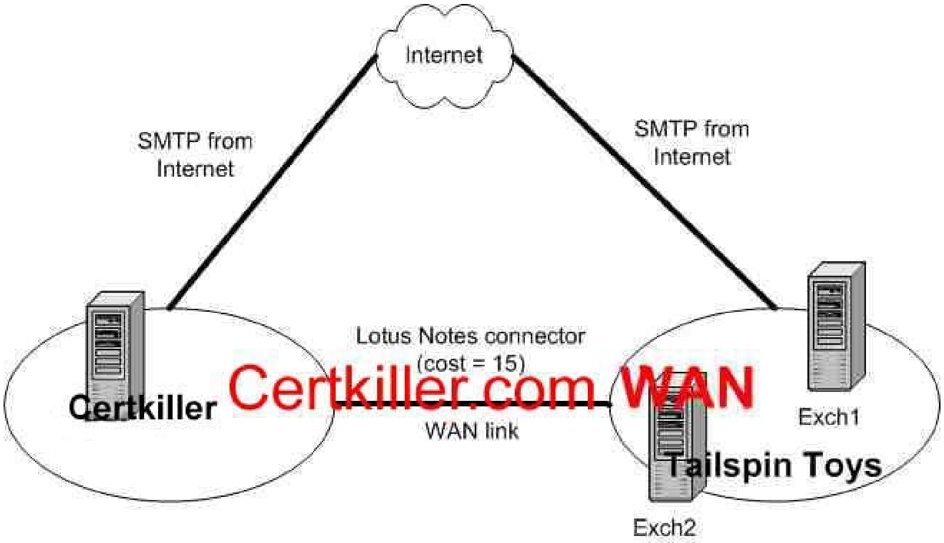
QUESTION 18
You are the Exchange administrator for Certkiller .
The Exchange organization contains a single Exchange Server 2003 computer.
Users at Certkiller frequently exchange e-mail with another company.
A new security agreement between the two companies specifies that all e-mail containing proprietary information must be encrypted when it is transmitted across the Internet.
The other company does not have a public key infrastructure.
The other company's management refuses to use a commercial certification authority (CA) to obtain certificates for its users.
However, they are willing to purchase a small number of certificates for their servers.
You need to ensure that e-mail transmitted across the Internet complies with the new security agreement.
What should you do?

A. Obtain digital certificates for each user in Certkiller .
Instruct each user to send digitally signed messages to all users at the other company.
B. Configure your Exchange server to use Transport Layer Security (TLS) when it connects to the mail server at the other company.
Instruct the e-mail administrator at the other company to configure its mail server in the same way.
C. Configure your Exchange server to use IPSec to encrypt all outgoing SMTP traffic.
D. Configure the Exchange HTTP virtual server to require SSL connections.

Answer: B
Explanation
We can avoid using commercial PKI infrastructure using TLS.
Incorrect Answers

A. The other company's management refuses to use a commercial certification authority, therefore we cannto get certificates of each user.
B. IPSEC can be used, but we need to use certificates or preshared key and encrypt the communication not just the outgoing email.
D. They do not tell us that they are using OWA to communicate
Reference
Exchange 2003 Server Help

QUESTION 19
You are the Exchange administrator for Certkiller .
The network consists of a single Active Directory domain named Certkiller .com.
The Exchange organization contains a single routing group that consists of two Exchange Server 2003 computers named Exch1 and Exch2.
Exch1 is configured as a bridgehead server for SMTP traffic to and from the Internet.
Exch2 contains all user mailboxes.
Certkiller purchases Foobar Inc., which is located in another city.
The Foobar network contains a single Lotus Notes server name Notes1.
Notes1 can receive SMTP messages that are addressed to foobar.com.
IP routing is configured so that the WAN link will be used as the default rote for all network traffic between computers in the two locations.
Contact objects for all Lotus Notes mailboxes in Foobar were previously created in the Certkiller .com domain.
Each Contact object contains the foobar.com SMTP address of the associated user.
Each Contact object is updated with the Lotus Notes address of the associated user.
The network is configured as shown in the following diagram.



Users in Certkiller report slow delivery of messages that are sent to users in Foobar.
When you track these messages, you discover that they are being sent by Exch1 as SMTP messages over the Internet.
You need to ensure that messages sent to users in Foobar by users in Certkiller will be sent by using the Lotus Notes connector.
What should you do?

A. Configure the cost of the SMTP connector on Exch1 to be 20.
B. Configure the cost of the Lotus Notes connector on Exch2 to be 5.
C. Configure a Lotus Notes connector between Exch1 and Notes1.
D. Configure the SMTP connector on Exch1 to allow a maximum message size of 1,000 KB for outgoing messages.
E. Configure the Contact objects for the Lotus Notes users to set the default e-mail address for each contact to be the Lotus Notes address.

Answer: E

Explanation:
The smtp route will be taken irrespective unless the Lotus notes connector is configured for an address space of *foobar.com and has a lower cost than the smtp route over the internet. Hence setting the cost on the connector from the Bridgehead Exch1 alone will not be enough. Note it Exch1 not 2 as the answer in B says

---

QUESTION 20
You are the Exchange administrator for Certkiller .
All seven servers in the Exchange organization run Exchange Server 2003.
Certkiller acquires another company that uses a single Novell GroupWise server that runs on NetWare.
The GroupWise mailboxes are assigned SMTP addresses in a namespace that is different from the namespace used by the Exchange mailboxes.
For business reasons, it is not possible for you to migrate the GroupWise users to Exchange immediately.
You configure one of the Exchange servers, which have no local mailboxes, as a dedicated bridgehead server for communications to the GroupWise server.
Exchange users can see the GroupWise users in the Exchange global address list (GAL) and can send

messages to them. However, when the Exchange users want to send meeting requests, they cannot view the free or busy status of GroupWise users.
You need to ensure that the Exchange users can view the free or busy status of the GroupWise users.
What should you do?

A. On the Exchange bridgehead server, configure the Calendar Connector.
B. On the Exchange bridgehead server, install the Gateway Service for NetWare.
C. On the Exchange bridgehead server, add a replica of the Schedule+ Free Busy folder.
D. On the Exchange bridgehead server, create an SMTP connector to one of the GroupWise SMTP bridgehead servers.
E. On all Exchange servers, install the Microsoft Exchange Connector for Novell GroupWise.

Answer: A

Explanation:
The Calendar Connector always stores free and busy information in its administrative group's public folder, specifically the Schedule+ Free Busy public folder. If there are multiple administrative groups on an Exchange 2003 server, each administrative group has its own public folder. In this case, free and busy information for Exchange 2003 users may be stored in a different public folder than the free and busy information for users on partner computers.
You cannot initiate real-time queries to downstream Exchange 2003 routing groups. Exchange users in routing groups that are not directly connected by the Calendar Connector to a partner system (routing groups downstream of the routing group in which the Calendar Connector is installed) are not able to initiate real-time queries. Instead, they receive the calendar data that has been replicated from the Calendar Connector's site (routing group). If you want to provide real-time free and busy access to all Exchange users, install and configure a Calendar Connector in each Exchange site (routing group). There is no way to relay a real-time free and busy query over a Site Connector or Routing Group connector.
You cannot use the Calendar Connector as a free and busy switch between Notes and GroupWise. Exchange does not support free and busy switches or queries from one partner computer to another by using Exchange as a backbone. In addition, you cannot use a partner computer as a backbone between two Exchange computers.
You cannot configure multiple Calendar Connectors in a single administrative group that connects to the same partner post office
Reference
Appendix B - Configuration Procedures for Migrating from Novell Groupwise Messaging Functionality

---

QUESTION 21
You are the Exchange administrator for Certkiller .
Some user mailboxes are on servers that run Exchange Server 2003, and other user mailboxes are on servers that run Lotus Notes.
The Lotus Notes connector is installed on an Exchange server.
The sales department has been partially migrated from Lotus Notes to Exchange Server 2003.
In Active Directory, you create a mail-enabled universal distribution group named SalesDepartment, to which you add all the Exchange mailboxes for users in the sales department.
The other users in the sales department have Lotus Notes mailboxes.
These users are members of a Lotus Notes group named Sales.
Mail-enabled contact objects have been created in Active Directory for users who have Lotus Notes

mailboxes.
A mail-enabled contact named Sales has been created in Active Directory for the Sales group in Lotus Notes.
Currently, when an Exchange user sends an e-mail message to the SalesDepartment distribution group, it is delivered to users in the sales department who have Exchange mailboxes, but it is not delivered to users who have Lotus Notes mailboxes.
You need to ensure that Exchange users can send messages to all users in the sales department.
However, Exchange administrators must not be required to make changes when additional mailboxes are added to Lotus Notes for users in the sales department.
Your solution should minimize traffic between the Exchange servers and Lotus Notes servers.
What are two possible ways to achieve this goal? (Each correct answer presents a complete solution. Choose two)

A. In Active Directory, add the Sales contact object to the SalesDepartment universal group.
B. In Active Directory, add the contact objects for sales department users who have Lotus Notes mailboxes to the SalesDepartment universal group.
C. In Lotus Notes, create a contact for the SalesDepartment universal group. Add the contact to the Sales group on Lotus Notes.
D. Instruct Exchange users to send message both to the SalesDepartment universal group and the Sales contact when they need to send messages to the entire sales department.

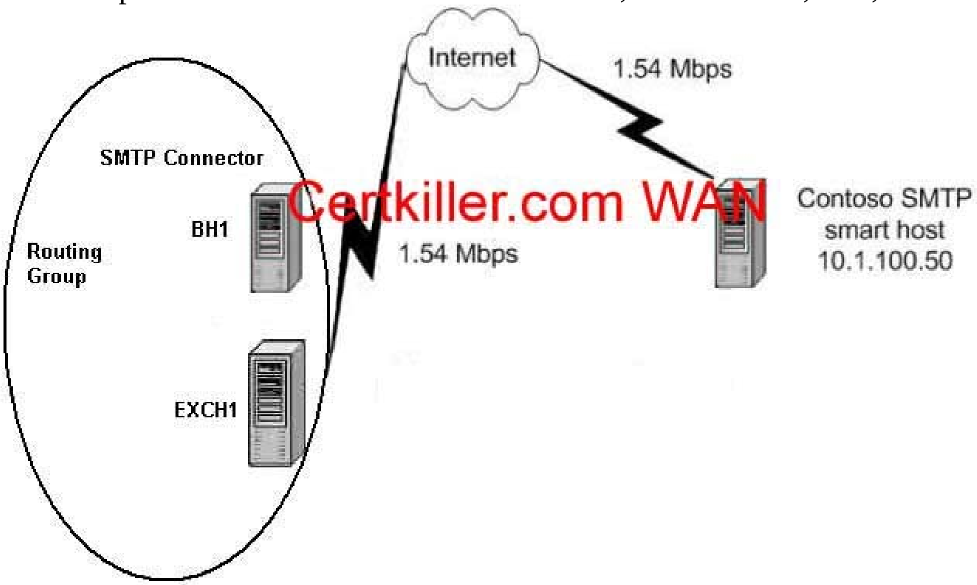
Answer: A, C

Explanation:

A. Adding the Sales contact to the SalesDepartment group will work, as the Sales contact encompasses all Notes users in the Sales group in Active Directory
C. Adding the SalesDepartment contact to Notes will work because the SalesDepartment contact is mailenabled in Active Directory.
Incorrect Answers:
B. Adding the contacts individually would mean a great deal of administration. In addition, when more Notes users are added, the administrator would have to go back and add these users to the proper group. Since there is administration overhead involved with this process, this answer is not correct.
D. The administrator would have to inform the new Notes user that he has to send to two groups instead of one. This can be easily overlooked, and would result in help desk phone calls when this problem returned. While this answer would technically work, it is not the best answer.

QUESTION 22
You are the Exchange administrator for Certkiller . The network consists of a single Active Directory domain named Certkiller .com. The functional level of the domain is Microsoft Windows Server 2003. The Exchange organization contains two servers that run Exchange Server 2003.
The servers are named Exch1 and BH1. All mailboxes are located on Exch1.
BH1 is a bridgehead server and contains no mailboxes.
BH1 is configured with an SMTP connector for all Certkiller Internet e-mail.
Certkiller employees need to begin to communicate with employees at a separate company named Contoso, Ltd. The employees need to communicate by using e-mail during business hours.

Employees from Certkiller and Contoso, Ltd., need to send each other attachments that average 20 MB in size.
Certkiller purchases a new leased line to Contoso, Ltd. Contoso, Ltd., used a UNIX-based e-mail system.



You create aliases in your global address list (GAL) for the employees at Contoso, Ltd.
You need to ensure prompt delivery of all messages and attachments from Certkiller to Contoso, Ltd.
You do not want these attachments to delay delivery of other Certkiller messages to the Internet.
What should you do?

A. Configure a second SMTP virtual server. Create a dedicated SMTP connector that uses this virtual server. Forward all mail going through this connector to 10.1.100.50. Add Certkiller .com as an address space on this connector.
B. Configure a second SMTP virtual server. Create a dedicated SMTP connector that uses this virtual server. Forward all mail going through this connector to 10.1.100.50. Add contoso.com as an address space on this connector.
C. Allow 10.1.100.50 as the only IP address to connect to the Certkiller SMTP virtual server. Create a dedicated SMTP connector that uses the existing virtual server. Forward all mail going through this connector to 10.1.100.50. Add contoso.com as an address space on this connector.
D. Configure the Certkiller SMTP virtual server to forward all unresolved recipients to 10.1.100.50. Create a dedicated SMTP connector that uses the existing virtual server. Forward all mail going through this connector to 10.1.100.50. Add contoso.com as an address space on this connector.

Answer: B
Explanation
We need to forward non Exchange mail recipients for the *.contoso.com name space to the Unix server. We can achieve this by using a second connector in a second virtual using an SMTP for *.contoso.com on the bridgehead server because BH1 just is configured with an SMTP connector for all Certkiller Internet e-mail. We need to reroute *.contoso.com name space also take care about this Exchange System Manager only accepts entries with an asterisk at the beginning, similar to "*.microsoft.com".

QUESTION 23

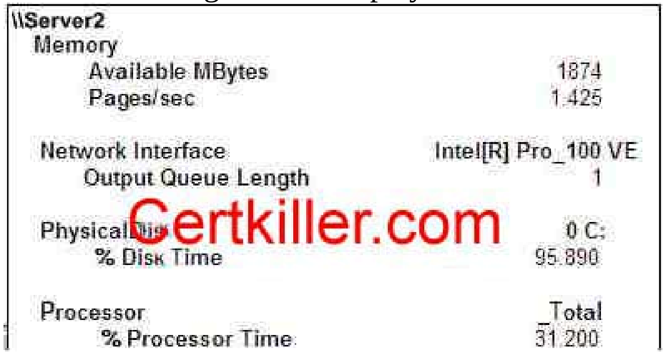
You are the Exchange administrator for Certkiller . Exchange Server 2003 runs on a Microsoft Windows Server 2003 member server named Server2. The server is a quad-processor, 2-2-GHz computer with 4 GB of RAM and RAID-5 disk array that has 550 GB of disk storage. All Exchange binary files, log files, and database files are located on drive C.

During the peak-usage times, the server supports 1,600 active Microsoft Outlook 2002 users. The Outlook 2002 client computers are configured as MAPI clients.

Users report that Outlook often takes 10 seconds or more to send a message that are 1 K or less in size.

You run System Monitor logging for three hours during the time users report performance problems.

You record a log file and display the results in the following report.



```
\\Server2
   Memory
          Available MBytes                         1874
          Pages/sec                                1.425

   Network Interface                     Intel[R] Pro_100 VE
         Output Queue Length                          1

   PhysicalDisk                                    0 C:
           % Disk Time                           95.890

   Processor                                     _Total
           % Processor Time                      31.200
```

You need to improve Outlook response time for sending messages as much as possible.

What should you do?

A. Add 2 GB of additional RAM to Server2.

B. Increase the size of the TCP sliding window.

C. Move the transaction log files to a new physical hard disk.

D. Set the processor affinity for the Microsoft Exchange Information Store service to the fourth processor.

Answer: C

Explanation:

The percent Disk Time is an indicator of the amount of time the hard disk is queuing items. A high number is an indication that the hard drive subsystem is being overworked. Moving the transaction log files to a new physical hard disk will alleviate a disk bottleneck

Incorrect answers:

A. Adding RAM would lessen the stress on the Memory subsystem. Looking at the exhibit, the available memory is still 1874MB, which is ample for running Exchange Server.

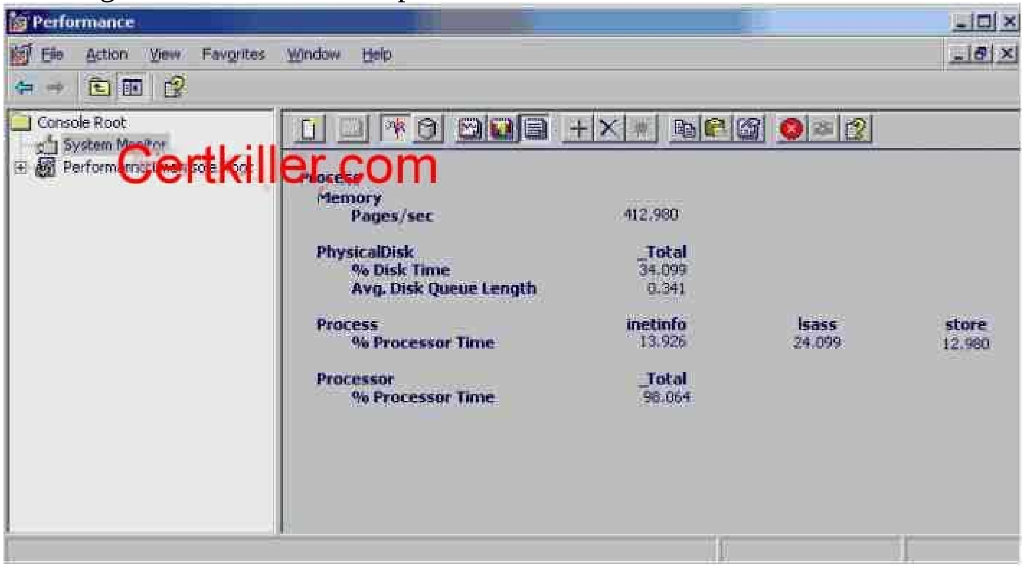
B. Increasing the size of the TCP sliding window is used to improve network communications. Since the output queue length is one, manipulating the TCP/IP settings in any way is not necessary.

D. Setting the processor affinity would put more emphasis on one processor over another. Since the processor time is relatively low (anything under 80% is acceptable), this is not an issue.

QUESTION 24

You are the Exchange administrator for Certkiller . The main office has 5,700 users. A total of 1,500 users work in 70 different branch offices. All branch offices are connected to the main office by WAN connections.

The Exchange organization contains four servers that run Exchange Server 2003. Each Exchange server contains 1,800 mailboxes. All Exchange severs are located in the main office and are configured as Microsoft Outlook Web Access servers. Only SSL connections are accepted for Outlook Web Access. Branch office users connect to the Exchange servers by using Outlook Web Access. They report unacceptably slow response times when they access the servers. You use System Monitor on one Exchange server to collect the performance data shown in the exhibit.



```
Memory
     Pages/sec                      412.980

PhysicalDisk                        _Total
     % Disk Time                    34.099
     Avg. Disk Queue Length         0.341

Process                             inetinfo     lsass      store
     % Processor Time               13.926       24.099     12.980

Processor                           _Total
     % Processor Time               98.064
```

You need to optimize the performance of Outlook Web Access for branch office users.
What should you do?

A. Install additional RAM on each Exchange server.
B. Install additional physical disk on each Exchange server. Move the paging file to the new disk.
C. Install an additional Exchange Server 2003 computer. Configure the new server for SSL and configure it as a front-end server. Instruct all branch office users to use the new server for Outlook Web Access.
D. Install an additional Exchange Server 2003 computer. Move all mailboxes for branch office users to the new server. Configure the new server for SSL. Instruct all branch office users to use the new server for Outlook Web Access.

Answer: C

Explanation:
The need for a second server for SSL would come if the processor usage is high. Since the processor is almost maxed out (98%), there is an indication that a second server (or a second processor) would be needed to offload the SSL work.
Incorrect answers:

A. Looking at the performance counters, it is apparent that the number of pages per second is high (412.980). Exchange makes heavy use of the paging file, and a high number of pages in and of itself does not indicate a performance issue. Therefore, this counter MUST NOT be used alone in determining problems. For this reason, this is not the best answer.
B. Adding a physical disk will not help much. The percent disk time is relatively low (34%), so the workload on the hard drives is minimal

D. Moving all the mailboxes to the new server, configuring it for SSL, and having all OWA users' use the new server effectively takes the first server out of operation. The problem would simply shift to the new server, while leaving the old server without much to do. This is not the optimal solution, as one server is effectively wasted.
Reference:
Exchange Server 2000 Server Operations Guide, Section 4 - Performance Monitoring
http://www.microsoft.com/technet/prodtechnol/exchange/2000/maintain/e2kops4.mspx

---

QUESTION 25
You are the Exchange administrator for Certkiller .
The Exchange organization contains three servers that run Exchange Server 2003.
All users send and receive e-mail messages by using Microsoft Outlook.
One Exchange server is configured as a bridgehead server for Internet e-mail.
The other two servers are configured as mailbox servers.
Each mailbox server contains one storage group that contains one public store and two mailbox stores.
Each mailbox server has two CPUs and 1 GB of RAM.
Users report that Outlook requires more than one minute to open.
Each e-mail message requires more than two minutes to send or open.
You monitor the mailbox servers and discover that the primary bottleneck is insufficient RAM. You add an additional 1 GB of RAM to each mailbox server. Users report no change in the performance of Outlook.
You need to modify each mailbox server to maximize its performance.
What should you do?

A. Add the switch that enables physical address extensions to the Boot.ini file.
B. Add the switch that increases user mode memory usage to the Boot.ini file.
C. Add an additional physical disk and move the paging file to the new disk.
D. Create an additional mailbox store and move half of the existing mailboxes to the new mailbox store.

Answer: B
If you have more than 1 GB of physical memory installed on a server that is running Exchange Server 2003, you must make sure that Exchange Server 2003 can make efficient use of that memory.
If you are running Exchange Server 2003 on a Windows Server 2003-based computer, and if the /3GB switch is set, Microsoft recommends that you set the /USERVA=3030 parameter in the Boot.ini file. This configuration option increases the virtual address space.
Incorrect answers:

A. The /PAE switch lets developers perform similar testing of device drivers by forwarding 64-bit addresses to kernel-mode components. This feature is known as Physical Address Extension (PAE), and it may not work on all chip sets.
C. Adding a hard drive will not resolve the problem. In this case, the problem is coming from an incorrect memory configuration.
D. This answer is not relavant, as front-end servers do not have mailboxes configured on them.

QUESTION 26
You are the Exchange administrator for Certkiller . The Exchange organization contains five servers that

run Exchange Server 2003. There are 1,200 users at Certkiller .
An Exchange server named OWA1 is configured as a front-end server running Microsoft Outlook Web Access. OWA1 requires SSL for all client connections. A pilot group of users currently uses Outlook Web Access to send and receive e-mail messages. Over the next two months, you plan to make Outlook Web Access incrementally available to all users.
You need to collect server performance data on OWA1. You will use the data to forecast when you might need to upgrade the hardware on OWA1.
What should you do?

A. Use System Monitor to monitor the Exchange store.
B. Use Task Manager to monitor network utilization.
C. Use Exchange System Manager to configure an e-mail notification that will send you an e-mail message whenever CPU usage exceeds 80 percent for five minutes.
D. Use Performance Logs and Alerts to configure a counter log to monitor CPU and memory usage.
E. Use Performance Logs and Alerts to configure an alert that will log an entry in the application event log whenever memory usage exceeds 80 percent of available memory.

Answer: D

Explanation:
The only answer that allows for the LOGGING of data is choice D. The question specifically states that you need to collect data and forecast when a hardware upgrade may be needed. In order to do that, any data collected must be logged.
Incorrect answers:
A, B. Monitoring the Exchange Store will not give the necessary logging of information. All that can be done is looking at the current data. Trends can't be spotted, and this data can't be presented to anyone to forecast what may happen.
C. Sending an email notification can't be used to forecast trends unless each and every email is kept for comparison purposes. While this can be done, there is no mention of doing this in the question, and is not the optimal solution.
E. Placing an event in the event log is a good idea, and can help in determining a necessity for an upgrade. However, memory usage is only one counter that could indicate a need for a hardware upgrade. If the CPU is overworked, for example, there will be no entry in the log to reflect this, but there would still be a need for a faster processor. Since there is a "hole" in this answer, it is not the best answer.

QUESTION 27
You are the Exchange administrator for Certkiller .
The Exchange organization contains three servers that run Exchange Server 2003.
All users access e-mail by using Microsoft Outlook. Last year there were 5,000 users at Certkiller .
Over the past year, the number of users increased by 15 percent, to its current level of 5,750.
Response time for Outlook increased significantly as the number of users increased.
Currently, some users report that Outlook requires more than three minutes to open and that each email message requires an additional two minutes to open.
However, less than 10 percent of network bandwidth is in use.
Current projections indicate that the number of users will increase by 25 percent within one year.
Management asks you whether upgrading the Exchange servers will prevent further degradation in

Outlook performance.
You need to gather additional data in order to reply.
Which data should you monitor?

A. Usage of processor, memory, and disk space on each Exchange server.
B. Usage of processor and memory on each global catalog server.
C. Length of the SMTP queue on each Exchange server.
D. Number of messages sent to recipients inside and outside the Exchange organization.

Answer: A

Explanation:
Usage counters on the Exchange server will be the best determination of load on the Exchange server. Since the network usage is not a problem, the issue must lie in the hardware. The most logical place for the problem will be in the Exchange server itself. In addition, Microsoft recommends not having more than 5000 users on an Exchange server. This is a clear indication that the server needs to be addressed.
Incorrect answers:
B. Viewing the Global Catalog server counters would be all but useless. While Exchange makes use of the GC, there are many other items that rely on it as well. Monitoring the usage on that server will tell very little about the Exchange environment.
C. The SMTP queue on each server is valuable in determining how long messages wait to be delivered. A long queue is an indication that there is a network or hardware problem, but monitoring it alone will not give information on server hardware statistics, and hence what hardware may need to be purchased to upgrade the server.
D. The number of messages sent to recipients will have no bearing on the server hardware load all by itself. It would require additional hardware counters to fully determine what is causing the degradation. Even if the number of messages has drastically increased, if the server has enough hardware to support it (this would only be determined by looking at the counters specified in answer "A") then it's not a problem for the server to handle the increased work load.
Reference
Troubleshooting Microsoft Exchange 2000 Server Performance
Microsoft Exchange 2000 Front-End Server and SMTP Gateway Hardware Scalability Guide

---

QUESTION 28
You are the Exchange administrator for Certkiller .
Exchange Server 2003 runs on two Microsoft Windows Server 2003 computers.
Each Exchange server contains one mailbox store.
Written Certkiller policy states that a copy of each e-mail message that is sent and received by every user in the auditing department must be kept for five years.
You need to ensure that only the auditing department e-mail meets this requirement.
Which two actions should you perform? (Each correct answer presents part of the solution. Choose two)

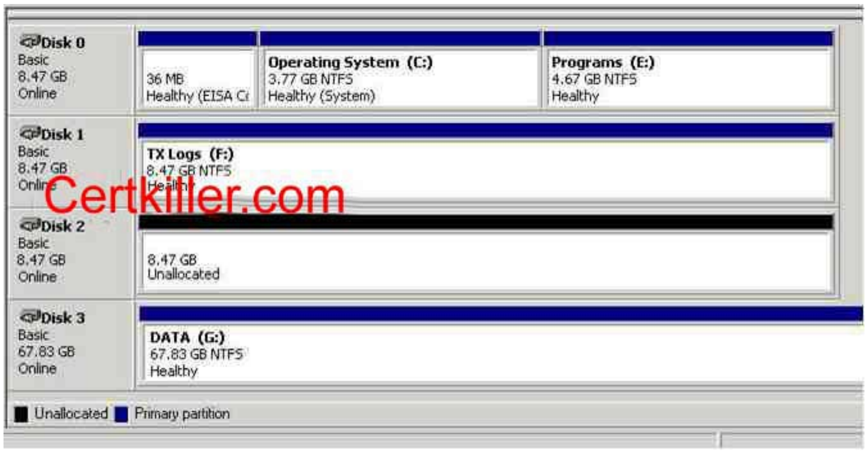
A. Configure the auditing department's mailbox store to archive all e-mail messages.
B. Create an additional mailbox store and move all auditing department mailboxes to that mailbox store.
C. Create a recipient policy that manages mail retention for all users in the auditing department.
D. Create a recipient policy that manages the auditing department's mailbox store and does not purge the

users' Inbox folder or Sent Items folder for five years.

Answer: A, B

Explanation:
They tell us Each Exchange server contains one mailbox store.
To be able to apply the retention just to user's of auditing department you will need to create a new mailbox store and move all the users in auditing department to the new mailbox store
The Message Journaling function is a new feature introduced in Microsoft Exchange 2000 Server. You can enable this function on a per-mailbox store object basis.
Incorrect answers:
C You can't apply a recipient policy to all the users.
D You can't specify the time for the retention in a system policy to a mailbox store, but you can apply the time for retention to deleted items and mailboxes not to the messages that are in the mailbox used to keep all the messages
Reference
XADM: How to Enable the "Message Journaling" Function for an Exchange Server Mailbox Store KB 261173

QUESTION 29
You are the Exchange administrator for Certkiller .
The network contains an active/passive Exchange Server 2003 cluster that contains two nodes named Exchange1 and Exchange2.
The cluster contains an Exchange Virtual Server (EVS) named Exch1.
Exch1 contains two storage groups named SG1 and SG2.
Each storage group contains two mailbox stores.
The written company policy states that the most current data must be restored in the in the event of a database restore.
Exch1 stores its transaction log files and databases on a Storage Area network.
The relevant Storage Area Network disks, Disk 1, Disk 2, and Disk3, are configured as shown in the exhibit.



Disk 0 Basic 8.47 GB Online	36 MB Healthy (EISA Co	**Operating System (C:)** 3.77 GB NTFS Healthy (System)	**Programs (E:)** 4.67 GB NTFS Healthy
Disk 1 Basic 8.47 GB Online	**TX Logs (F:)** 8.47 GB NTFS Healthy		
Disk 2 Basic 8.47 GB Online	8.47 GB Unallocated		
Disk 3 Basic 67.83 GB Online	**DATA (G:)** 67.83 GB NTFS Healthy		

■ Unallocated ■ Primary partition

A RAID-protected array is dedicated for the mailbox stores.
The array that contains the mailbox stores uses 37 GB of disk space on drive G.
There are 30 GB of available disk space on drive G.
A mirrored pair of disks is dedicated for the transaction log files.

The transaction log files routinely use approximately 8 GB of disk space on drive F before nightly backups are performed.
You need to ensure that there is sufficient space for the transaction log files and that highly availability is maintained.
What are two possible ways to achieve this goal? (Each correct answer presents a complete solution. Choose two)

A. Create a partition on Disk 2 and format it as drive H. Add this disk as a cluster resource. Move the transaction log files for SG2 to drive H.
B. Create a partition on Disk 2 and format it as a volume mount point to drive F. Add this disk as a cluster resource. Place the transaction log files for SG2 on this mount point.
C. Create a partition on Disk 2 and format it has drive H. Add this disk as a cluster resource. Move the transaction log files for SG2 to drive E. Move the database files for SG2 to drive H.
D. Create a partition on Disk 2 and format it as a volume mount point to drive E. Add this disk as a cluster resource. Place the transaction log files for SG2 on this mount point.

Answer: A, B

Explanation:
Non shared disk (disk E) can not be made a cluster resource in the first place
Volume mount point created on disk 2 (shared disk) and mounted on a shared disk (Drive F) gives an addiitonal 8 GB of disk space for logs. 8 GB for SG1, and 8 GB for SG2 logs
High availability is maintained since new disk - Disk 2 is also added as a cluster resource.

QUESTION 30
You are the Exchange administrator for Certkiller .
The Exchange organization contains 12 Exchange servers with a single administrative group.
All exchange servers run Exchange Server 2003.
Each Exchange server contains for mailbox stores.
The written company e-mail policy specified a maximum amount of e-mail storage that each user is allowed to use.
You need to ensure that the e-mail storage restrictions are consistently applied on all Exchange mailbox stores in the organization.
You need to achieve this goal by using the minimum amount of administrative effort.
What should you do?

A. Apply global message delivery options that define maximum message sizes.
B. Define mailbox store size limits for each mailbox store on all Exchange servers.
C. Configure a Mailbox Manager recipient policy that applies to all users in the organization.
D. Create a mailbox store policy that defines storage limits. Apply the policy to all mailbox stores.

Answer: D

Explanation:
You need to ensure that the e-mail storage restrictions are consistently applied on all Exchange mailbox stores in the organization.

Incorrect Answers

A. Apply global message delivery options that define maximum message sizes. Do not define the limits
B. Define mailbox store size limits for each mailbox store on all Exchange servers. Is more time consuming that configured a general policy to apply to all mailbox stores
C. Configure a Mailbox Manager recipient policy that applies to all users in the organization. Trick in the term Mailbox Manager recipient policy
Reference
HOW TO: Use System Policies to Configure Mailbox Storage Limits in Exchange Server 2003 KB 822938

QUESTION 31
You are the Exchange administrator for Certkiller .
Exchange Server 2003 runs on a Microsoft Windows Sever 2003 member server.
The Exchange server contains one mailbox store and one public folder store.
A free disk space warning threshold is configured for the Exchange server.
However, when the amount of free disk space is below the threshold, the help desk mailbox does not receive an e-mail notification.
You need ensure that the help desk is notified if the server's free disk space is below the specified threshold.
What should you do?

A. Configure an e-mail notification to occur when free disk space is in a warning state.
B. Configure the server's mailbox management process to send summary reports to the help desk.
C. Configure the help desk's e-mail address as the non-delivery report (NDR) address on the SMTP virtual server.
D. Configure the warning message intervals on the mailbox store and the public folder store to use a custom schedule that allows notification 24 hours per day, seven days per week.

Answer: A

Explanation:
You can send an e-mail message to an administrator when a server or connector enters a warning state or critical state. The server and connector states are set on the Monitoring tab of a server or connector. The subject line and body of the e-mail message are automatically created; their content depends on which server is monitoring the servers and connectors in your organization, and which servers and connectors are being monitored. However, if problems exist between the monitoring server and the server or connector being monitored, the message may not be delivered.
Reference
Exchange 2003 Server Help

QUESTION 32
You are the Exchange administrator for Certkiller .
Exchange Server 2003 is the messaging system.
The Exchange organization includes a two-node active/active server cluster that provides failover capabilities for each of the two Exchange Virtual Servers (EVSs).
You need to ensure that the cluster will automatically balance the two EVSs evenly across both cluster

nodes, as long as both nodes are operational.
You must not remove the existing failover capabilities.
Which two actions should you perform? (Each correct answer presents part of the solution. Choose two)

A. Configure failover for each EVS.
B. Configure failback for each EVS.
C. Configure a single preferred node for each EVS.
D. Configure a single possible node for each EVS.
E. Configure the quorum disk resource so that it does not affect the cluster resource group when a failure occurs.

Answer: B, C
Explanation
In server clusters, failover is the process of taking resource groups offline on one node and bringing them online on another node. When failover occurs, all resources within a resource group fail over in a predefined order; resources that depend on other resources are taken offline before, and are brought back online after, the resources on which they depend. If an individual application in a server cluster fails (but the node does not), the Cluster service typically tries to restart the application on the same node. If that fails, it moves the application's resources and restarts them on another node of the server cluster. This process is called failover
When a node becomes inactive for any reason, the Cluster service fails over any groups hosted by the node. When the node becomes active again, the Cluster service can fail back the groups originally hosted by the node. The Cluster service fails back a group using the same procedures it performs during failover. That is, the Cluster service takes all of the resources in the group offline, moves the group, and then brings all of the resources in the group online. This is called Failback.
You can set failback to occur during a specific time period. It is important to set the failback time because you may not want failback to occur during hours of peak usage.
Reference:
Exchange 2003 Administration guide

QUESTION 33
You are the Exchange administrator for Certkiller .
The network contains an Exchange Server 2003 active/passive cluster that contains nodes named Certkiller SrvA and Certkiller SrvB.
The cluster contains a single Exchange Virtual Server (EVS).
Certkiller SrvA is the preferred owner of the EVS.
Certkiller SrvA has intermittent hardware failures that cause it to go offline.
When Certkiller SrvA goes offline, the EVS fails over to Certkiller SrvB.
You need to change the cluster configuration so that the EVS remains online while you troubleshoot the cause of the hardware failure.
What should you do?

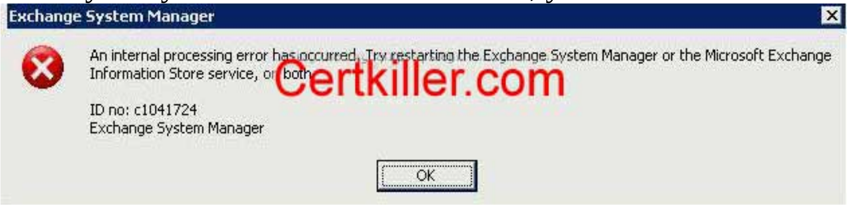
A. In Cluster Administrator, select the option to move the cluster group to Certkiller SrvB.
Remove Certkiller SrvA as a possible failover node.
B. In Cluster Administrator, select the option to move the cluster group to Certkiller SrvB.
Select the option to prevent failback to Certkiller SrvA.
C. Create a new cluster group.

Move all the Exchange cluster resources to the new cluster group.
Select Certkiller SrvA and Certkiller SrvB as the preferred owners of the cluster, and ensure that Certkiller SrvA is selected at the top of the possible owners list.
D. Create a new cluster.
Move all the Exchange cluster resources to the new cluster group.
Select the option to prevent failback to Certkiller SrvA.

Answer: B
Explanation
Specifying Preferred Owners
During the creation of an Exchange Virtual Server, you have the option of defining a list of preferred cluster nodes or preferred owners for that server. Cluster Service uses this list of preferred owners when assigning the Exchange Virtual Server to a node. Cluster Service first tries to assign the Exchange Virtual Server to the first node in the list. If that node is unavailable, Cluster Service tries the next node in the list. If that node is unavailable, Cluster Service continues down the list, until it can assign the Exchange Virtual Server to a node. If Cluster Service cannot find an available node in the preferred owners list, it tries to fail over to the other available nodes in the cluster that have Exchange installed.
By default, you do not have to specify any preferred owners. If you do not specify owners, Cluster Service assigns an Exchange Virtual Server to the next available node that has Exchange installed.
You have the option of preventing failback from occurring automatically (the default), or allowing failback to occur automatically.
If you do not allow an Exchange Virtual Server to fail back, you must intervene and manually move the server back to the original, preferred node.
This may be your preferred setting because it allows you to control when the failback occurs. For example, you may want to select Prevent failback if you want to take time to troubleshoot or run diagnostics on the failed node before allowing the node to take ownership of the Exchange Virtual Server again.
You can also use this setting to minimize downtime for users. For example, consider a scenario where a failover that occurs at 3:00 P.M. causes EVS1 to move from Node 1 to Node 4 (the stand-by node). By preventing failback, you can wait until the end of the work day to manually move EVS1 back to Node 1, and users do not have to experience downtime waiting for the server to come back online after the move.
By allowing an Exchange Virtual Server to fail back to the preferred node automatically, you can also specify when this failback should happen: either immediately or during a specified time interval.
This is the preferred setting if you want to have Cluster Service manage the cluster without any manual administrator intervention.

QUESTION 34
You are the Exchange administrator for Certkiller .
The Exchange organization contains a server named Exch1 that runs Exchange Server 2003. Exch1 contains a single storage group with a single mailbox store.
The storage group stores transaction logs on E:\Exchsrvr\Mdbdata.
The mailbox store is located on F:\Exchsrvr\Mdbdata.
The disks on the Exchange server fail.
All the disks for drive E and drive F are replaced.
You attempt to mount the mailbox store.
You acknowledge the message and create new mailbox store files.
Then you restore the mailbox store from a tape backup and configure C\Temp as the location for the

transaction log files.
When you try to mount the mailbox store, you receive the following error message.



Exchange System Manager

An internal processing error has occurred. Try restarting the Exchange System Manager or the Microsoft Exchange Information Store service, or both.

ID no: c1041724
Exchange System Manager

You need to ensure that the mailbox store mounts successfully with the restored data.
Which three actions should you perform before mounting the store? (Each correct answer presents part of the solution. (Choose three)

A. Delete the transaction log files from C:\Temp.
B. Delete the Restore.env file from C:\Temp.
C. Delete the transaction log files from E:\Exchsrvr\Mdbdata.
D. Delete the checkpoint file from E:\Exchsrvr\Mdbdata.
E. Run the eseutil /cc command against the files in C:\Temp.
F. Run the eseutil /d command against the restored mailbox store.

Answer: C, D, E

Explanation:
This is on basis of what needs to be done before the eseutil /cc.
Since we mounted a new database and created new log files that have nothing to do with the restore we are performing - we need to delete the log files from the production folder (not the temp path) - since the new log file numbers could be the same and may interfere with the replaying of the logs.
Prior to mounting the databases in the storage group to initiate transaction log replay, the current checkpoint file (E0n.chk) must be renamed, or deleted, so that all logs can be played.
eseutil /d does a defrag. We need to do eseutil /cc to initiate hard recovery - this is the same as checking last restore set option.

QUESTION 35
You are the Exchange administrator for Certkiller .
The Exchange organization contains a single Exchange Server 2003 computer named Certkiller 1.
Certkiller 1 contains a single storage group that has two mailbox stores.
Occasionally, a user deletes a message and later wants the message to be restored.
The written company policy allows users to retrieve deleted messages for 30 days after they are deleted.
Certkiller 1 connects to a Storage Area Network where the mailbox store databases and transaction log files are stored. Currently, 80 GB of disk space is available to Exchange on the Storage Area Network.
You need to ensure that users can retrieve deleted messages according to company requirements. You need to achieve this goal by using the minimum amount of administrative effort.
What should you do?

A. Create a daily shadow copy of the mailbox store databases.
B. Perform incremental backups of the mailbox store databases Monday through Saturday. Perform a full backup of the mailbox store databases Sunday night. Place all the mailbox store database backups on the Storage Area Network.

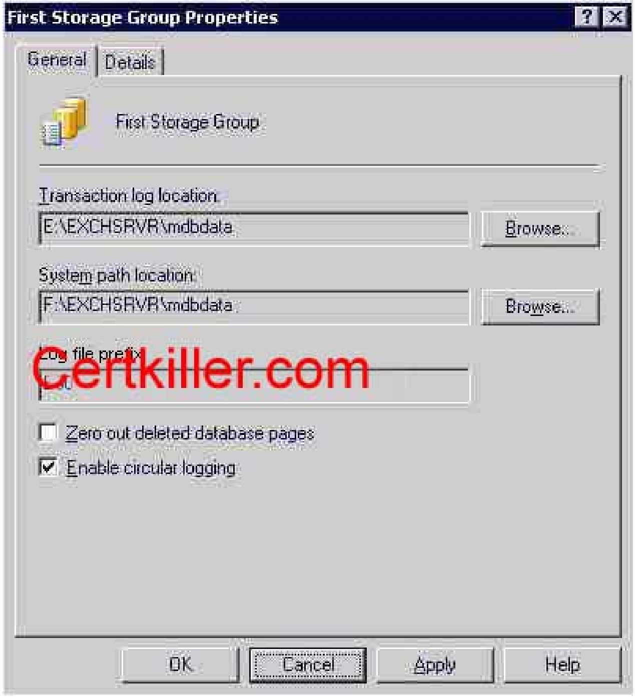
C. Create a mailbox store policy and select the option to keep deleted messages for 30 days. Add each mailbox store database to this policy.
D. Create a recipient policy and select 30 days as the age to process deleted items for all message sizes for all users.

Answer: C

Explanation:
Creating a mailbox store policy is the simplest administration method. It can be applied to multiple stores with minimal intervention. In addition, setting the deleted item retention option is an available option within this policy.
Incorrect answers:

A. Creating a daily shadow copy will work, but it will take more effort, and require a great deal of storage space. While this is a viable answer, it is not the best answer.
B. Performing backups of any type require a lot of manual intervention. This violates the requirement of using the least administrative effort.
D. Recipient policies do not allow for the retention of deleted items. This is a mailbox storage policy. Therefore, this answer is not correct.

QUESTION 36
You are the Exchange administrator for Certkiller .
The network contains a single Exchange Server 2003 computer.
The Exchange server contains one storage group and one mailbox store.
Full backups of the mailbox store and transaction log files are performed every night.
After the mailbox store is restored from tape, users report that some of their e-mail messages are not restored.
You discover that the storage group is configured as shown in the exhibit.



First Storage Group

Transaction log location:
E:\EXCHSRVR\mdbdata

System path location:
F:\EXCHSRVR\mdbdata

Log file prefix:

☐ Zero out deleted database pages
☑ Enable circular logging

You need to ensure that after you restore the mailbox store, users have all of the most current data.
What should you do?

A. Zero out deleted database pages after you perform a restore operation.
B. Disable circular logging before you perform a backup.
C. Perform only shadow copy backups and shadow copy restore operations.
D. Create a mailbox store policy. Select the option to keep deleted messages for 30 days. Add the mailbox store to this policy.

Answer: B

Explanation:
Circular logging is used to minimize the amount of storage space required for log files. The issue with this however, is that in the event of a restore, only the database is restored. Since all the log files are not available, no transactions still in the logs at the time of the last backup will be restored.
Incorrect answers:

A. Zeroing out" sets a variable value or a series of bits to zero. Zeroing out deleted database pages allows Exchange Server to reuse previously created data pages. You can control the zeroing out of database pages at the storage group level. Each storage group can have a different policy for zeroing out deleted database pages. If you click this option, security is increased because deleted database pages are overwritten on the hard disk with zeros. This is the exact opposite of what needs to take place.
C. Performing shadow copy backups and restores is not sufficient, as the data is sensitive to the time of the last backup. Running the backup continuously is not an option. Therefore, there is a high likelihood that some data will be lost between the last backup and the time of the problem that causes the need for recovery.
D. Setting a deleted item retention policy will not resolve the issue. The problem stems from the fact that at any time, there are transactions waiting to be written from the transaction log to the database. The messages that would not be restored in the event of a recovery are not the deleted items, but instead the items in the transaction logs that have not been written to the database.
Reference:
MS-Exchange 2003 Help
HOW TO: Turn On or Turn Off Circular Logging in Exchange 2003 Server Article - 314605

QUESTION 37
You are the Exchange administrator for Certkiller .
Certkiller hosts Exchange e-mail for other companies.
The service level agreement (SLA) for a customer named Trey Research states that failed Exchange mailbox stores must be online again in one hour or less.
The SLA also states that all e-mail data must be retained for one year.
Trey Research uses two mailbox stores named MBX01, and MBX02.
Both mailbox stores reside on a Storage Area Network.
MBX01 is 25 GB in size and MBX02 is 22 GB in size.
There is 153 GB of available disk space on the Storage Area Network for Trey Research data.
You can back up or restore Trey Research mail at a rate of 12 GB per hour.
You need to ensure that you can meet the SLA requirements for the Trey Research mailbox stores.

What should you do?

A. Every night, perform full backups to tape and archive them. Then perform a shadow copy backup to the Storage Area Network.
B. Perform full backups to tape on Saturday night and archive them. Perform differential backups to tape every Sunday through Friday night.
C. Perform full backups to tape on Saturday night and archive them. Perform differential backups to tape every Sunday through Friday night.
D. Perform full backups to tape on Saturday night and archive them. Perform incremental backups to tape every Sunday through Friday night.

Answer: A
They tell us there is 153 GB of available disk space on the Storage Area Network for Trey Research data.
By default, when you perform a backup in Windows Server 2003, the volume shadow copy method is used to create the backup. Shadow Copies and full backups made every night and archived would allow us to meet the SLA requirements.
However, the Exchange 2003 Writer supports only a Full backup at the storage group (SG) level.
VSS performs Exchange Full backups at the SG level, even though the Exchange Writer treats individual databases as separate components.
VSS uses the AddComponent call to add each database component to the Shadow Copy set, which in the case of a Full backup, is the entire SG (i.e., databases or log files).
In a Full backup of a SG, VSS creates a complete Shadow Copy of all volumes-the Shadow Copy contains database and transaction log files associated with that SG.
In addition, as is the case with non-VSS Full backups, VSS truncates the transaction log files after successfully creating and backing up the Shadow Copy.
To truncate the transaction log files, the Shadow Copy set must include all databases
Although VSS backup for Exchange 2003 is at the SG level, you can recover individual databases from the SG Shadow Copy set.
VSS-based restoration of an Exchange 2003 SG is useful when data in one or more databases in the SG is lost or corrupted, but the current log files remain intact on disk; when the current log files on disk are lost or corrupted, but the databases remain intact; or when databases and current log files within an SG are lost or corrupted.
References:
Overview of Dependencies and Requirements for Exchange Server 2003 Features 822178
Exchange Server 2003 Data Back Up and Volume Shadow Copy Services 822896

QUESTION 38
You are the Exchange administrator for Certkiller .
The Exchange organization contains a single server that runs Exchange Server 2003.
The Exchange server contains one storage group and one mailbox store.
You discover that the mailbox store is corrupted and will not mount.
You need to ensure that you restore the most current data possible.
What should you do?

A. Create the Recovery Storage Group. Set the path to the same as the path for the existing mailbox store.
B. Create the Recovery Storage Group. Set the database path to C:\Program Files\Exchsrvr\Recovery

Storage Group.
C. Restore the mailbox store and then mount the mailbox store.
D. Delete the database and transaction log files. Then mount the mailbox store.

Answer: C

Explanation:
The told us that mailbox store is corrupted and will not mount. The use of Recovery Storage Group is not for this case. Recovery Storage Group is a solution to be used to recover individual user mailbox and use exmerge to mix the data with the corrupted mailbox. Recovery Storage Group feature, you can mount a second copy of an Exchange mailbox store (database) on the same computer as the original mailbox store, or on any other Exchange computer that is in the same administrative group.
If we need to deal with an Exchange server that just contains one storage group and one mailbox store, we need to restore the database form backup to be able to mount it, of course there is the tricky statement that told us You need to ensure that you restore the most current data possible., but we can't use the actual database or log because are already corrupted
Reference
HOW TO: Recover or Restore a Single Mailbox in Exchange Server 2003 KB 823176
How to Use Recovery Storage Groups in Exchange Server 2003 KB 824126
Using Exchange Server 2003 Recovery Storage Groups MS White Paper

---

QUESTION 39
You are the Exchange administrator for Certkiller .
The Exchange organization contains a single Exchange Server 2003 computer named Exch1. Exch1 contains one storage group and one mailbox store.
You build an Exchange server in your lab to test the defragmentation utilities against the Exchange store.
The Exchange data you are currently using in the lab is two months old.
You want to use the most current data on the lab server.
You perform a full backup of the data on Exch1 every night.
You obtain a second tape with a full backup for the lab environment.
You need to ensure that the lab server contains the most current copy of the data from Exch1. You must maintain the existing backup rotation schedule on Exch1.
What are two possible ways to achieve this goal? (Each correct answer presents a complete solution. Choose two)

A. Perform a full backup of the Exch1 data to the second tape. Restore this data to the lab server.
B. Perform a copy backup of the Exch1 data to the second tape. Restore this data to the lab server.
C. Perform a differential backup of the Exch1 data to the second tape. Use this tape with the most recent full backup to restore the production data to the lab server.
D. Perform an incremental backup of the Exch1 data to the second tape. Use this tape with the most recent full backup to restore the production data to the lab server.

Answer: B, C
Explanation
You can perform four types of online backups on the Exchange store:
• A full backup (called a normal backup in Windows Backup) backs up the store and transaction

log files. After the backup, transaction log files in which all transactions are complete are deleted.

- A copy backup backs up the store and transaction log files, but leaves the transaction logs in place.
- An incremental backup backs up the transaction logs and removes all transaction logs in which all transactions are completed.
- A differential backup backs up the transaction logs, but leaves them in place.

Reference
Exchange Server 2003 Administration Guide

QUESTION 40
You are the Exchange administrator for Certkiller .
The Exchange organization contains a single Exchange Server 2003 computer.
The Exchange server contains one storage group that has three mailbox stores.
Each mailbox store contains 200 mailboxes.
Certkiller 's service level agreement (SLA) requires that Exchange must not be offline for more than four hours.
The SLA requires that in the event of data corruption, the most current data must be restored.
You want to test the recovery process on the existing Exchange server after business hours.
You need to ensure that the mailbox stores can be restored within four hours without losing the current production data.
What should you do before performing the test restore operation?

A. Create a new storage group that contains three mailbox stores. Select the option to allow the mailbox stores to be overwritten by a restore operation.
B. On the existing mailbox stores, select the option to allow the mailbox stores to be overwritten by a restore operation.
C. Create the Recovery Storage Group and add the three mailbox stores. Configure the Recovery Storage Group to use the default Recovery Storage Group path for each of the mailbox stores.
D. Create the Recovery Storage Group and add the three mailbox stores. Configure the Recovery Storage Group to use the existing database path for each of the mailbox stores.

Answer: C

Explanation:
Setting up a recovery storage group involves two basic steps: creating the recovery storage group and adding the databases to be restored. This process creates the logical structures that Microsoft(r) Exchange Server 2003 uses to manage the restored data. Restoring the content of the databases is a separate process,
The Recovery Storage Group feature in Microsoft(r) Exchange Server 2003 allows you to mount a second copy of an Exchange mailbox database on the same server as the original database, or on any other Exchange server in the same Exchange administrative group. This can be done while the original database is running and serving clients. This capability allows you to recover data from an older backup copy of the database without disturbing user access to current data.
Recovery storage groups were designed to aid in database recovery under the following conditions:

- The logical information about the storage group and its mailboxes remains intact and unchanged in Microsoft(r) Active Directory(r) directory service.

• In addition, you need to recover a single mailbox, a single database, or a group of databases in a single storage group. Recovery scenarios include:
• Recovering deleted items that a user mistakenly purged from their mailbox.
• Recovering or repairing an alternate copy of a database while another copy remains in production (typically, with the goal of merging data between the two databases using the ExMerge tool).
• Recovering a database on a server other than the original server for that database. If needed, you can then merge the recovered data back to the original server (although performance would be slower than if the recovery storage group and the original database were on the same server).
Incorrect Answers:
A, B: They want to test the recovery process on the existing Exchange server after business hours.
You can't put online same user mailbox in any mailbox sore in any storage group because both will have same mailbox GUID is the most fundamental attribute of a mailbox. The value of this attribute is set in the database as the mailbox is created, and the value remains the same for the lifetime of the mailbox. It is a unique value that distinguishes a mailbox from all others. Deleted or purged mailboxes cannot easily be recovered in the recovery storage group because deleting a mailbox strips all mailbox attributes from the Active Directory user object that previously owned the mailbox.
D: If the original storage group does not exist on the server on which you are creating the recovery storage group, the recovery storage group must have the same name as the original storage group. For example, if you are creating the recovery storage group on a recovery server that has no other storage groups, the recovery storage group must have the same name as the original storage group.
If the original storage group exists on the server on which you are creating the recovery storage group, the recovery storage group must have a different name. For example, if you are creating the recovery storage group on the server where the original database and storage group reside, the recovery storage group can have any name (other than the names that have already been used).
Reference
Using Exchange Server 2003 Recovery Storage Groups MS White Paper

---

QUESTION 41
You are the Exchange administrator for Certkiller .
The Exchange organization contains a single new Exchange Server 2003 computer.
The Exchange server contains one storage group and one mailbox store.
You create mailboxes on the new mailbox store.
At the end of the day, before your first backup job has run, the disk controller fails.
You replace the disk controller.
You discover that the mailbox store is corrupted.
You also discover that the mailbox store is dismounted.
You need to ensure that you can mount the mailbox store with the minimum amount of data loss.
What should you do?

A. Run the exchdump command. Then run the isinteg -fix command to repair the mailbox store.
B. Move the files in the transaction log folder to a safe location. Run the isinteg -fix command to repair the mailbox store.
C. Move the files in the transaction log folder to a safe location. Then run the eseutil /p command in repair mode.
D. Run the eseutil /r command in recovery mode. Then, if necessary, run the eseutil /p command in repair

mode.

Answer: D

Explanation:
You will need to run Eseutil /r e00 /l "c:\program files\exchsrvr\mdbdata"
If the database is in an inconsistent state, run the following command: eseutil /r. This command will bring all the databases to a consistent state. After running this command, you should be able to restart the databases.
If you receive an error message when running this command, or if the databases still won't start, there's a chance that the databases could be corrupt after all.
If you suspect database corruption, you can try running the following command eseutil /p to repair the database. However, be very careful about using this command: It repairs the database by deleting anything that it doesn't understand. The command is eseutil /p /database name.
Incorrect Answers:
A: The ExchDump tool is designed to gather configuration information and the current state information of your Exchange organization. This information is useful to help troubleshoot various Exchange Server support issues. This tool does not change any configuration parameters. It is strictly a read-only tool that gathers data. Currently, the ExchDump tool is supported only on the following operating systems:
• Microsoft Windows Server 2003
• Microsoft Windows XP
• Microsoft Windows 2000
B: You can repair Exchange database files (.edb files) by using Eseutil.exe and Isinteg.exe.
Repairing Exchange databases with Eseutil and Isinteg can cause lost data in the Exchange databases you repair. For this reason, copy the database files you are repairing before attempting the repair process.
• If you plan to put the repaired database back in production you must:
a. Run Eseutil /P.
b. After Eseutil /P completes successfully, run Eseutil /D.
c. After Eseutil /D is completed successfully, run Isinteg -fix -test alltests.
A hard repair occurs when you run an eseutil /p or edbutil /d /r command against an Exchange Server database file, such as the Priv.edb, Pub.edb, or Dir.edb database. The repair goes through the database and checks and repairs critical structures inside the database (such as system tables, attachment tables, and so on) and checks for damaged pages in the databases.
If the repair encounters a page that is damaged (for example, an invalid checksum caused by a modification to the page that was not preformed by Jet) it deletes the page (-1018). When this happens, critical data may be lost after the repair finishes. This data may be part of an e-mail message, a calendar appointment, a note, an attachment, or in the worst-case scenario, part of a system table.
If that system table is the attachment table, every user on the server may lose the attachments to their messages. This is only one possible scenario, but if there are damaged pages in the database, data will be lost following a hard repair.
References
How to Back Up and Restore an Exchange Computer by Using the Windows Backup Program
258243,
Offline Backup and Restoration Procedures for Exchange KB 296788
XADM: Exchange 2000 Server Eseutil Command Line Switches 317014
Overview of the ExchDump tool for Exchange 2000 Server and for Exchange Server 2003 KB 839116

QUESTION 42
You are the Exchange administrator for Certkiller .
The Exchange organization contains a single server Certkiller Srv that runs Exchange Server 2003.
The Exchange server hosts 500 users and contains one storage group and one mailbox store.
The size of the mailbox store is 23 GB. Every night, a full backup is performed on the storage group.
The mailbox store fails. When you attempt to bring it back online, the mailbox store fails to mount. You discover that the mailbox store is corrupted.
You need to restore all the Exchange mailboxes without losing any data.
What should you do?

A. Restore the mailbox store and the transaction log files.
Replay the transaction log files.
B. Restore the mailbox store but not the transaction log files.
Do not replay the existing transaction log files.
C. Restore the mailbox store but not the transaction log files.
Replay the existing transaction log files.
D. Restore the mailbox store and the transaction log files.
Delete the restored transaction log files.

Answer: A
Explanation
You can not select to restore the database and not to restore logs. Which backup software allows you to do this? We are also assuming the database crashed and the current logs are still there (these are logs left after the last full backup). We have to assume that when performing the restore from the FULL backup, the logs are being restored to a temp location, and the last backup set option has been selected,. After the restore, the restored logs will bring the database to a consistent state - then the current logs after the last full backup will be played and the store will be mounted - thus not loosing any data.

QUESTION 43
You are the Exchange administrator for Certkiller .
The Exchange organization contains a single Exchange Server 2003 computer named Certkiller Srv
A. The
Exchange server contains one mailbox store.
The Active Directory administrator informs you that he accidentally deleted a user account and mailbox.
You immediately investigate and discover that the mailbox is still listed in the mailbox store.
You need to ensure that the user can access the mailbox.
What should you do?

A. Run the Cleanup Agent on the mailbox store.
B. Execute the mailbox management process on the Exchange server.
C. Ask the Active Directory administrator to perform an Active Directory authoritative restore of the user object.
D. Ask the Active Directory administrator to perform an Active Directory non-authoritative restore of the user object.

Answer: C
Explanation
In this case the user account has been deleted along with the mailbox account. It is possible to recreate the user account and reconnect the mail to the new account, but in that case the new account will have a new SID and would lose its permissions. Therefore, the administrator needs to perform an authoritative restore for the user account that was deleted.
Incorrect answers:

A. Running the Cleanup Agent will show the orphaned mailbox. It can be used to connect to a recreated account to retrieve mail. However, doing this will not recreate all permissions the account contained. In addition, a new user account has to yet been created so there will be no user account to attach the email account to.
B. The Mailbox Management process will not affect a Mailbox recovery in any way. Mailbox Management is used to define Mailbox Recipient Policies
D. Performing a non-authoritative restore would restore the mailbox and the associated account. However, when the domain controller is restarted, the changes from other domain controllers would once again remove the user object. Remember that a non-authoritative restore will restore an object, but it is not authoritative, and hence will be overwritten by any other domain controller that has newer information.

QUESTION 44
You are the Exchange administrator for Certkiller .
The network consists of a single Active Directory domain Certkiller .com.
The functional level of the domain is Windows Server 2003.
The network contains a single Exchange Server 2003 computer that contains a single storage group with one mailbox store.
You perform full nightly backups of the storage group.
You store the transaction log files on drive F and the database files on drive G.
You have created the Recovery Storage Group by using the G:\Exchsrvr\Recovery Storage Group path for the restored database files.
A user named Jack reports that she can no longer access any network files and that her mailbox is not functioning.
Other users report that they cannot find Jack's name in the global address list (GAL).
You discover that Jack's Active Directory account was deleted 20 minutes ago.
You re-create Jack's accounts in Active Directory.
You need to ensure that Jack has access to her most current e-mail message. Your solution must result in the least amount of mailbox downtime for Tess.
What should you do?

A. Create a new mailbox for Tess.
Restore the Exchange database to the Recovery Storage Group.
Mount the mailbox store.
Use Exmerge to extract Jack's mailbox to a .pst file.
Deliver this .pst file to Tess.
B. Create a new mailbox for Tess.
Restore the Exchange database to the Recovery Storage Group.
Mount the mailbox store.

Use Exmerge to merge Jack's old mailbox data into her new mailbox.
C. Set up a recovery mailbox server.
Restore the Exchange database.
Use Exmerge to extract Jack's mailbox to a .pst file.
Deliver this .pst file to Tess.
D. Run the Cleanup Agent.
Use Mailbox Recovery Center to reconnect Jack's mailbox to her newly created account.

Answer: D
Explanation
By default Exchange keep any deleted mailbox for seven days, to recover a single mailbox you just need to recreate the deleted USER ACCOUNT, run the cleanup agent and reconnect the mailbox to the new account.
Reference
HOW TO: Recover or Restore a Single Mailbox in Exchange Server 2003 823176

QUESTION 45
You are the Exchange administrator for Certkiller .
The Exchange organization consists of several sites containing Exchange Server 5.5 computers and several administrative groups containing Exchange Server 2003 computers.
The site named London contains an Exchange Server 5.5 computer named Certkiller 1, which will be retained for the next two years.
You install a computer named Certkiller 2 into the London site.
You install Exchange Server 2003 on Certkiller 2.
You move some mailboxes to Certkiller 2.
You find that the hardware configuration of Certkiller 2 is not adequate for the required workload. In preparation for replacing Certkiller 2, you install a new computer named Certkiller 3 into the administrative group.
You install Exchange Server 2003 on Certkiller 3 and move all mailboxes from Certkiller 2 to Certkiller 3.
You need to ensure that Certkiller 2 can be removed from the network without disrupting Exchange services. To minimize the load on Certkiller 3, you must not move any unnecessary roles to it.
Which three actions should you perform? (Each correct answer presents part of the solution. Choose three)

A. Replicate the Offline Address Book Folder to Certkiller 3. Remove the replica from the original owner of the folder.
B. Replicate the OAB Version 2 folder to Certkiller 3. Remove the replica from the original owner of the folder.
C. Replicate the Schedule+ Free Busy folder to Certkiller 3. Remove the replica from the original owner of the folder.
D. Modify the Recipient Update Service to use Certkiller 3.
E. Create an instance of the Site Replication Service on Certkiller 3. Remove the original instance.
F. Configure the routing group to designate Certkiller 3 as the routing group master.

Answer: A, C, D

Explanation:

The first Exchange Server 2003 computer that is installed in an administrative group holds certain important roles. The first server hosts Offline Address Book folder, the Schedule+ Free Busy folder, Events Root folder, and other folders.
All public folders and system folders that are housed on the first Exchange 2003 computer must be replicated to another Exchange 2003 computer that is in the site
After replicas have been made on the destination server, wait for replication to complete, and then make sure that the replica folders are synchronized with the source folders.
After replicas have been made on the destination server, wait for replication to complete, and then make sure that the replica folders are synchronized with the source folders.
Select Exchange Server dialog box, click the name of another Exchange 2003 Server computer as the new server to host the Recipient Update Service, OAB Version 2 folder will be recreated on server Certkiller 3 by the
RUS service
By default, the offline Address Book replicates its contents to the public folder store of the server on which it is installed. If the public folder store is removed from the offline Address Book's replication configuration we will get an error, but this is solved with the Public folders replication that is nthe first step to do
Reference
How to Remove the First Exchange 2003 Server Computer from the Site KB 822931

QUESTION 46
You are the Exchange administrator for Certkiller .
The Exchange organization consists of four administrative groups.
Each group contains only Exchange Server 2003 computers.
Each administrative group contains a single routing group, which connects to other routing groups by using routing group connectors.
The administrative group named Beijing is upgraded from an Exchange Server 5.5 site.
This administrative group contains two Exchange Server 2003 computers named Certkiller 1 and Certkiller 2.
Certkiller 1 was the first Exchange Server 2003 computer installed into the administrative group. It is used as a mailbox server.
There are no user-created public folders on Certkiller 1.
All connectors in the routing group use only Certkiller 2 as a bridgehead server.
Certkiller 2 is configured as the routing group master.
Certkiller 1 cannot support the required workload.
You add a new Exchange Server 2003 computer named Certkiller 3 into the Beijing administrative group.
Certkiller 3 will perform all tasks that are currently performed by Certkiller 1.
You move all mailboxes from Certkiller 1 to Certkiller 3.
You need to ensure that you can remove Certkiller 1 from the Beijing administrative group without disrupting Exchange services.
Which three actions should you perform? (Each correct answer presents part of the solution. Choose three)

A. Replicate the Offline Address Book folder and the OAB Version 2 folder to Certkiller 3. Remove the original replica.
B. Replicate the Schedule+ Free Busy folder to Certkiller 3. Remove the original replica.
C. Modify the Recipient Update Service to use Certkiller 3.

D. Create an instance of the Site Replication Service on Certkiller 3. Remove the original instance.
E. Configure the Beijing routing group to designate Certkiller 3 as the routing group master.
F. Configure all the routing group connectors in the Beijing routing group to use Certkiller 3 as the bridgehead server.

Answer: B, C, D

Explanation:
Compare with the previous to question. This time they told us that Certkiller 2 is configured as the routing group
master and in this case we need to move any service in Certkiller 1 to Certkiller 3.
Certkiller 1 was the first Exchange Server 2003 computer installed into the administrative group, for this reason this server will be will have the Site Replication Service on it no the master routing group
Reference
How to Remove the First Exchange 2003 Server Computer from the Site KB 822931

QUESTION 47
You are the Exchange administrator for Certkiller .
The company has eight branch offices in addition to the main office.
All network computers are members of a single Active Directory domain named Certkiller .com.
Each office has 1,000 users, two DC's, and one server running Exchange Server 2003.
Microsoft Outlook 2003 is the only e-mail client in use.
Users often schedule meetings by using Outlook's meeting scheduling feature.
They report that the available and unavailable times for other users are frequently incorrect, especially for users located in other offices.
You discover that the availability information for a user can be as much as two days out of date when viewed by users in other offices.
You need to ensure that availability information is as accurate as possible in all offices.
What should you do?

A. Configure all Active Directory site links and site link bridges to increase the frequency of Active Directory replication.
B. Configure all Exchange servers to increase the frequently of public folder replication with other Exchange servers.
C. Instruct all users to configure the Microsoft Office Internet Free/Busy Service in Outlook 2003.
D. Install Microsoft Schedule+ 7.0 on all client computers in all offices.

Answer: B

Explanation:
Usually The Public folders are out of date because replication is not happening often enough. This is especially true in larger organizations where a folder may be a replica of a replica they have two DC and just one server running Exchange 2003 per office this means that they have 9 Exchange servers,
In this way an organization architecture like this and if Public Folders are not configured with the defaukts values if possible to get a two days delay for Schedule+ Free Busy Folder,
By default schedule + free busy connector use the default settings for replication interval with is inherit from

Public Store setting. That by default is always run that means each 15 minutes or message limit of 300 Kb
They told us that the availability information for a user can be as much as two days out of date this means that they are not using the defaults setting for schedule + free busy connector folder
They also tell us that they are using outlook 2003 as mail client with the Microsoft(r) Office Internet Free/Busy Service, users can publish their free/busy times to a shared Internet location or an Exchange server. Members of the service can view each other's free/busy information and can help to control which members have access to their information.
Because they do not tell us that there is any bandwidth constrain, a best solution is answer B
Incorrect answer:

A. Increasing the frequency of AD replication could potentially make the situation worse, as more network traffic is generated to the remote offices. In any event, this will not resolve the problem as the Public Folders are out of date, not Active Directory.
C. They can do it in this way but best answer will be B.
D. Installing Schedule+ 7.0 on all client computers will remove functionality. In addition, the problem is not that the data can't be seen. The problem is that the data seen is out of date. No client will change that issue.
References
http://www.microsoft.com/office/ork/2003/six/ch22/ColC02.htm

QUESTION 48
You are the Exchange administrator for Certkiller .
The Exchange organization contains a single server named Exch1.
Exch1 runs Exchange Server 2003 and hosts all user mailboxes.
All remote users access Exch1 by using Microsoft Outlook Express 6.
All internet users access Exch1 by using Outlook.
You create several new public folders.
All internal users can successfully access the new folders, but some remote users cannot.
All users can still access their personal mailboxes.
You need to ensure that all remote users can access the public folders.
What should you do?

A. Instruct the users who cannot access the folders to re-create their Outlook Express e-mail accounts as IMAP accounts.
B. Instruct the users who cannot access the folders to establish a VPN connection with the internal network before they open Outlook Express.
C. Modify the company firewall so that only SMTP, HTTP, and POP3 traffic is allowed to pass to Exch1.
D. Modify the company firewall so that NNTP is added to the list of protocols allowed to pass to Exch1.

Answer: A

Explanation:
The issue stems from the fact that most of the OE6 clients set up their mail as POP3. POP3 can be sued to retrieve mail, but can't display such things as calendar or Public Folders. Changing the clients to use IMAP enables these features.
Incorrect answers:

B. Establish a VPN connection before launching Outlook Express - This will not work, as the client is still using a protocol (POP3) that can't display Public Folders. If the clients were to use a VPN connection and Outlook, then this configuration would work, but as stated, the clients will still not see Public Folders.
C. Modify the company Firewall - This will not allow the IMAP traffic through, and hence will prevent all the OW6 clients that are currently working successfully from seeing the public folders, as well as preventing them from connecting as their connections are set for IMAP, and not HTTP, POP3, or SMTP.
D. Modify the firewall to allow NNTP traffic - NNTP is a news protocol. The Public Folders in question are not using News Groups, so this protocol would have no effect on the problem. In addition, some remote users can access the folders without incident, so the absence of the protocol in the firewall can't be causing the problem.

QUESTION 49
You are the Exchange administrator for Certkiller .
The company intranet is protected by a firewall.
The Exchange organization includes a server named Certkiller SrvA, which runs Exchange Server 2003.
Certkiller SrvA contains only public folders. It does not contain user mailboxes.
Currently, your customers send comments in e-mail messages to an alias named Comments.
These e-mail messages are received by the customer service manager.
Management decides to collect customer comments in one location so they can be easily viewed by all users.
You remove the Comments e-mail SMTP address from the mailbox of the customer service manager.
You use Exchange System Manager to create a new public folder named Comments and Certkiller SrvA.
Then you send a test e-mail message to the Comments e-mail address.
You receive a non-delivery report (NDR).
You need to ensure that customers will be able to send comments to the Comments alias, and that the comments will be saved in the new Comments folder.
What should you do?

A. Modify the configuration of the Comments folder so that it is mail-enabled.
B. Modify the configuration of the firewall to allow SMTP traffic to pass from the Internet to Certkiller SrvA.
C. On your DNS server, create a mail exchanger (MX) resource record that has a priority of 10 and that points to the host (A) resource record for Certkiller SrvA.
D. In Active Directory, create a new Contact object named Comments.
Configure the contact object to have the Comments e-mail alias as its e-mail address.

Answer: A

Explanation:
To use Exchange System Manager to create a new public folder named Comments and Certkiller 1, you will need to mail enable the public folder
Reference
Exchange Server 2003 Server admin help

QUESTION 50
You are the Exchange administrator for Certkiller .
The Exchange organization contains two Microsoft Windows Server 2003 computers that run Exchange Server 2003.
Inbound SMTP mail from the Internet is delivered to both Exchange servers.
Customers report that messages they send to Certkiller over the Internet are not delivered and they receive non-delivery reports (NDRs).
You discover that the customers are sending messages to e-mail aliases that do not exist.
You need to ensure that all customer e-mail messages sent to an incorrect address are delivered to a mailbox.
What should you do?

A. Configure the SMTP connector to have an address space of " Certkiller .com.
B. Configure the info user's e-mail addresses to have the additional SMTP address of *.*@ Certkiller .com.
C. Configure each server's SMTP virtual server to forward all messages that have unresolved recipients to the other Exchange server.
D. Configure each server's SMTP virtual server to send a copy of all NDRs to an existing mailbox whose email address is info@ Certkiller .com.
E. Create a mailbox-enabled user account whose e-mail address is NDRMailbox@ Certkiller .com.

Answer: D

Explanation:
In Exchange 2003, you can send a copy of all Non-Delivery Reports (NDRs) to a specific mailbox or SMTP email
address.
Incorrect answers:

A. Certkiller .com is not a valid email address, so this will not work.
B. Configuring user's email address to have additional SMTP address would qualify for outbound mail, but would have no effect on the administrator seeing any NDR's.
C. Configuring all unresolved addresses to be forwarded to the other Exchange Server is could lead to a lot of unnecessary traffic as messages ping-pong back and forth. In addition, since each Exchange Server contains the same AD information, the external email address would not get resolved anyway.
E. Creating a mailbox enabled account called NDRMailbox@ Certkiller .com would not work as there is no link between actual undeliverable messages and this mailbox.

QUESTION 51
You are the Exchange administrator for Certkiller .
Exchange Server 2003 runs on two Microsoft Windows Server 2003 member servers.
Certkiller 's network consists of a single Active Directory domain named Certkiller .com.
Two domain controllers are located in a single Active Directory.
Inbound SMTP mail from the Internet arrives on both Exchange servers.
You configure sender filtering to reduce the amount of junk e-mail that is received by company users.
You specify a list of known junk e-mail senders in the blocked-sender list.
Users report that they still receive e-mail from these senders.

You need to ensure that users do not receive messages from the blocked-sender list.
What should you do on both Exchange servers' SMTP virtual servers?

A. Enable the filter on the servers' IP address.
B. Assign relay permissions to only authenticated users.
C. Configure the servers' authentication settings to resolve anonymous e-mail.
D. Configure the servers to perform reverse DNS resolution on incoming messages.

Answer: A

Explanation:
The filter is created, but has not been applied. Hence, the junk mail still arrives.
The incorrect answers:
B. Assigning relay permissions is helpful to avoid Denial of Service (DoS) attacks, but would not affect the delivery of inbound spam messages. Also does not apply the given filter anywhere.
C. By default all incoming mail, whether spam or not, is authenticated anonymously. Resolving these names would incur significant overhead, and many times would block even valid email. This also does not utilize the given filter.
D. Configuring servers to perform DNS resolution on incoming messages would not prevent spam, and certainly would not take into consideration the filter that was defined.

QUESTION 52
You are the Exchange administrator for Certkiller .
The Exchange organization contains three Microsoft Windows Server 2003 member servers that run Exchange Server 2003.
The company's network has a firewall.
One of the functions of the firewall is queuing and delivery of outbound SMTP mail.
The written company policy states that Exchange servers must not send SMTP mail directly to the Internet.
The three Exchange servers must be able to send mail directly to each other.
You need to ensure that messages for external recipients are delivered to the Internet through the firewall.
What should you do?

A. Configure each SMTP virtual server to use the firewall as a smart host.
B. Configure each SMTP virtual server to use the firewall as its external DNS server.
C. Configure each SMTP virtual server to forward e-mail with unresolved recipients to the firewall.
D. Configure an SMTP connector that will use the firewall as a smart host.

Answer: A

Explanation:
The three Exchange servers must be Able to send mail directly to each other. We can achieve this by using routing groups. The company policy states that Exchange servers must not send SMTP mail directly to the Internet. Therefore, we will need to configure on each a SMTP connector that will send all the traffic to an smart host in this case the firewall because they require that One of the functions of the firewall is queuing and

delivery of outbound SMTP mail.
Incorrect answers:
B. Since the firewall has no DNS lookups, this will not work. In addition, any external lookups from the Exchange Server will fail.
C. The mail would cease to be routed at this point, as the firewall would not know what to do with the SMTP traffic once it arrived
D. To be a possible answer the statement must be Configure an SMTP connector for each SMTP virtual server to use the firewall as a smart host
References
MS article 821911, How to Configure Exchange Server 2003 to Use a Smart Host IP Address
Using ISA Server 2000 with Exchange Server 2003 MS White paper

---

QUESTION 53
You are the Exchange administrator for Certkiller .
The network contains two Exchange Server 2003 computers named Certkiller 1 and Certkiller 2.
Certkiller 1 is used as the mailbox server for all users. It is not accessible from the Internet.
Certkiller 2 is configured as a front-end server.
Users connect to Certkiller 2 from the Internet and access their mailboxes by using Microsoft Outlook Web Access.
The company plans to implement a new Web service application.
The application will store data in public folders on Certkiller 1.
You create a dedicated public folder tree named Appdata for the public folders used by the new application.
All users of the Web service application will be located outside the company network.
The Web service will access the public folders in the Appdata public folder tree by using HTTP to connect to Certkiller 1 over the Internet.
TCP port numbers will be used to identify all additional HTTP virtual servers that need to be created.
The Web service will be configured to include the TCP port number under the URL of each request.
You need to enable access to the public folders in the Appdata public folder tree.
Which two actions should you perform? (Each correct answer presents part of the solution. Choose two)

A. Add a second HTTP virtual server to Certkiller 1. Configure the virtual server to use TCP port 80. Associate the virtual server with the Appdata public folder tree.
B. Add a second HTTP virtual server to Certkiller 2. Configure the virtual server to use TCP port 80. Associate the virtual server with the Appdata public folder tree.
C. Add a second HTTP virtual server to Certkiller 1. Configure the virtual server to use TCP port 8000. Associate the virtual server with the Appdata public folder tree.
D. Add a second HTTP virtual server to Certkiller 2. Configure the virtual server to use TCP port 8000. Associate the virtual server with the Appdata public folder tree.
E. Add a second HTTP virtual server to Certkiller 1. Configure the virtual server to use TCP port 8000. Associate the virtual server with the default public folder tree.
F. Add a second HTTP virtual server to Certkiller 2. Configure the virtual server to use TCP port 8000. Associate the virtual server with the default public folder tree.

Answer: C, D

Explanation:
They tell us TCP port numbers will be used to identify all additional HTTP virtual servers that need to be created. Because Certkiller 1 is used as the mailbox server for all users and also it is not accessible from the Internet and Certkiller 2 is the server that can be accessed from Internet this means a front end back end configuration
They tell us all users of the Web service application will be located outside the company network this means that all the users that will access to the application will be accessing to Certkiller 2 server
In a front end configuration the users can access form OWA to their inbox and to the public folders. There is no need that Certkiller 2 contain mailbox or public folder, Certkiller 2 will redirect the petition to public folders housed on Certkiller 1 backend server
Because they want that Web service will be configured to include the TCP port number under the URL of each request and port 80 is used by normal OWA access and normal public folders you will need to configure a second port in this case the 8000 port to access to the dedicated public folder tree named Appdata.
Incorrect answers:
A, B. You can't use port 80, as it is in use by the default web site
E, F. Associating the new HTTP Public Store with the Default site will allow all external users to see the Default Store, and NOT the AppData store. This is the opposite of the intended effect.

QUESTION 54
You are the Exchange administrator for Certkiller .
The Exchange organization contains a single server that runs Exchange Server 2003.
Users send many order confirmations and order acknowledgement receipts to customers by using e-mail.
Users report that they are not being notified quickly enough when a message to an external customer is not deliverable.
You need to ensure that when a message is not delivered within one hour, a notification is sent to the message originator.
How should you configure the SMTP virtual server?

A. Configure the local delay notification to one hour.
B. Configure the local expiration timeout to one hour.
C. Configure the subsequent retry interval to one hour.
D. Configure the outbound delay notification to one hour.

Answer: D

Explanation:
Outbound delay notification specifies when to notify users that messages are delayed
Incorrect answers:
A, B. The Local Delay Notification and Local Expiration Timeout applies to the local store only, and not to any outbound message
C. Subsequent Retry will have no effect on any notification settings

---

QUESTION 55
You are the Exchange administrator for Certkiller . Certkiller operates two offices; one in London and one in Leipzig.
The Exchange organization contains eight servers that run Exchange Server 2003. Each office contains

four Exchange servers.
Each office is configured as a routing group.
The routing groups are connected by a routing group connector.
In each office, one Exchange server is configured as a bridgehead server.
Each bridgehead server is configured with two SMTP virtual servers.
One SMTP virtual server is configured as the bridgehead server for the SMTP connector for e-mail messages sent to and from the Internet.
The other SMTP virtual server is configured as the bridgehead server for the routing group connector.
You need to ascertain the number and size of e-mail messages sent between the two offices, and to and from the Internet, every day.
You need to specify the number of messages sent, the total size of messages sent, and the appropriate queue length on each server.
You will use this data to plan for future growth.
How should you modify each bridgehead server?

A. Configure a counter log to monitor both SMTP virtual servers.
B. Configure a counter log to track all messages sent by Microsoft Exchange MTA Stacks service.
C. Configure SMTP logging on both SMTP virtual servers.
D. Configure SMTP logging on the SMTP virtual server that sends and receives e-mail messages to and from the Internet. Configure a counter log to track all messages sent between routing groups by the Microsoft Exchange MTA Stacks service.

Answer: D

Explanation:
Some may be think that configuring SMTP logging on both SMTP virtual servers will accomplish all necessary tasks.
You can't accomplish all necessary tasks only using SMTP logging. Besides the Store.exe process, other processes that consume memory (and may affect performance) include:
- Inetinfo.exe Process that handles Internet protocols
- Emsmta.exe Microsoft Exchange Message Transfer Agent (MTA) Stacks service
- Mad.exe Microsoft Exchange System Attendant

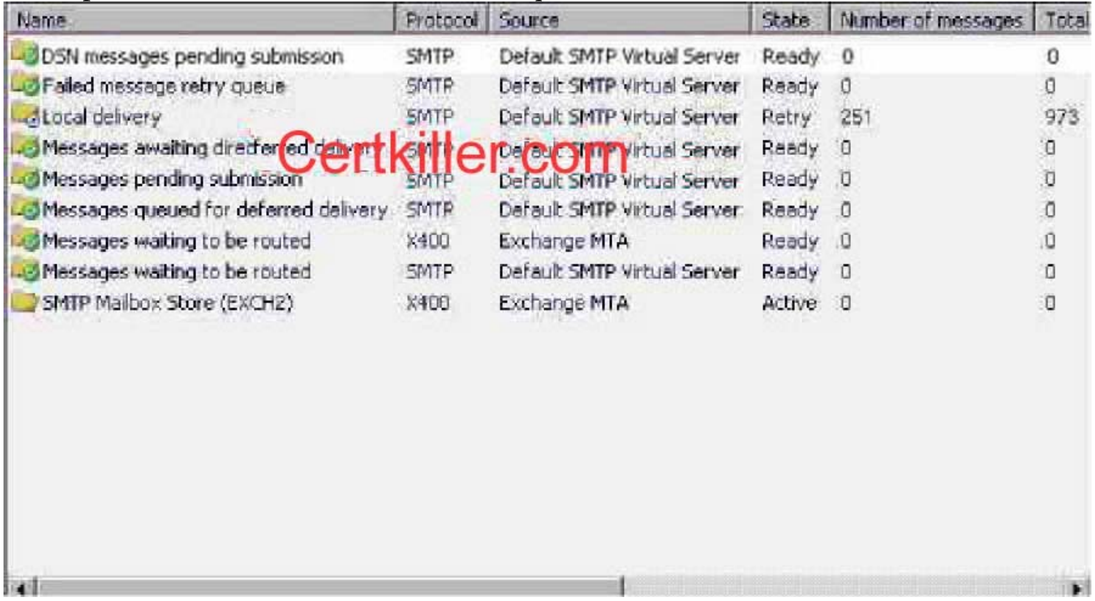
Microsoft Exchange MTA Stacks (MSExchangeMTA) maintain the link state table between SMTP and the routing engine that is used to communicate link state information between routing groups and throughout the organization
Is supposed that this service is only needed for backwards compatibility, but is also used when mailbox moves, or if there are X.400 connectors on the computer and for error handling of some messages
The message transfer agent (MTA) in Exchange now uses Gwart.dll to make a legacy compatible gateway address routing table (GWART). MTA uses Mtaroute.dll as the connection between the legacy MTA and the Microsoft Exchange Routing Engine
Incorrect answers:

A. Configuring a counter log to monitor both SMTP servers is incorrect because it is vague. No mention of what counters are needed or where to do the logging is named. In addition, it is unclear what is meant by "monitoring the servers". Do they mean the physical servers? SMTP virtual servers? This is not the best answer.

B. MTA stacks service will not help here. They can't log items daily for review. The MTA Stacks service is only used for compatibility between Exchange 5.5 and Exchange 200x servers. Since there are no Exchange 5.5 servers here, this counter is not needed.
C. You can't do it the entire required job just using SMTP logging,
Reference
An e-mail message is not delivered and an event ID 210 "content conversion failed" warning message is logged for the MTA in Exchange Server 2003 KB 834570
The Microsoft Exchange MTA Stacks service cannot start in Exchange 2003 and event IDs 137 and 9405 appear in the application event log KB 840470
Microsoft Operations Manager Message Transfer Agent Rule Group

---

QUESTION 56
You are the Exchange administrator for Certkiller . The company network consists of a single Active Directory domain named Certkiller .com that contains two domain controllers. One domain controller is also a global catalog server. The Exchange organization contains two Exchange Server 2003 computers names Exch1 and Exch2. All users send and receive e-mail messages by using Microsoft Outlook.
Users who have mailboxes on Exch2 report that they cannot open their mailboxes. However, users who have mailboxes on Exch1 can open their mailboxes and send e-mail message to all users on the network.
You open Queue Viewer on Exch2. The queue information is shown in the exhibit.



Name	Protocol	Source	State	Number of messages	Total
DSN messages pending submisson	SMTP	Default SMTP Virtual Server	Ready	0	0
Failed message retry queue	SMTP	Default SMTP Virtual Server	Ready	0	0
Local delivery	SMTP	Default SMTP Virtual Server	Retry	251	973
Messages awaiting directory lookup	SMTP	Default SMTP Virtual Server	Ready	0	0
Messages pending submission	SMTP	Default SMTP Virtual Server	Ready	0	0
Messages queued for deferred delivery	SMTP	Default SMTP Virtual Server	Ready	0	0
Messages waiting to be routed	X400	Exchange MTA	Ready	0	0
Messages waiting to be routed	SMTP	Default SMTP Virtual Server	Ready	0	0
SMTP Mailbox Store (EXCH2)	X400	Exchange MTA	Active	0	0

You must ensure that users on Exch2 can send and receive e-mail messages.
What should you do?

A. Add a mail exchanger (MX) resource record for Exch2 to the DNS zone.
B. Start the IMAP4 and POP3 services on Exch2.
C. Configure Exch2 to use the global catalog server for all directory services access.
D. Mount the mailbox store on Exch2.

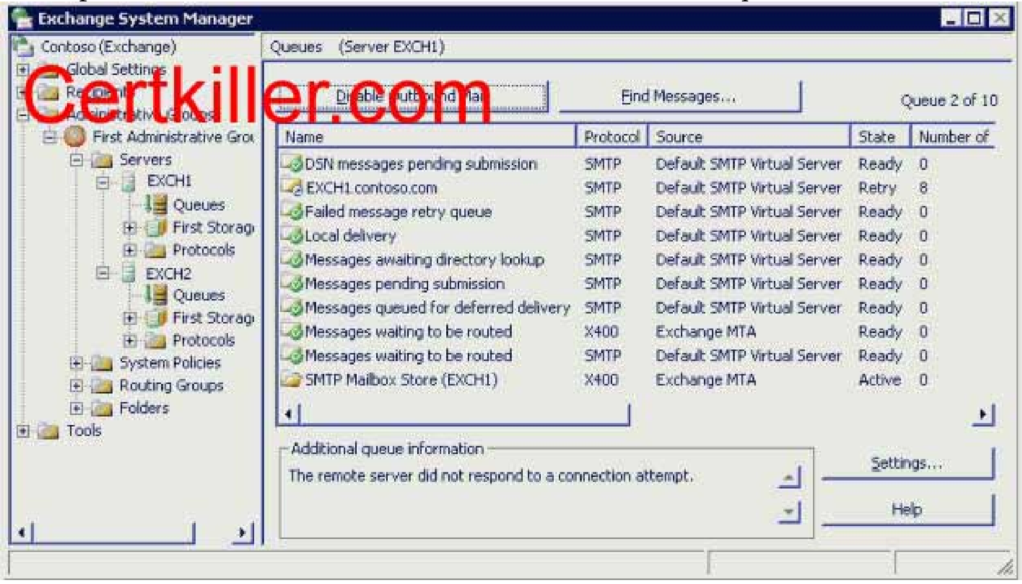
Answer: D

Explanation:

The local delivery queue shows a large number of messages waiting to be delivered. Because they do no show us that SMTP service is not available the answer must be to mount the mailbox store.
Incorrect answers:

A. Adding a mail exchange record is only useful for internet mail inbound to the Exchange server. In this case however, the mail is all internal to the server. Therefore, this can't be the answer.
B. Starting the IMAP and POP3 services will also accomplish nothing. All Exchange mail is sent through SMTP. IMAP and POP3 have no participation in the transfer of mail from a server to itself. Further, unless a server is specifically set up for these services (not mentioned here) it will not use it for server to server communications. Both of these facts disqualify this answer.
C. Configuring Exch2 as a global catalog server will not relieve the situation. The problem, according to the exhibit, is in the local delivery queue. The Global Catalog will only be useful when the server has to look to it to resolve a name. That is only done when the name is NOT local to the Exchange Server. Since the local delivery queue has the problem and not external delivery queue.

QUESTION 57
You are the Exchange administrator for Certkiller .
The network consists of a single Active Directory domain named Certkiller .com.
The Exchange organization contains two servers named Exch1. Certkiller .com and Exch2. Certkiller .com.
Both servers run Exchange Server 2003.
Users who have mailboxes on Exch1. Certkiller .com report that their e-mail messages are not being delivered to other users on the network.
However, these users can open their mailboxes and read the e-mail messages in their mailboxes.
You discover that users who have mailboxes on Exch2. Certkiller .com can send e-mail messages to mailboxes on the same server. However, e-mail messages sent to mailboxes on
Exch1. Certkiller .com is not delivered.
You open Queue Viewer on Exch2. Certkiller .com. The queue information is shown in the exhibit.



Name	Protocol	Source	State	Number of
DSN messages pending submission	SMTP	Default SMTP Virtual Server	Ready	0
EXCH1.contoso.com	SMTP	Default SMTP Virtual Server	Retry	8
Failed message retry queue	SMTP	Default SMTP Virtual Server	Ready	0
Local delivery	SMTP	Default SMTP Virtual Server	Ready	0
Messages awaiting directory lookup	SMTP	Default SMTP Virtual Server	Ready	0
Messages pending submission	SMTP	Default SMTP Virtual Server	Ready	0
Messages queued for deferred delivery	SMTP	Default SMTP Virtual Server	Ready	0
Messages waiting to be routed	X400	Exchange MTA	Ready	0
Messages waiting to be routed	SMTP	Default SMTP Virtual Server	Ready	0
SMTP Mailbox Store (EXCH1)	X400	Exchange MTA	Active	0

Additional queue information
The remote server did not respond to a connection attempt.

You need to ensure that all users can send and receive e-mail messages.
What should you do?

A. Configure the SMTP virtual server on Exch1. Certkiller .com to accept only authenticated connections.

B. Start the SMTP service on Exch1. Certkiller .com.
C. Configure a mail exchanger (MX) resource record for Exch1. Certkiller .com on the DNS server that is authoritative for Certkiller .com.
D. Start the IMAP4 and POP3 services on Exch1. Certkiller .com.

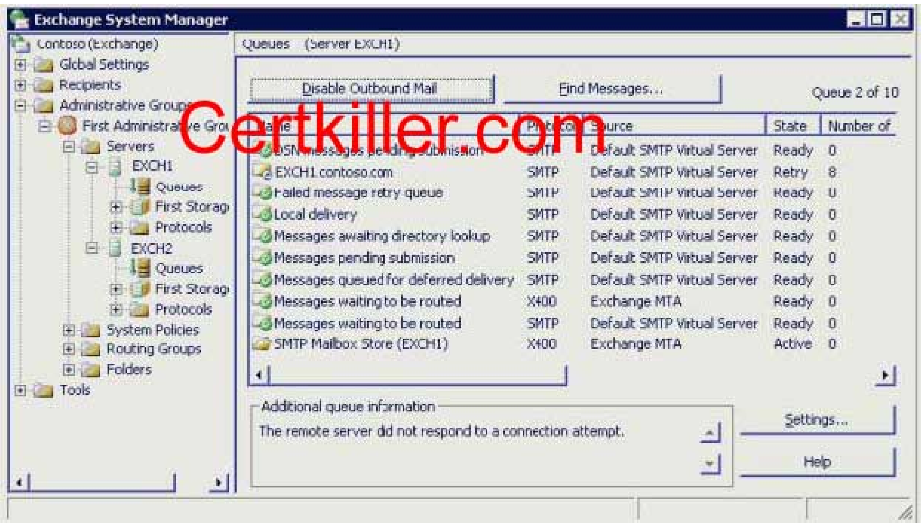
Answer: B

Explanation:
On the server where STMP has been stopped, the state column will show SMTP as Not available.
In the server queues where the message has been originated you will see how many messages are queuing, awaiting deleivery.
In this figure you see the queues in EXCH2 because SMTP service is stopped in EXCH1. If you start the SMTP service in EXCH1 and force the connection, the messages will be delivered and will move out of the queue.
Incorrect answers:

A. Configuring Exch1 to only accept authenticated connections will not resolve the problem here. Since there is an error message stating that the remote server did not respond to a connection attempt, it is a safe assumption that there is something preventing connections. Since servers all authenticate through Kerberos, the authentication method can't be the problem.
C. Configuring an MX record for Exch1 will not help. MX records are only useful for receiving mail from outside the organization. Since users local to Exch1 can't send or receive mail, adding an MX record will not change anything.
D. Starting the IMAP and POP3 services will also accomplish nothing. All Exchange mail is sent through SMTP. IMAP and POP3 have no participation in the transfer of mail from a server to itself. Further, Unless a server is specifically set up for these services (not mentioned here) it will not use it for server to server communications. Both of these facts disqualify this answer.
Reference: KB article 823489 - How to Use Queue Viewer to Troubleshoot Mail Flow Issues

---

QUESTION 58
You are the Exchange administrator for Certkiller . The network consists of a single Active Directory domain named Certkiller .com. The Exchange organization contains two servers named Exch1. Certkiller .com and Exch2. Certkiller .com. Both servers run Exchange Server 2003.
Users who have mailboxes on Exch1. Certkiller .com report that their e-mail messages are not being delivered to other users on the network. However, these users can open their mailboxes and read the email messages in their mailboxes. You discover that users who have mailboxes on Exch2. Certkiller .com can send e-mail messages to mailboxes on the same server. However, e-mail messages sent to mailboxes on Exch1. Certkiller .com are not delivered. You open Queue Viewer on Exch2. Certkiller .com. The queue information is shown in the exhibit.



Queues (Server EXCH1)

Queue 2 of 10

Name	Protocol	Source	State	Number of
DSN messages pending submission	SMTP	Default SMTP Virtual Server	Ready	0
EXCH1.contoso.com	SMTP	Default SMTP Virtual Server	Retry	8
Failed message retry queue	SMTP	Default SMTP Virtual Server	Ready	0
Local delivery	SMTP	Default SMTP Virtual Server	Ready	0
Messages awaiting directory lookup	SMTP	Default SMTP Virtual Server	Ready	0
Messages pending submission	SMTP	Default SMTP Virtual Server	Ready	0
Messages queued for deferred delivery	SMTP	Default SMTP Virtual Server	Ready	0
Messages waiting to be routed	X400	Exchange MTA	Ready	0
Messages waiting to be routed	SMTP	Default SMTP Virtual Server	Ready	0
SMTP Mailbox Store (EXCH1)	X400	Exchange MTA	Active	0

Additional queue information

The remote server did not respond to a connection attempt.

You need to ensure that all users can send and receive e-mail messages.
What should you do?

A. Configure the SMTP virtual server on Exch1. Certkiller .com to accept only authenticated connections.
B. Start the SMTP service on Exch1. Certkiller .com.
C. Configure a mail exchanger (MX) resource record for Exch1. Certkiller .com on the DNS server that is authoritative for Certkiller .com.
D. Start the IMAP4 and POP3 services on Exch1. Certkiller .com.

Answer: B
Explanation
In this case the problem is due to the smtp service, if the service is stopped on a server, the messages can't be resolved to any destination and the service must be restarted.
Incorrect Answers:
A: Configuring Exchange to accept Authenticated connections is used only to permit Domain authenticated users to send mail. It will not affect mail delivery in this case, as all users have authenticated connections.
C: Exchange Server does not need to have a MX record to deliver mail within the organization. Exchange use SRV records to locate a Global Catalog through the DSaccess component.
D: There is no problem with POP3 or IMAP4 protocols. Exchange Server uses IMAP4 by default
Reference
How to Use Queue Viewer to Troubleshoot Mail Flow Issues 823489

QUESTION 59
You are the Exchange administrator for Certkiller .
The network contains two Exchange Server 2003 computers named Certkiller 1 and Certkiller 2. Both servers run Microsoft Windows 2000 Server.
Certkiller 1 functions as the mailbox server for all users.
It is not accessible from the Internet.
Certkiller 2 is configured as a front-end server and is used only when users need to connect to their mailboxes by using HTTP and IMAP4.
You need to disable all services on Certkiller 2 that are not required for the server to function in its

designated role.
Which service or services should you disable? (Choose all that apply)

A. IIS Admin Service
B. World Wide Web Publishing Service
C. Microsoft Exchange Information Store
D. Microsoft Exchange Post Office Protocol version 3 (POP3)
E. Microsoft Exchange Message Transfer Agent (MTA) Stacks
F. Microsoft Exchange Internet Message Access Protocol, Version 4 (IMAP4)

Answer: C, D, E

Explanation:
You do not need Microsoft POP3 Service, which provides e-mail transfer and retrieval services. The Microsoft POP3 Service system service is combined with the SMTP Service, which allows users to send outgoing e-mail, for full e-mail services.
The Exchange Information Store service supports data storage (mailboxes and public folders data) on the server. Since a front end OWA server queries backend server for data, this service can be disabled during regular operations.
Microsoft Exchange MTA Stacks service supports message routing to foreign messaging system using X.400 and gateway connectors. It is not a required service on a front end OWA server.
Incorrect Anwers:
A: You can't disable IIS Admin Service this service as IIS Admin Services allows administration of IIS components such as FTP, Applications Pools, Web sites, Web service extensions and both Network News Transfer Protocol (NNTP), and Simple Mail Transfer Protocol (SMTP) virtual servers. If this service is stopped or disabled, you will not be able to run Web, FTP, NNTP, or SMTP sites
B: World Wide Web Publishing service is the generic service under IMAP and HTTP.
F: Exchange 2003 and Outlook 11 combined with Windows Server 2003 now supports RPC over HTTP but the TRICK HERE is Exchange are running in servers that run Microsoft Windows 2000 Server same setting as Exchange 2000 apply
Reference:
SECURING AN EXCHANGE 2000 OWA FRONTEND SERVER WITH SECURITY TEMPLATES

QUESTION 60
You are the Exchange administrator for Certkiller .
The network contains two Exchange Server 2003 computers named Certkiller 1 and Certkiller 2. Certkiller 1 contains all user mailboxes.
Certkiller 2 is configured as a front-end server and is used for all Microsoft Outlook Web Access client connections from the Internet.
Written Certkiller security policy states that all messaging traffic from the Internet must be encrypted, including traffic between Certkiller 1 and Certkiller 2.
You configure Certkiller 2 to require HTTPS for all connections to Outlook Web Access.
When you monitor network traffic, you notice that traffic between Certkiller 1 and Certkiller 2 is not encrypted.
You need to ensure that all Outlook Web Access client traffic between Certkiller 1 and Certkiller 2 is encrypted.

What should you do?

A. Configure Certkiller 2 to accept Kerberos authentication only.
B. Configure Certkiller 1 and Certkiller 2 to use IPSec for all connections between them.
C. Configure Certkiller 2 to require IPSec for all connections to Outlook Web Access.
D. Configure Certkiller 1 to require HTTPS for all connections to Outlook Web Access.

Answer: B

Explanation:
Configuring Certkiller 1 and Certkiller 2 to use IPSec for all connections between them is the only listed option that will allow both servers to use encrypted communications.
Incorrect answers:

A. Kerberos is for authentication only. Once the servers are authenticated, the traffic passes without any form of encryption by default. Note also that Kerberos is standard for Windows 200x servers.
C. Configuring Certkiller 2 to require IPSec for all OWA connections is unnecessary since all communications done via OWA are already encrypted via HTTPS. Further, this does nothing for the traffic between the two servers.
D. Configuring Certkiller 1 to use HTTPS for all OWA traffic is not relevant. The question states that Certkiller 2 is a front end server. Therefore, no OWA traffic should penetrate to Certkiller 1 directly. In addition, even if this were the case, all the traffic would be encrypted between Certkiller 1 and OWA, and not between the servers as required.

QUESTION 61
You are the Exchange administrator for Certkiller .
The network contains two Exchange Server 2003 computers named Certkiller 1 and Certkiller 2. Certkiller 1 contains all user mailboxes and is not accessible from the Internet.
Certkiller 2 is configured as a front-end server and is used for all Microsoft Outlook Web Access client connections from the Internet.
Certkiller 2 is also used as a relay for all incoming and outgoing SMTP messages.
The company uses the domain name suffix adatum.com for all SMTP addresses.
Users report that they do not receive non-delivery reports (NDRs) when e-mail messages cannot be delivered.
You discover this only occurs when Certkiller 2 cannot deliver e-mail messages addressed to Internet recipients.
You need to ensure that users receive NDRs when delivery of Internet e-mail messages fails. Users must still be able to use Outlook Web Access from the Internet.
What should you do on Certkiller 2?

A. Configure the default SMTP virtual server to forward all mail with unresolved recipients to Certkiller 1.
B. Configure the default SMTP virtual server to send a copy of the NDRs to the e-mail address of administrator@adatum.com.
C. Start the Microsoft Exchange Information Store service and mount the default mailbox store.
D. Create an SMTP connector and associate the connector with the namespace of adatum.com. Specify Certkiller 1 as a smart host.

Answer: D

Explanation:
The primary issue is that the NDR's on Certkiller 2 are not getting relayed to Certkiller 1. Adding the SMTP connector performs a "reverse connector", and will enable the NDR's to be sent back to Certkiller 1 for delivery to the users on the Certkiller 1 mail store.
Incorrect answers:

A. Simply sending all unresolved recipients is not sufficient. It is entirely possible that the address will be resolved, but the receiving mailbox is unable to deliver the message. This would generate an NDR, but would not be caught by the unresolved recipients' configuration.
B. Sending a copy of the NDR's to the Administrator will not allow the users to receive the NDR's.
C. The default mailbox store is already mounted. You know this because users are able to receive email messages. The only thing that is not being delivered is the NDR's.

QUESTION 62
You are the Exchange administrator for Certkiller .
One front-end server and three back-end servers run Exchange Server 2003.
The front-end server provides remote users with access to Microsoft Outlook Web Access.
The only server that is accessible from the Internet is the front-end server.
Many users report problems to the help desk when using Outlook Web Access for the first time.
You discover that the majority of the problems are a result of the user's lack of familiarity with Outlook Web Access.
You need to ensure that users are automatically presented with a customizable Help and Outlook Web Access logon Web page.
Which two actions should you perform? (Each correct answer presents part of the solution. Choose two)

A. Enable forms-based authentication to the front-end server.
B. Enable SSL on the front-end server. Require all users to use SSL when they connect.
C. Enable SSL on all the back-end servers. Require all users to use SSL when they connect.
D. Create an Active Server Pages (ASP) sign-on page for each back-end server.
E. Set the HTTP Exchange virtual directory's Execute permissions to allow scripts.

Answer: A, B
Explanation
Enabling forms based authentication on the SMTP virtual server will allow the form to be displayed when the user attempts to connect to the OWA server. Enabling Forms Based Authentication requires that you configure SSL and restart the IIS service.
Incorrect Answers:
C. Enabling SSL on all the back end servers will have no effect, as all the external clients are connecting to the front end servers only. Remember that only the front end server connects to the back end servers, and that communication is beyond the scope of this question.
D. Creating an ASP sign-on page on the back end server is not helpful. All external clients use the front end servers to communicate; therefore, no external user would see the sign-on page created on the back end server.

E. Setting the HTTP site's virtual page to allow scripts will be automatically accomplished by allowing forms based authentication. Therefore, this is not explicitly required.
Reference
Exchange Server 2003 Administration Guide
What's New in Exchange 2003.
Exchange Server 2003 Product Help

QUESTION 63
You are the Exchange administrator for Certkiller .
The network consists of a single Active Directory domain named Certkiller .com.
The mixed-mode Exchange organization consists of two administrative groups named Toronto and Dallas.
Certkiller 's Dallas site contains a computer that runs Exchange Server 5.5.
The Toronto administrative group contains a computer named Certkiller 1 that runs Exchange Server 5.5 and a computer named Certkiller 2 that runs Exchange 2000 Server.
Certkiller 2 fails and is replaced with a new computer named Certkiller 3 that runs Exchange Server 2003.
You create an SMTP connector on Certkiller 3.
When you view the site configuration in the Exchange Administrator account on Certkiller 1, you notice that the new SMTP connector is not shown.
You need to ensure that configuration changes on the Exchange Server 2003 computers are replicated to the Exchange Server 5.5 computers.
What should you do?

A. Create a new Site Replication Service on Certkiller 3.
B. Replicate the system folders for the Toronto administrative group to Certkiller 3.
C. Create a new Active Directory Connector (ADC) recipient connection agreement for the Toronto site.
D. Modify the directory replication connectors between the Toronto and Dallas sites to use Certkiller 3 as the bridgehead server in the Toronto site.

Answer: A

Explanation:
Toronto administrative have two exchange servers one 5. 5 and one 2000, this means that between exchange 5.5 and exchange 2000 exist one SRS service, because Exchange 2000 Server computer has the Site Replication Service (SRS) installed and running on it, you must create a new SRS in Exchange System Manager, this role must be moved to the new exchange 2003 to be able to see SMTP connector
References
XADM: How to Create an Additional Site Replication Service for a Mixed Site KB 255285
XADM: How to Change the Role of a Server Within a Routing Group KB 239556
XADM: How to Rebuild a Site Replication Service Without a Backup KB 282061

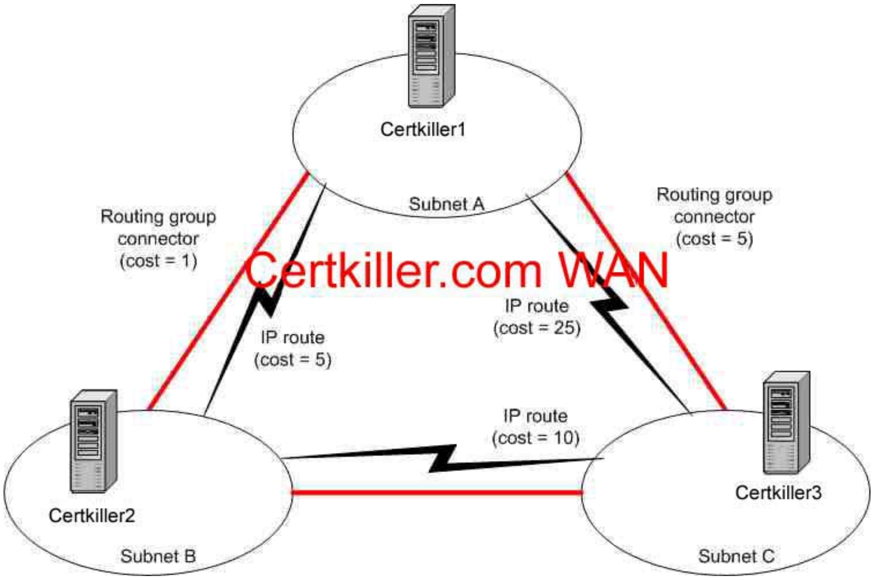
QUESTION 64
You are the Exchange administrator for Certkiller .
The company's network consists of a single Active Directory forest.
The forest contains three domains named Certkiller 1, Certkiller 2, and Certkiller 3.
The functional level of the domains is Windows 2000 mixed.

Certkiller 1 contains a single Exchange 2000 Server computer named Exch1.
Certkiller 2 contains a single Exchange 2000 Server computer named Exch2.
Certkiller 3 contains a single Exchange Server 5.5 computer named Exch3, which runs Windows 2000 Server.
Exchange 2000 Server Active Directory Connector (ADC) is installed on Exch1 and Exch2.
There is a two-way connection agreement on Exch1.
This connection agreement replicates changes between Certkiller 1 and Exch3.
There is also a two-way connection agreement on Exch2.
This connection agreement replicates changes between Certkiller 2 and Exch3.
You upgrade ADC on Exch1 to Exchange Server 2003 ADC.
The connection agreement updates and replicated normally.
Then you notice that the connection agreement on Exch2 stop replicating.
You need to ensure that all connection agreements are replicating properly.
What are two possible ways to achieve this goal? (Each correct answer presents a complete solution. Choose two)

A. Move all connection agreements from Exch2 to Exch1.
B. Upgrade ADC on Exch2 to Exchange Server 2003 ADC.
C. Promote Exch2 to a domain controller and a global catalog server.
D. Raise the functional level on Certkiller 3 to Windows 2000 native.

Answer: A, B
Explanation
Because Exch1 is already working, we can achieve the solution by moving the agreements from Exch2 to Exch1. Because of the different ADC versions are running, they also need to upgrade ADC in the Exch2 domain.
Reference
Exchange 2003 Administration guide
SECTION 5: Monitor, manage, and troubleshoot infrastructure performance (8 questions)

QUESTION 65
You are the Exchange administrator for Certkiller .
The relevant portion of the network is configured as shown in the exhibit:



Each subnet is configured as a separate routing group.
Certkiller 1 through Certkiller 3 run Exchange Server 2003.
When you monitor Certkiller 1, you discover that messages addressed to recipients on Certkiller 3 remain in the delivery queues for a long time.
You discover that these messages are delivered over the WAN link between subnet A and subnet B.
During business hours, this WAN link often has no available bandwidth.
However, the WAN link between subnet A and subnet C usually has available bandwidth.
You need to ensure that messages sent from Certkiller 1 to Certkiller 3 are delivered as quickly as possible.
What should you do?

A. Request the network administrator to increase the cost of the IP route between subnet A and subnet B to 10.
B. Request the network administrator to decrease the cost of the IP route between subnet A and subnet C to 10.
C. Increase the cost of the routing group connector between the subnet A and Subnet B routing groups to 10.
D. Decrease the cost of the routing group connector between the subnet A and subnet C routing groups to 1.

Answer: C

Explanation:
Messages are sent over routing group connectors with the lowest cost. Since the A-B-C route has a lower cost than the A-C route, messages are sent over the A-B-C route.
Incorrect Answers:

A. Changing the costs of the IP route will have no effect. Site connectors do not have anything to do with IP connectors.
B. This answer is incorrect for the same reason as "A". Site connectors and routing connectors are different, and may have costs that are completely opposite of each other.
D. Decreasing the routing group connector on the A-C subnet will only help the problem, but not resolve it.

By changing the connector cost to 1, messages will be placed in both outbound queues equally. This will solve the problem for half of the messages, but the other half would still be behind the bottleneck.
Reference:
MS white paper Exchange 2003 Transport and Routing Guide

QUESTION 66
You are the Exchange administrator for Certkiller .
The network consists of a single Active Directory domain named Certkiller .com.
You administer a single Exchange routing group named Mainoffice, which contains six Exchange Server 2003 computers.
All the Exchange servers in the Mainoffice routing group are located in the Mainoffice Active Directory, which contains two Microsoft Windows Server 2003 controllers named Certkiller 1 and Certkiller 2.
Certkiller 1 and Certkiller 2 are configured as shown in the following table.

Domain controller	**Roles**
Certkiller 1	Schema master
	Domain naming master
	Global catalog
Certkiller 2	Infrastructure master
	PDC emulator
	RID master

Users in the Mainoffice routing group report that their mail delivery is frequently slow.
You discover a large number of Exchange-related errors and warning in the event logs.
The majority of these errors and warning have an event source of either MSExchangeAl or MSExchangeDSAccess.
You need to ensure normal message delivery to local recipients in the Mainoffice routing group.
What should you do?

A. Transfer the PDC Emulator FSMO role to Certkiller 1.
B. Configure Certkiller 2 as an additional global catalog server.
C. Configure all Exchange servers to use Certkiller 2 as their configuration domain controller.
D. Configure universal group membership caching on the Mainoffice Active Directory site.

Answer: B

Explanation:
They have two Domain Controllers, Certkiller 1 and Certkiller 2. MSExchangeDSAccess is used for Exchange 2000 and Exchange 2003 to query to a domain controller who is also the global catalog, to resolve any

recipient. They have 6 exchange servers an just one DC as global catalog to manage the load, adding a second global catalog on Certkiller 2 will permit exchange to send queries to Certkiller 2 for any recipient in the case that
Certkiller 1 is not available
Adding the global catalog role to Certkiller 2 should enable Exchange to contact the global catalog regardless of which server it uses to connect.
References
How to Use Queue Viewer to Troubleshoot Mail Flow Issues KB 823489
No Such Object on the Server" Error Message Occurs When You Create a Recipient Update Service 822927
Event ID 2075 Occurs When You Try to Obtain a List of the Global Catalog Servers KB 312425
Error Message When You Restart Exchange Services If Global Catalog Cannot Be Contacted KB 273428
Exchange System Attendant Does Not Start and You Receive a "Global Catalog Servers Not Responding" Error Message KB 322801

QUESTION 67
You are the Exchange administrator for Certkiller .
The Exchange organization contains two Exchange Server 2003 computers named Certkiller 1 and Certkiller 2.
Certkiller 1 functions as a mailbox server.
Certkiller 2 is configured as a front-end server and is used to handle all Microsoft Outlook Web Access connections from the Internet.
HTTPS is not used for Outlook Web Access.
Users report that Outlook Web Access and MAPI clients are slow during times of peak network usage.
Network utilization of the Internet link does not reach capacity at these times.
Management authorizes you to add an additional Exchange server to the network, to be named Certkiller 3.
You need to ensure that performance of Outlook Web Access is improved during peak network usage.
What should you do?

A. Configure Certkiller 3 as an Exchange front-end server. Instruct half of the users to connect to Certkiller 2 when using Outlook Web Access. Instruct the other half of the users to connect to Certkiller 3 when using Outlook Web Access.
B. Configure Certkiller 3 as an Exchange front-end server. Configure a Network Load Balancing cluster that contains both Exchange front-end servers. Instruct all users to connect to the cluster name when they want to use Outlook Web Access.
C. Configure Certkiller 3 as an Exchange front-end server. Create an alias (CNAM) resource record in DNS that map to the IP addresses of both Exchange front-end servers. Instruct all users to connect to the alias when they want to use Outlook Web Access.
D. Configure Certkiller 3 as an additional mailbox server. Move half of the user mailboxes to Certkiller 3. Instruct all users to connect to Certkiller 2 when they want to use Outlook Web Access.

Answer: D

Explanation:
Users report that Outlook Web Access and MAPI clients are slow during times of peak network usage, if you

add Certkiller 3 as new front end server and configure NLB for Certkiller 2 and Certkiller 3, as mail Certkiller .com you
can tell to your users that use OWA to use mail Certkiller .com for their user connection. In this way you will reduce the OWA network traffic, balancing the network peak use between both front end servers because they tell you Network utilization of the Internet link does not reach capacity at these times. Only using NLB you will dismiss the Network load but because both server will be accessing to the same database in the back end server to *.stm, database and because MAPI clients will use *.edb database, and because by default both databases will be placed in the same disk
You will get a better I/O disk performance for MAPI users and OWA users in a 50 % of load in mail server Certkiller 1 during peak hours if you add the new server as mailbox server and move half of your users to the new server. In this way Certkiller 3 will be used by MAPI users and Certkiller 1 by OWA users
The incorrect answers:

A. The problem is not network bandwidth, so dividing the users is not necessary for that reason. In addition, HTTPS is not being used, so the load on the server should be fairly light. The question does not mention how many users, but a front end server can service thousands of clients, so it is doubtful that the server is being overworked.
B. Again, the problem is not with network bandwidth. The problem must lie someplace other than the network or the front end server. The most likely scenario is that the back end server is overworked.
C. This option would not work as the DNS alias would be on a local DNS server and not anything that would be accessible via the internet. In addition, the problem is not in the front end, but more likely in the back end.

QUESTION 68
You are the Exchange administrator for Certkiller .
The Exchange organization contains five servers that run Exchange Server 2003.
An Exchange server named Certkiller 3 functions as the public folder server.
Certkiller 3 contains 1,000 mailboxes.
Each of the other four Exchange servers contains 2,000 mailboxes.
Certkiller 3 is configured with eight physical disks, as shown in the following table.

Physical disk	**Logical disk**	**Disk contents**	**Available space**
Disk 0, Disk 1	C	System files	2 GB
(mirrored)			
Disk2	D	Paging file	3 GB
Disk3, Disk 4	E	Transaction log	12 GB
(mirrored)		files	
Disks 5-7 (RAID 5)	F	Exchange	10 GB

		databases	

The public folder store on Certkiller 3 is currently 20 GB in size.
It is growing at a rate of 100 MB per week.
The public folders on Certkiller 3 are frequently used by all users.
Most messages in the public folders include large attachments. Users frequently need to search for documents in the public folders. Each search requires more than three minutes to complete. Most searched are based on specific words. However, searches often fail to return all appropriate documents.
You enable full-text indexing on the public folder store. You restore the index files on drive E. Users now report that search results are more accurate, but each search still requires more than three minutes.
You need to ensure that public folder searches are completed as quickly as possible. You must minimize the impact on server performance for ordinary public folder and mailbox usage.
What should you do?

A. Move the index files for the full-text index to drive D.
B. Move the index files for the full-text index to drive F.
C. Move the paging file to drive E.
D. Move the transaction log files to drive F.

Answer: B

Explanation:
There is no optimal answer here. The best answer is to add another drive, and move the searches to that drive. Since that is not an option, moving the files to the fastest drive is the best answer. RAID5 will give the best performance for much frequency read and less for write of all the options listed.
Incorrect Answers:

A. Moving the index files to drive D would seriously degrade performance, as it is a single drive and already contains the operating system's paging file. In addition, the drive is not big enough, as MS states that the full text indexing will take approximately 10% of the original store's size. Since the store is 20GB, the index will take 2GB. This maxes out the drive. The first time it grows (in a week) the index drive will be out of space. Therefore, this is not the best answer.
C. Moving the paging file to drive E is not the best answer since doing that will degrade the overall server performance. MS recommends having the paging file on its own drive. By placing the page file and the transaction logs on the same drive, the paging file will become fragmented, and will cause the server to slow down. This performance degradation will affect the entire server - including Exchange. Therefore, it is not the best answer.
D. Moving the transaction log files to drive F will degrade the performance of the mailbox store. This is due to the constant writing that the transaction log will incur. This will be a bigger performance hit than
Physical disk Logical disk Disk contents Available space
Disk 0, Disk 1

(mirrored)
C System files 2 GB
Disk2 D Paging file 3 GB
Disk3, Disk 4
(mirrored)
E Transaction log
files
12 GB
Disks 5-7 (RAID 5) F Exchange
databases
10 GB
the option of moving the index to drive F. The index will not be writing constantly. The log files will be. Read operations are much faster than writes.

QUESTION 69
You are the Exchange administrator for Certkiller . The network contains a single Exchange Server 2003 computer. The Exchange server contains a single storage group that contains one mailbox store and one public folder store.
The server is configured with two logical drives. System files and Exchange transaction log files are located on drive C. Exchange database files, which have a total size of 80 GB, are located on drive D.
Except for the company's 10 managers, all users have a mailbox size limit of 100 MB. Managers have no size limit set on their mailboxes. The average mailbox size for managers is 2 GB. Managers frequently use advanced searched to locate messages in their mailboxes. Each search requires more than three minutes to complete.
You need to ensure that managers can search their mailboxes more quickly and that each manager's search includes all messages in the mailbox. Your solution must have the minimum amount of impact on e-mail performance for other users.
What should you do?

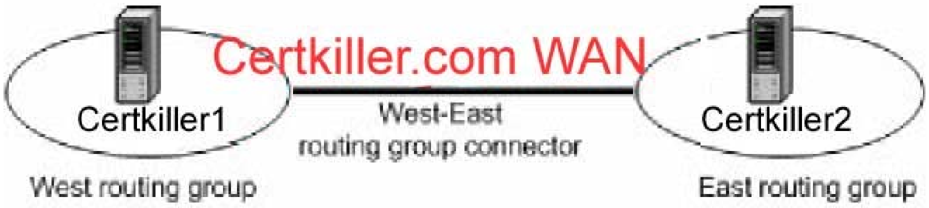
A. Create a full-text index on the mailbox store and configure full-text indexing to run once per week during non business hours.
B. Create a full-text index on the mailbox store and configure full-text indexing to run continuously.
C. Create an additional mailbox store. Move all managers' mailboxes to the new mailbox store.
Create a full-text index on the mailbox store and configure full-text indexing to run continuously.
D. Create an additional mailbox storage group and an additional mailbox store.
Move all managers' mailboxes to the new mailbox storage group.
Create a full-text index on the mailbox store and configure full-text indexing to run continuously.

Answer: C

Explanation:
To ensure that managers can search their mailboxes more quickly, and that all their messages are included in the search you must create a full-text index on the mailbox store and configure the full-text indexing to run continuously.
However, you only need the manager's messages to be indexed. Therefore you should place their mail boxes in

a separate mailbox store. This solution will have less of an impact on the e-mail performance of other users.
Incorrect Answers
A: Running the full text indexer once a week will not include all messages in index, and will give incomplete search results. Therefore it does not satisfy the requirement given in the question to ensure that each manager's search includes all messages in their mailbox.
B: Indexing the entire store will take significant CPU usage as well as hard drive time and space. It is not necessary to do full text indexing on the entire store when only the managers need this capability. The solution must have the minimum amount of impact on e-mail performance for other users.
D: Creating another storage group and mailbox store on the same disk will decrease performance.
Reference
Exchange 2003 Admin Guide

QUESTION 70
You are the Exchange administrator for Certkiller .
The network serves two offices named West and East. Each office contains an Exchange Server 2003 computer.
Each office has an Exchange routing group.
The Exchange server in the West routing group is named Certkiller 1.
The Exchange server in the East routing group is named Certkiller 2.
The Exchange topology is shown in the following diagram.



A financial application that runs on a server in the West office generates a 15-MB automated report every morning at 8:00 A.M.
The report is automatically sent from a mailbox on Certkiller 1 to a mailbox on Certkiller 2.
Because the report is not needed until the next day, it is sent with low priority.
While the message that contains the automated report is being sent, the delivery of other messages between the West and East offices is delayed.
Other users are allowed to send only messages that are smaller than 2,000 KB.
You need to ensure that the sending of the automated report does not delay the delivery of any other messages between the West and East offices.
Which two actions should you perform? (Each correct answer presents part of the solution. Choose two)

A. Configure the West-East routing group connector to deliver messages throughout the day.
B. Configure the West-East routing group connector to allow only Normal and High priority messages.
C. Configure the West-East routing group connector to use an allowed maximum message size of 2,000 KB.
D. Configure the West-East routing group connector to use a custom schedule that allows message delivery only after 6.00 P.M.
E. Configure the West-East routing group connector to use a custom schedule that allows message delivery only after 6:00 P.M. for messages larger than 15,000 KB.

Answer: C, E
Explanation
Because users are only allowed to send messages that are smaller than 2,000 KB you cannot configure the West-East routing group connector to deliver messages throughout the day as this will permit will permit messages to exceed the 2,000 KB limit. We need to limit users to 2,000 KB
Also you need to ensure that the sending of the automated report does not delay the delivery of any other messages between the West and East offices you do not need to send the report until the next day, you will need to send it with low priority.
Reference
Exchange server 2003 Admin Help

QUESTION 71
Certkiller operates two offices and has a single Exchange organization.
You are the Exchange administrator in the Los Angeles office.
Another Exchange administrator is responsible for the other office in Boston. Both Exchange administrators are members of a mail-enabled universal group named ExchAdmins.
Each office contains five servers that run Exchange Server 2003.
Each office is configured as a separate routing group and a separate administrative group. One server in each office is a bridgehead server for the routing group.
The routing groups are connected by a routing group connector.
You need to ensure that the Exchange administrators are notified whenever e-mail services between the two offices are disrupted.
Which two actions should you perform? (Each correct answer presents part of the solution. Choose two)

A. Add a new resource to monitor the status of the SMTP queue on each bridgehead server. Configure the new resource to reach a warning state if the SMTP queue continues to grow for 10 minutes.
B. Add a new resource to monitor the status of the X.400 queue on each bridgehead server. Configure the new resource to each a warning state if the X.400 queue continues to grow for 10 minutes.
C. Add a new resource to monitor the status of the Microsoft Exchange Information Store service on each bridgehead server. Configure the new resource to each a warning state when the Microsoft Exchange Information Store service shuts down.
D. Configure one e-mail notification to monitor both bridgehead servers by using one bridgehead server as the monitoring server. Configure the notification to send an e-mail message to the ExchAdmins group when monitored items reach a warning state.
E. Configure one e-mail notification to monitor both bridgehead servers by using the bridgehead server in your routing group as the monitoring server. Configure another e-mail notification to monitor both bridgehead servers by using the bridgehead server in the other routing group as the monitoring server. Configure both notifications to send an e-mail message to the ExchAdmins group when monitored items reach a warning state.

Answer: A, E

Explanation:
One of the steps should be to monitor the SMTP status on each bridgehead server. A growing SMTP queue is an indicator that the connector has failed due to the fact that the queue is the number of mail messages waiting to be delivered. If this queue continues to grow for 10 minutes, then there is probably a problem in the link.

In order for the monitoring to correctly take place, a notification must be sent if the warning state triggered in answer "A" is reached. Simply monitoring the queue is not enough. A message must be sent to notify the administrator of the problem. Note that the warning must be set up on each server, since the connector's being down would prevent one administrator from receiving the message.
Incorrect answers:
B. Monitoring the X.400 queue would not make any difference since SMTP uses X.500 to communicate. Furthermore, since there is no x.400 connector between the sites, it would never register as being down to the x.400 queue.
C. If the connector fails, the Exchange Store will not shut down; it will simply store the messages until the connector is restored. Therefore, this would not be a good event to monitor.
D. Using one bridgehead server as the monitoring server is not sufficient. If the disruption is caused by a bridgehead server going down, and that is the server doing the monitoring, there would be no notification sent. In short, there is a "hole" in the coverage.
Reference
Exchange 2000 Chapter 4 - Enterprise Monitoring

QUESTION 72
You are the Exchange administrator for Certkiller .
All network computers are members of a single Active Directory domain named Certkiller .com.
The company has one regional office, which is connected to the central office by a WAN connection. Each office has its own intranet.
Network characteristics are shown in the following table.

Office	**Servers running Exchange Server**	**Domain**	**Users**
	2003	**controllers**	
Central Office	5	10	12,000
Regional	2	3	8,000
Office			

The sales department is located in the main office.
An Exchange Server 2003 computer named Exch3 contains all mailboxes for users in this department.
Currently, company users do not have public folders.
The sales department purchases a custom application that is based on Exchange public folders. Another administrator creates a new public folder for sales department users and installs the custom application in the public folder.
Three weeks later, you discover that the WAN connection and the intranets have high volumes of network traffic associated with public folder replication.
You need to reduce the replication traffic as much as possible, without affecting the ability of sales users to access the custom application in Microsoft Outlook.
What should you do?

A. Configure public folder replication to use low priority replication.
B. Remove the public folder replicas from all Exchange servers except Exch3.

C. Make the sales public folder available only on Exch3 and on one Exchange server in the branch office.
D. Remove the custom application from the sales public folder. Create a new Exchange server in the main office and place the new server in a new Exchange organization. Install the application on the new server.

Answer: B

Explanation:
The question deals with the high volume of replication traffic.
To reduce the traffic, you need to reduce the amount of replication traffic generated. The sales department is located in the main office. An Exchange Server 2003 computer named Exch3 contains all mailboxes for users in sales department. There are no users of sale department in regional office, therefore, we can remove the public folder replicas

---

QUESTION 73
You are an Exchange administrator for Certkiller .
The Exchange organization contains an Exchange Server 2003 computer named Certkiller 2.
Certkiller 2 is configured as a front-end server that hosts only Microsoft Outlook Web Access.
A firewall is configured to reverse proxy HTTP requests to Certkiller 2.
All users access Certkiller 2 from the Internet.
Several internet e-mail messages are intercepted from Certkiller 2 by unauthorized users.
To improve security, another administrator reconfigures Certkiller 2 to accept SSL connections. The administrator successfully tests the new configuration by connecting to Certkiller 2 from the internal network.
However, users report that they cannot connect to Certkiller 2 by using a secure connection. They can still establish an unsecured connection.
You need to ensure that all users can establish secure connections to Certkiller 2.
What should you do?

A. Configure the firewall to block incoming HTTP traffic.
B. Configure the firewall to allow HTTPS traffic to pass from the Internet to Certkiller 2.
C. Configure Certkiller 2 to use IPSec to secure communications between Certkiller 2 and the firewall.
D. Configure Certkiller 2 to trust the certification authority (CA) that issued the SSL certificate.

Answer: B

Explanation:
Since the administrator was able to successfully test the connection, it must be assumed that he was able to connect via HTTPS. This is proof that the SSL configuration is correct. All that needs to be done is to allow HTTPS traffic from the internet.
Incorrect Answers:

A. Blocking HTTP traffic has nothing to do with allowing HTTPS traffic to pass.
C. Using IPSec is not needed since SSL has been implemented, and will not help remote users to connect.

D. The trust of the CA must already be in place on the server since the administrator was able to connect successfully. If Certkiller 2 did not have this trust, the administrator's test would have failed.

QUESTION 74

You are the Exchange administrator for Certkiller .
Certkiller has a perimeter network that is protected by firewalls.
The perimeter network contains all computers that are accessible from the Internet.
One of these computers is an Exchange Server 2003 front-end server named Certkiller 1.
Certkiller 1 handles all communication between the Internet and the company's Exchange organization.
Certkiller 1 is used for all Microsoft Outlook Web Access connections and also functions as a bridgehead server for incoming SMTP traffic.
The secure server IPSec policy has been configured on Certkiller 1 to limit the TCP ports to which network connections can be made.
Written company policy specifies that SSL encryption must be used for all Outlook Web Access sessions.
Users report that they cannot access e-mail messages by using Outlook Web Access over the Internet.
You verify that you can open Outlook Web Access locally using a Web browser on Certkiller 1.
You test connectivity to Certkiller 1 from another computer in the perimeter network.
You discover the following facts.

- You cannot open Outlook Web Access.
- You can connect to Certkiller 1 by using SMTP.
- You cannot connect to Certkiller 1 by running the ping command.
- You can open the other Web sites on Certkiller 1 that do not require SSL encryption.

You need to ensure that users can connect to Outlook Web Access on Certkiller 1.
Your solution must comply with company security policy.
What should you do?

A. Disable SSL on the Exchange HTTP virtual server.
B. Configure the IPSec policy on Certkiller 1 to allow incoming HTTPS traffic.
C. Configure new filters on the firewalls that protect the perimeter network to allow incoming HTTPS traffic.
D. On Certkiller 1, create a new Exchange HTTP virtual server that is configured to require SSL encryption of traffic.

Answer: B

Explanation:
The issue in this case is that the Secure Server IPSec policy is not allowing unencrypted traffic to flow into the server.
IPSEC default rules permit

- IP Protocol ID 50: For both inbound and outbound filters. Should be set to allow Encapsulating Security Protocol (ESP) traffic to be forwarded.
- IP Protocol ID 51: For both inbound and outbound filters. Should be set to allow Authentication Header (AH) traffic to be forwarded.
- UDP Port 500: For both inbound and outbound filters. Should be set to allow ISAKMP traffic to be forwarded.

L2TP/IPSec traffic looks just like IPSec traffic on the wire. The firewall only has to allow IKE (UDP 500) and

IPSec ESP formatted packets (IP protocol = 50). Since HTTPS traffic does not communicate via IPSec, this traffic is being dropped. In addition, the IPSec Secure Server policy does not allow for ICMP traffic, which explains why the Ping command does not work.
Adding the allowance of HTTPS traffic will enable the server to communicate successfully.
Incorrect Answers:

A. Disabling SSL on the server will break company policy by preventing the OWA clients from connecting securely. Therefore, this answer can't be correct.
C. Since you can't connect to Certkiller 1 from another computer in the perimeter network, the firewall can't be the problem. Therefore, this answer can't be correct.
D. Creating another HTTP virtual server on Certkiller 1 would not resolve the problem. This virtual server would have the same issues that the original server had. There is no reason to believe that another virtual server would resolve the problem since the issue exists within the perimeter network.
Reference
How to Enable IPSec Traffic through a Firewall 233256

QUESTION 75
You are the Exchange administrator for Certkiller .
The intranet is connected to the Internet through a firewall.
The Exchange organization contains two servers named Certkiller 1 and OWA1.
Both servers run Exchange Server 2003. Certkiller 1 is configured as a mailbox server.
OWA1 is configured as a front-end server.
OWA1 is configured to allow users to access their e-mail by using Microsoft Outlook Web Access over SSL.
Internet users report that they cannot access OWA1.
However, intranet users can use either HTTP or HTTPS to access Outlook Web Access.
You need to ensure that all users can access Outlook Web Access by using only HTTPS.
What should you do?

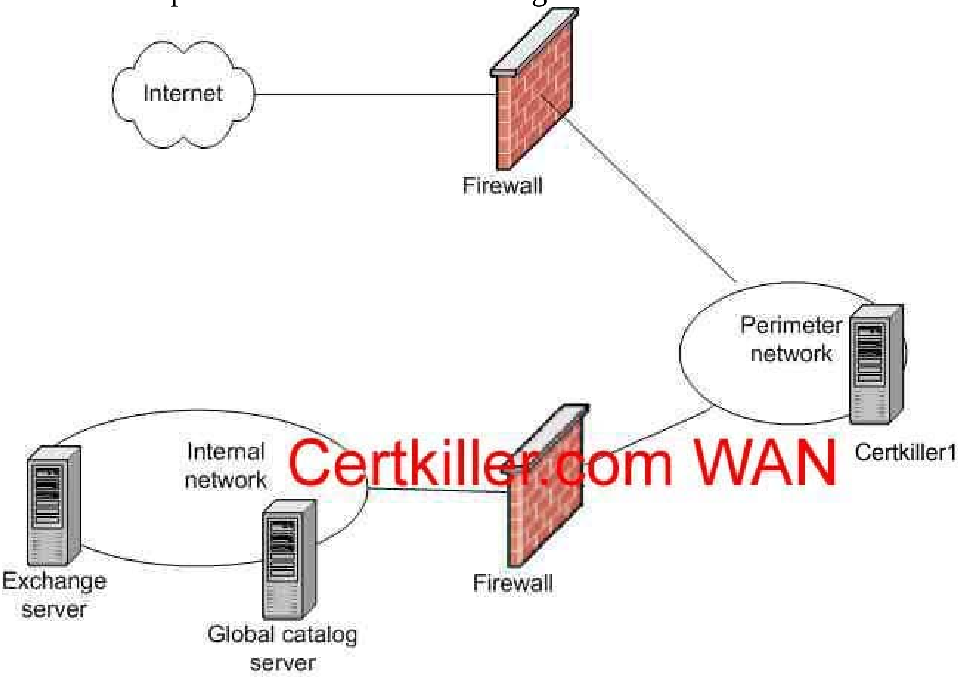
A. Configure the firewall to permit Internet users to access port 443 on OWA1. Configure the default Web site on OWA1 to require SSL.
B. Configure the firewall to permit Internet users to access port 80 on OWA1. Configure the default Web site on Certkiller 1 to use port 443 for SSL communications.
C. Configure the firewall to allow Internet users to access port 993 on OWA1. Configure the default Web site on Certkiller 1 to require SSL and 128-bit encryption.
D. Configure the firewall to allow Internet users to access port 143 on OWA1. Configure the Exchange HTTP virtual server on OWA1 to enable forms-based authentication for Outlook Web Access.

Answer: A

Explanation:
SSL utilizes port 443. The external firewall does not currently allow traffic on port 443 to pass. Opening up this port will take care of that issue. The default OWA site is currently not correctly setup to use HTTPS. This is why internal clients can connect to OWA using HTTP. Modifying the security on the OWA web site will solve this problem.
Incorrect Answers:

B. Port 80 is used for standard HTTP traffic. Allowing it will not satisfy the requirement of HTTPS traffic being passed only.
C. Port 993 is used for secure IMAP traffic. Enabling it will not allow HTTPS traffic.
D. Port 143 is used for insecure IMAP traffic. It will have no effect on HTTPS traffic.
Reference:
MS white paper Exchange Server 2003 RPC over HTTP Deployment Scenarios
MS white paper Exchange Server 2003 Client Access Guide
MS white paper Exchange 2003 Front-End Back-End Topology

QUESTION 76
You are the Exchange administrator for Certkiller .
All Exchange servers run Exchange Server 2003.
The relevant portion of the network configuration is shown in the exhibit.



Certkiller C is a front-end server.
Its only function is to enable Internet users to access their Exchange mailboxes by using Microsoft Outlook Web Access over SSL- Internet users report that they cannot access their mailboxes.
They receive an error message stating that the page or server cannot be located.
You discover that internal users can access Certkiller C and can use Outlook Web Access.
You need to ensure that Internet users can access their e-mail.
To achieve this goal, you plan to reconfigure the Internet firewall so that Internet users can access only one port on Certkiller C.
Which protocol should be accessed by Internet users?

A. HTTP
B. IMAP4
C. HTTP SSL
D. IMAP4 SSL

Answer: C

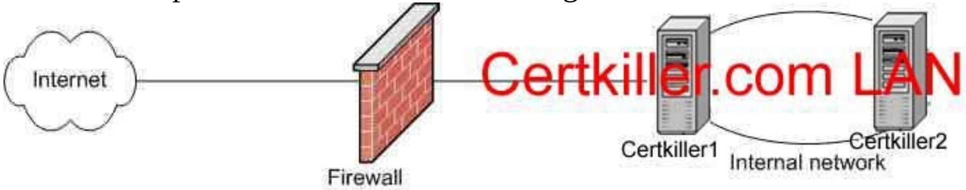
Explanation:
HTTP SSL use port 443. The external firewall does not currently allow on port 443 traffic to pass. Reconfigure Internet firewall on port 443 will permit to Internet users to access by OWA to Certkiller C.
Ports to open for OWA access in a perimeter Firewall architecture

Origin	**Destination**	**Service**	**Protocol and port**
Internal/External	Perimeter	HTTP	TCP 80
	network	HTTPS	TCP 443
		IMAP4	TCP 143
		IMAP4TLS	TCP 993
		DNS	TCP, UDP 53
		HTTP	TCP 80
		RPC	TCP 135
Perimeter	Network	EndPoint	
Network	Internal/Private	Mapper	
		KERBEROS	TCP UDP 88
		LDAP	TCP 389
		NETLOGON	TCP 445
		DSAccess	TCP 3268
		(GC)	
		TCP High Ports	TCP 1024+

Reference:
MS white paper Exchange Server 2003 RPC over HTTP Deployment Scenarios
MS white paper Exchange Server 2003 Client Access Guide
MS white paper Exchange 2003 Front-End Back-End Topology

QUESTION 77
You are the Exchange administrator for Certkiller .

The Exchange organization contains two servers named Certkiller 1 and Certkiller 2.
Both servers run Exchange Server 2003.
The relevant portion of the network is configured as shown in the exhibit.



Certkiller 1 is configured as a front-end server.
Certkiller 1 supports only IMAP e-mail clients.
Certkiller 2 supports both IMAP4 and IMAP4 over SSL.
Certkiller 2 is configured as a back-end server.
It hosts user mailboxes and public folders.
You need to ensure that all users can send and receive Internet e-mail messages by accessing Certkiller 1.
Your solution must not open any unnecessary network ports.
Which protocol or protocols should you open on the firewall? (Choose all that apply)

A. SMTP
B. POP3
C. HTTPS
D. IMAP4
E. IMAP4 over SSL
F. POP3 over SSL

Answer: E

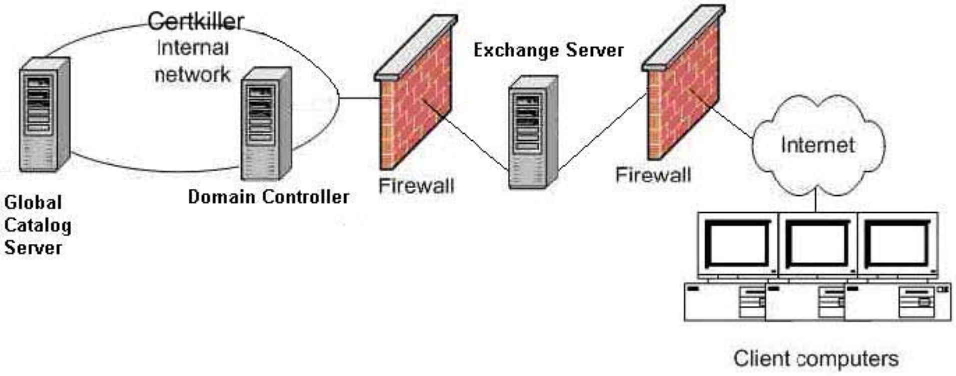
Explanation:
You need to ensure that all users can send and receive Internet e-mail messages by accessing Certkiller 1. In order not to open more ports than necessary, we can close IMAP port and use https but they told us Certkiller 1 supports only IMAP e-mail clients and there is not any statement about Certkiller 1 being reconfigured.
Therefore, we can close IMAP port 143 and leave only IMAP over SSL port 993.
Ports to open for OWA access in a perimeter Firewall architecture

Origin	**Destination**	**Service**	**Protocol and port**
Internal/External	Perimeter	HTTP	TCP 80
	network	HTTPS	TCP 443
		IMAP4	TCP 143
		IMAP4TLS	TCP 993
		DNS	TCP, UDP 53
		HTTP	TCP 80

		RPC	TCP 135
Perimeter	Network	EndPoint	
Network	Internal/Private	Mapper	
		KERBEROS	TCP UDP 88
		LDAP	TCP 389
		NETLOGON	TCP 445
		DSAccess	TCP 3268
		(GC)	
		TCP High	TCP 1024+
		Ports	

Reference:
MS white paper Exchange Server 2003 RPC over HTTP Deployment Scenarios
MS white paper Exchange Server 2003 Client Access Guide
MS white paper Exchange 2003 Front-End Back-End Topology

QUESTION 78
You are the Exchange administrator for Certkiller .
Exchange Server 2003 is implemented as the companywide messaging system.
The Exchange server runs Windows 2000 Server.
The relevant portion of the network is configured as shown in the exhibit.



Certkiller e-mail policies state that Internet users must be able to securely download e-mail messages, view downloaded e-mail messages on their local computers, send outbound e-mail messages, and access the company's internal e-mail address list.
You need to configure the firewall to meet these requirements.
Which three ports should you make accessible to Internet users? (Each correct answer presents part of

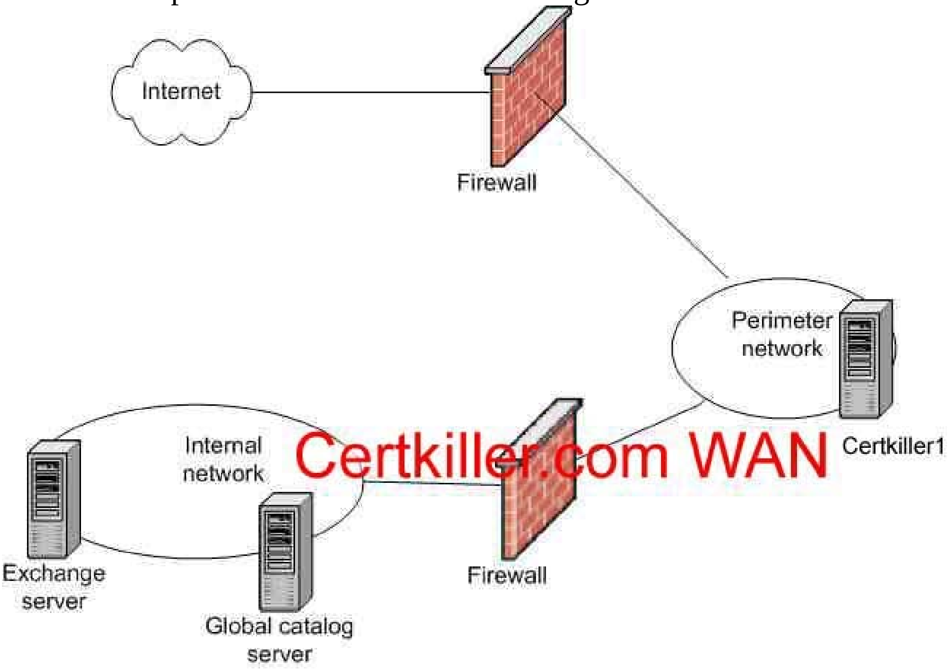
the solution. Choose three)

A. Global catalog LDAP
B. HTTPS
C. RPC endpoint mapper
D. IMAP4 SSL
E. SMTP

Answer: A, B, C

Explanation:
The trick in this question is Exchange is running on Windows 2000 Server. We can't uses HTTPS over RPC, which is new in Exchange 2003 and Windows 2003 Architectures.
Reference:
MS white paper Exchange Server 2003 RPC over HTTP Deployment Scenarios
MS white paper Exchange Server 2003 Client Access Guide
MS white paper Exchange 2003 Front-End Back-End Topology

QUESTION 79
You are the Exchange administrator for Certkiller .
The network consists of as single Active Directory domain named Certkiller .com.
Exchange Server 2003 is implemented as the companywide messaging system.
The relevant portion of the networks is configured as shown in the exhibit.



Certkiller 1 is configured as a front-end server and as an incoming SMTP relay.
It also hosts Microsoft Outlook Web Access, which is used by Internet users to access company e-mail.
Users stop receiving e-mail messages from the Internet.
You use the DNS name and IP address to send test e-mail messages directly to Certkiller 1 from the Internet.

However, your e-mail messages are simply queued on Certkiller 1 along with a large number of other messages.
You need to ensure that users can receive e-mail messages from the Internet.
What should you do?

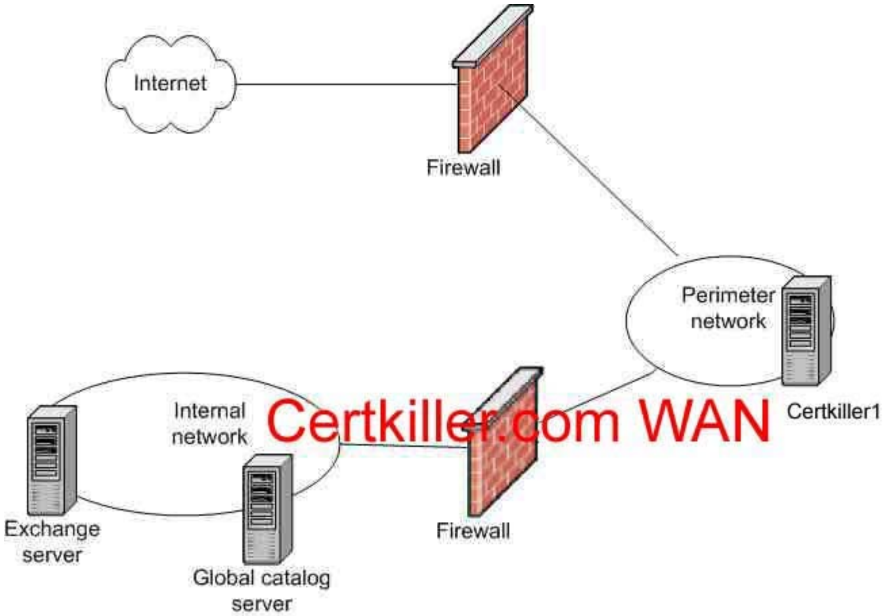
A. Configure the external DNS mail exchanger (MX) resource record of the e-mail domain to point to Certkiller 1.
B. Configure the internal firewall to allow Certkiller 1 to communicate with the Exchange server and the global catalog server.
C. Configure the default SMTP virtual server on Certkiller 1 to use the Exchange server as a smart host server.
D. Configure the default SMTP virtual server on Certkiller 1 to deliver all e-mail messages that have unresolved recipients to the Exchange server.

Answer: B

Explanation:
Certkiller 1 is not able to see either the back-end Exchange Server or the Global Catalog server. Opening the appropriate ports on the internal firewall should resolve the problem.
Incorrect answers:

A. Mail is being received by Certkiller 1, hence the MX record must exist and be correct.
C. Since no SMTP traffic is passing between the servers, setting up a smart host on Certkiller 1 will not work.
D. Messages sitting in the queue on Certkiller 1 have recipients. Therefore, this answer can't be correct. Note that the users state that they are not receiving e-mail. If the messages had no recipient, the users would not be aware that they were not getting their messages.
Reference:
MS white paper Exchange Server 2003 RPC over HTTP Deployment Scenarios
MS white paper Exchange Server 2003 Client Access Guide
MS white paper Exchange 2003 Front-End Back-End Topology

QUESTION 80
You are the Exchange administrator for Certkiller .
Exchange Server 2003 is used as the companywide messaging system.
The relevant portion of the network is configured as shown in the exhibit.



The front-end server provides e-mail access to HTTPS, IMAP4, and POP3 clients.
The front-end server also hosts a secure Web site for customers.
Some remote users report that they cannot access their e-mail from the Internet.
You discover that this problem affects only the users of the HTTPS e-mail clients.
All users can still access their e-mail from the internal network by using Microsoft Outlook directly connected to the Exchange mailbox servers.
You discover that the customer Web site is accessible from the Internet by using HTTPS.
You need to ensure that all users can access their e-mail from the internal network and from the Internet.
What should you do?

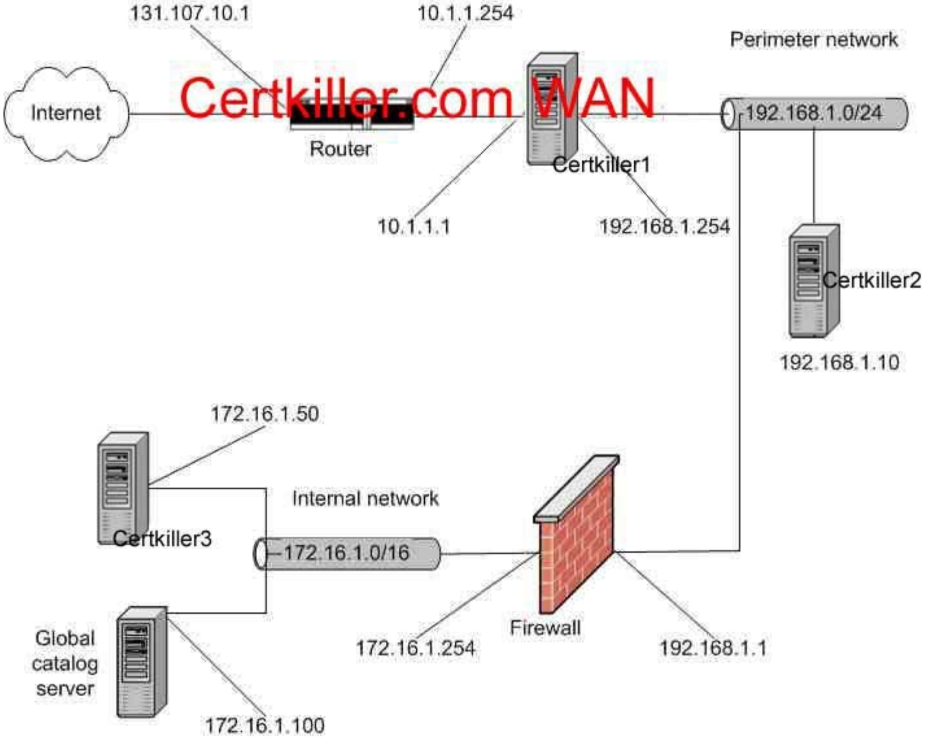
A. Allow the front-end server to initiate connections with all Exchange servers on the internal network by using the IMAP4 SSL port.
B. Allow the front-end server to initiate connections with all Exchange servers on the internal network by using the IMAP4 port.
C. Allow the front-end server to initiate connections with all Exchange servers on the internal network by using the HTTP port.
D. Allow the front-end server to initiate connections with all Exchange servers on the internal network by using the HTTPS port.

Answer: D

Explanation:
Outlook 2003, can connect using POP, IMAP or HTPPS over RCP protocols, Outlook Express can connect using POP and IMAP protocols, and OWA can connect using http and https. However, you must not use http because is not secure. A secure option is to logon in the front end server.
They can access to front-end server a secure Web means HTTPS is working correctly, but this site can be in a different IP for this secure Web site over port 443 and is not closed for this site but because you discover that this problem affects only the users of the HTTPS e-mail clients. This means that OWA site for HTTPS port is closed for the default web site
Reference:

MS white paper Exchange Server 2003 RPC over HTTP Deployment Scenarios
MS white paper Exchange Server 2003 Client Access Guide
MS white paper Exchange 2003 Front-End Back-End Topology

QUESTION 81
You are the Exchange administrator for Certkiller .
The network consists of a single Active Directory domain named Certkiller .com.
Exchange Server 2003 is used as the companywide messaging system.
The relevant portion of the network is configured as shown in the exhibit.



Certkiller 1 runs Microsoft Internet Security and Acceleration Server.
Certkiller 2 is configured as a front-end server that runs Microsoft Outlook Web Access. Certkiller 1 is configured to permit Internet users to access their e-mail by using Outlook Web Access on Certkiller 2.
Certkiller 1 also permits Internet mail servers to send SMTP mail to Certkiller 3.
Users report that they cannot access Certkiller 2 from the Internet.
However, the same users can successfully access Certkiller 2 from the internal network.
You discover that all Internet mail servers can successfully sent SMTP mail to Certkiller 3.
You need to ensure that all users can access Certkiller 2 from the Internet and from the internal network.
What should you do?

A. Configure the network adapter on Certkiller 2 to use both 192.168.1.254 and 192.168.1.1 as default gateways.
B. Configure the network adapter on Certkiller 2 to use 192.168.1.254 as the default gateway. Configure a static route to the 172.16.1.0/16 network by using 192.168.1.1 as the gateway.
C. Configure the perimeter network adapter on Certkiller 1 to use 192.168.1.1 as the default gateway.

Configure the Internet-facing network adapter to use 10.1.1.254 as the default gateway.
D. Configure the Internet-facing network adapter on Certkiller 1 to use 10.1.1.254 as the default gateway. On the perimeter network adapter, configure a static route to the 172.16.1.0/16 network by using 192.168.1.1 as the gateway.

Answer: B

Explanation:
After you set the external NIC on the ISA Server computer to use an Internet IP address, you need to configure ISA Server to listen on that IP address for incoming Web requests. This configuration is necessary for ISA Server to respond to Web page requests such as Outlook Web Access or Outlook Mobile Access traffic.
Make sure the IP address of the ISA Server computer's internal NIC is static. This configuration is necessary because you need to configure secure network address translation (SecureNAT) clients, such as your inbound SMTP server, and point them to the internal IP address of your ISA Server. If the IP address on your internal NIC changes, you need to manually update those clients. When you use a static IP address, you avoid this problem.
After you place your ISA Server computer in the perimeter network and configure your internal and external NICs, ISA Server is ready to start acting as the gatekeeper for inbound and outbound Internet traffic. To do this, you need to configure inbound and outbound e-mail traffic to go through ISA Server.
All inbound Internet traffic bound to your Exchange servers, such as Microsoft Office Outlook(r) Web Access, RPC over HTTP communication from Microsoft Office Outlook 2003 clients, Outlook Mobile Access, Post Office Protocol version 3 (POP3), Internet Message Access Protocol version 4rev1 (IMAP4), and so on are processed by ISA Server. When ISA Server receives a request from a client application such as Outlook 2003 to access information on an Exchange server, ISA Server routes the request to the appropriate Exchange servers on your internal network. The internal Exchange servers return the requested data to ISA Server, and then ISA Server sends the information to the client through the Internet.
Incorrect Answers:

A. Configuring two gateways is not a good idea. Messages can (and will) be sent to whichever gateway happens to be chosen. Sometimes it will be correct, and other times it will not. In any event, this does not lead to the best answer.
C. The perimeter network adapter on Certkiller 1 is functioning as it should. We know this because internet SMTP mail is getting where it needs to go. Therefore, this can't be the correct answer.
D. The adapters on Certkiller 1 are functioning as they should. If they were not, Certkiller 3 would not be getting SMTP mail. In addition, setting up the adapter this way would prevent Certkiller 3 from receiving the SMTP mail, as it would be routed to Certkiller 2. Since Certkiller 2 is not configured to send SMTP mail (only HTTP for OWA) the inbound mail will die at Certkiller 2.
Reference
Using ISA Server 2000 with Exchange Server 2003 MS white paper

---

QUESTION 82
You are the Exchange administrator for Certkiller .
The network consists of a single network subnet connected to the Internet by means of a firewall.
The network contains two Exchange Server 2003 computers named Certkiller 1 and Certkiller 2. Certkiller 1 contains all user mailboxes.
Certkiller 2 is configured as a front-end server and hosts Microsoft Outlook Web Access.

The firewall is configured to allow incoming HTTPS traffic to Certkiller 2.
The network is reconfigured to include a perimeter network.
The perimeter network is connected to the internal network by means of a new firewall.
Certkiller 1 remains on the internal network, and Certkiller 2 is relocated to the new perimeter network.
Internet users now report that Outlook Web Access in inaccessible.
You confirm that all services on Certkiller 2 start normally and that internal users can access their mail by using Microsoft Outlook to connect to Certkiller 1.
You need to ensure that Internet users can access Outlook Web Access over an encrypted connection.
What should you do?

A. Configure the internal firewall to allow HTTP traffic to pass from Certkiller 2 to Certkiller 1.
B. Configure the external firewall to allow HTTP traffic to pass from the Internet to Certkiller 2.
C. Configure the internal firewall to pass LDAP queries from Certkiller 2 to a domain controller on the internal network.
D. Configure the external firewall to allow RPC traffic to pass from the Internet to Certkiller 2.

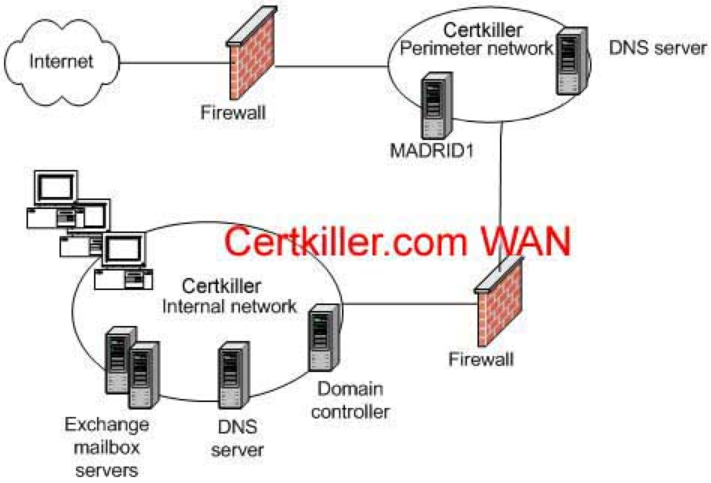
Answer: D

Explanation:
The Microsoft remote procedure call (RPC) over Hypertext Transfer Protocol (HTTP) implementation (RPC/HTTP) allows RPC clients to more securely and efficiently connect across the Internet to RPC server programs and execute remote procedure calls.
Because they do not tell us that they are using an ISA firewall we must assume that they are using RCP over http or classic approach
The classic approach require following ports:
Reference
Exchange 2003 Deployment guide
Planning Outlook Web Access Servers
Exchange 2003 RPC over HTTP Deployment Scenarios
Exchange Server 2003 Message Security Guide
Using ISA Server with Exchange 2003
Source Destination Service Protocol and port

Internet/External	Perimeter Network	HTTP HTTPS	port TCP 80 TCP 443
		IMAP4	TCP 143
		IMAP4TLS	TCP 993
Perimeter Network	Internal/Private Network	DNS HTTP	TCP, UDP 53 TCP 80
		RPC EP Mapper KERBEROS	TCP 135 TCP UDP 88

		LDAP	TCP 389
		NETLOGON	TCP 445
		DSAccess (GC) TCP High Ports	TCP 3268 TCP 1024+

QUESTION 83
You are the Exchange administrator for Certkiller .
The network consist of a single Active Directory domain named Certkiller .com. Exchange Server 2003 is used as the companywide messaging system.
The Exchange organization includes two mailbox servers.
The perimeter network contains one front-end server named madrid1. Certkiller .com, which hosts Microsoft Outlook Web Access.



The external firewall is configured to allow limited access to the servers on the perimeter network and the internal network. Internet users access all servers behind the external firewall by using the IP address of the firewall's external interface.
The internal firewall is configured to allow limited access to the servers on the internal network by using the actual IP address of each internal servers.
Users report that they cannot access madrid1. Certkiller .com from the internal network or the Internet.
Which two actions should you perform? (Each correct answer presents part of the solution. Choose two)

A. On the perimeter DNS server, configure a new host (A) resource record that maps madrid1. Certkiller .com to the IP address of the external interface of the external firewall.
B. On the perimeter DNS server, configure a new host (A) resource record that maps madrid1. Certkiller .com to the actual IP address of the server.
C. On the internal DNS server, configure a new host (A) resource record that maps madrid1. Certkiller .com to the IP address of the external interface of the external firewall.
D. On the internal DNS server, configure a new host (A) resource record that maps madrid1. Certkiller .com to the actual IP address of the server.

Answer: A, D

Explanation
In this scenario, we have OWA in the perimeter zone. We have two network cards, one is connected to internal network, and the other is the external IP address that is accessed from Internet.
If we would like to provide access to the OWA in the perimeter zone, we need to provide DNS resolution for their IP address in the internal network, to do that we just need to add their IP address to our internal DNS.
If we would like to provide external access from internet we need to provide DNS resolution form our external DNS to the external IP address of the OWA server.
References
Planning an Exchange Server 2003 http://www.microsoft.com/exchange/library

---

QUESTION 84
You are the Exchange administrator for Certkiller .
The Exchange organization contains a single server named Certkiller 3.
Certkiller 3 runs Exchange Server 2003 and hosts all user mailboxes.
Certkiller 3 also functions as an SMTP gateway for Internet e-mail.
A firewall separates the internal network from the Internet and allows only SMTP traffic to each Certkiller 3.
One afternoon, users report extremely slow response times on Certkiller 3.
Some users cannot access the server at all.
You examine network traffic to Certkiller 3 and conclude that the server is the target of an external distributed denial of service (DDoS) attack.
Your immediate need is to prevent the attack from affecting Certkiller 3. You must minimize the effect of your actions on internal e-mail users.
What should you do?

A. Stop the SMTP service on Certkiller 3.
B. Reconfigure Certkiller 3 to prohibit all POP3 and IMAP connections.
C. Reconfigure the firewall to prohibit all incoming SMTP traffic.
D. Reconfigure Certkiller 3 to accept only POP3 connections.
Instruct users to access Certkiller 3 by using POP3 client software.
E. Configure TCP/IP filtering on Certkiller 3 to permit only RPC traffic.

Answer: C
Explanation
The primary goal should be to stop the denial of service attack of the Exchange Server. The most efficient way to do this WITHOUT affecting the internal E-mail users is to shut down the SMTP traffic by reconfiguring the firewall to block SMTP traffic.
Incorrect answers:

A. Stopping the SMTP service will also shut down all the internal mail, which violates the last requirement of the question.
B. Prohibiting IMAP and POP3 connections will not prevent the incoming SMTP traffic. The SMTP traffic is the root of the DDoS attack.
D. While this would stop the DDoS attack, it would require a lot of reconfiguration on the clients, and hence disrupt all the internal e-mail users. This is a violation of the last requirement of the question.
E. Only allowing RPC traffic would prevent internal clients from connecting. Remember that internal

clients will be using SMTP to communicate. Allowing ONLY RPC traffic will prevent the internal users from connecting to the Exchange server.

QUESTION 85

You are the Exchange administrator for Certkiller .
The company network consists of a single Active Directory domain that contains two domain controllers.
A member server named Exch1 runs Exchange Server 2003 and hosts all user mailboxes.
All member servers and domain controllers implement security auditing.
A user named Dr King reports that some of his e-mail messages are missing.
Other messages are marked as read, although King did not read them.
You suspect that an unauthorized user is accessing King's mailbox when King is out of the office.
You need to save the appropriate log file or event log file to provide evidence of a security breach.
What should you do?

A. Save the security event log from Exch1.
B. Save the application event log from Exch1.
C. Save the message tracking log and the SMTP communications log from Exch1.
D. Save the security event log and the application event log from one domain controller.

Answer: D

Explanation:
They do not tell us if the domain controllers are running Windows 2000 or Windows server 2003, we must assume Windows 2003 because they are running Exchange 2003.
You need to setup the security audit in the domain controllers or best and less work in the domain controller's policy, after setup security policy you will can lookup for security break
Incorrect answers:

A. Security log will be local server related
B. Application log will be local related
C. Track messages is used to track bad mail delivery

QUESTION 86

You are the Exchange administrator for Certkiller .
The network contains four Exchange Server 2003 computers that are located in a single organizational unit (OU) in Active Directory.
Users who work during the night shift report that the Exchange servers are often not available at night.
You use System Monitor and find out that the Exchange services have been running for less than 24 hours.
You need to ensure that the security logs contain information necessary to isolate events that affect server uptime.
What should you do?

A. Configure an audit policy that logs successful logon events.
B. Configure an audit policy that logs successful system events.
C. Configure a security policy that audits the use of global system objects.

D. For the Microsoft Exchange Information Store service, configure the diagnostic logging category named General to the medium logging level.

Answer: C
They tell us you need to ensure that the security logs contain information necessary to isolate events that affect server uptime. To write to security events logs, you must use an audit policy because diagnostic logging category named General to the medium logging level will write Windows 2000 or 2003 application event logs, not security as is required.
Incorrect answers

A. Logon-related events when a user logs on interactively or remotely. These events are generated on the computer to which the logon attempt was made. By Login successful events you get just who user access with right access to do logon in the system
B. Tracks system events such as Windows logon network and power events. Notifies COM+ Events
D. Answer D is vague because MSExchangeIS have one general category for each three options: System, Public Folder, and Mailbox.
Reference
Exchange 2003 server Help
Windows 2003 Server Help

QUESTION 87
You are the Exchange administrator for Certkiller .
The network consists of a single Active Directory domain named Certkiller .com.
The network contains nine Exchange Server 2003 computers running on Microsoft Windows Server 2003 member servers.
All Exchange servers are in a single organizational unit (OU) named Exchange Servers.
Only the Exchange server computer objects are contained in the Exchange Servers OU.
Users in a group named Exchange Admins are exclusively responsible for managing the Exchange organization.
No other group, including the Enterprise Admins and Domain Admins groups, has permissions to manage the Exchange organization.
You discover that the Domain Admins group is in the membership list of the Exchange Admins group.
You need to ensure that any changes to group membership that would allow access to manage the Exchange organization are recorded.
What should you do?

A. Configure the Default Domain Controllers Policy to include auditing successful policy change events.
B. Create a Group Policy object (GPO) on the Exchange Servers OU to audit successful policy change events.
C. Create a Group Policy object (GPO) on the Exchange Servers OU to audit successful policy change events.
D. Create a Group Policy object (GPO) on the Exchange Servers OU to audit successful directory service access events.

Answer: C

Explanation:
They ask us you need to ensure that the security logs contain information necessary to isolate events that affect server uptime.
To write to security events you must use an audit policy because diagnostic logging category named General to the medium logging level will write Windows 2000 or 2003 application event log, not security as is required.
System Services permit o control the Startup and permissions for system services
Audit: Audit the access of global system objects
Incorrect answers

A. Logon-related events when a user logs on interactively or remotely. These events are generated on the computer to which the logon attempt was made. By Login successful events you get just who user access with right access to do logon in the system
B. Tracks system events such as Windows logon network and power events. Notifies COM Events
D. Answer D is vague because MSExchange have one general category for each three options
- System
- Public Folder
- Mailbox

And also because write to application log not security log is not valid
Directory Service Access refers to any time a user changes an Active Directory object. In this way we can see who added Domain Admins group to membership list of the Exchange Admins group. This needs to be done at the domain level.
References
Windows 2003 online doc
http://www.microsoft.com/resources/documentation/WindowsServ/2003/standard/proddocs/enus/
Default.asp?url=/resources/documentation/windowsserv/2003/standard/proddocs/en-us/520.asp
Microsoft Windows 2000 Security Configuration Guide, Chapter 3 - Secure Configuration
http://www.microsoft.com/technet/Security/topics/issues/w2kccscg/w2kscgc3.mspx

---

QUESTION 88
You are the Exchange administrator for Certkiller .
The network consists of a single Active Directory domain named Certkiller .com.
The Exchange organization contains eight servers that run Exchange Server 2003.
All Exchange servers are member servers, and all are located in the Computers container in Active Directory.
Written Certkiller security polices specify the audit settings, event log settings, and security policy settings that must be applied to all Exchange servers.
You need to ensure that the Exchange servers comply with the written security policies.
Your solution must require the minimum amount of administrative effort to maintain.
What should you do?

A. Create the policy settings by using the Local Security Policy tool. Apply the policy settings to the Exchange servers.
B. Create a security template that matches the policy requirements. Run Secedit.exe to apply the template to the Exchange servers.
C. Create a new organizational unit (OU) and move all Exchange servers into the OU. Create a Group Policy object (GPO) that applies the policy settings. Link the GPO to the OU.

D. Create a new Group Policy object (GPO) that defined the policy settings for the Exchange servers. Link the GPO to the Domain Controllers organizational unit (OU). Set a filter on the GPO to apply only to the Exchange servers.

Answer: C

Explanation:
This question is not realy an Exchange question, but instead a Group Policy question. The fact that these are Exchange Servers has no bearing on the question or its answer. The easiest solution is to place all the Exchange servers into their own OU, then create a GPO and apply it to the OU.
Incorrect Answers:

A. Applying the policy settings to one computer at a time is administrative intensive, and invites mistakes in implementation. Therefore, this is not the best answer.
B. Creating a security template and applying the template to the Exchange servers also involves a lot of administration, and as more servers are added, the template must be added to each one. That disqualifies this as a possible answer.
D. Creating a GPO and linking it to the domain controllers OU will not work due to the fact that the Exchange servers are in the Computers OU. It would be impossible to filter it to the Exchange Servers for that reason alone. Additionally, a group policy can't be filtered to one computer. It must be in an OU for filtering to apply.

QUESTION 89
Exchange server computer objects are contained in the Exchange Server OU.
Users in a group named Exchange Admins are exclusively responsible for managing the Exchange organization. No other group, including Enterprise Admins and Domain Admins groups, has permissions to manage the Exchange organization.
You discover that the Domain Admins group is in the membership list of the Exchange Admins group.
You need to ensure that any changes to group membership that would allow access to manage the Exchange organization are recorded.
What should you do?

A. Configure the Default Domain Controller Policy to include auditing successful policy change events.
B. Configure the Default Domain Controller Policy to include auditing successful account management events.
C. Create a Group Policy object (GPO) on the Exchange Servers OU to audit successful policy change events.
D. Create a Group Policy object (GPO) on the Exchange Servers OU to audit successful directory service access events.

Answer: B

QUESTION 90
You are the Exchange administrator for Certkiller . Exchange Server 2003 runs on a Microsoft Windows Server 2003 member server. The Exchange server contains two mailbox stores. All user accounts are located in the Accounts organizational unit (OU).

An e-mail virus infects all mailboxes on both mailbox stores. You create a non administrative user that needs to be able to use the Exmerge utility. This user does not have the necessary permissions to open other user's mailboxes.
You need to assign this user permission to open all users' mailboxes to extract the virus.
What should you do?

A. Assign the user Full Control permissions to the Accounts OU.
B. Assign the user Send As and Receive As permissions to the administrative group.
C. Add the user to the Exchange Domain Servers group.
D. Add the user to the Enterprise Admins global group and to the Exchange server's local Administrators group.

Answer: B

Explanation:
According to articles 262054 and Exmerge documentation the only permission that you need is receive as but according to article 322312 you will get following error in Exmerge log

```
[19:40:58] Copying data from mailbox 'user1' ('USER1') on Server 'SERVER3' to file 'C:\USER1.PST'.
[19:40:59] Error opening message store (MSEMS). Verify that the Microsoft Exchange Information
Store service is running and that you have the correct permissions to log on. (0x8004011d)
[19:40:59] Errors encountered. Copy process aborted for mailbox 'user1' ('USER1').
[19:40:59] Number of items copied from the source store for all mailboxes processed: 0
[19:40:59] Total number of folders processed in the source store: 0
[19:40:59] 0 mailboxes successfully processed. 1 mailboxes were not successfully processed. 0 non-fatal errors
encountered.
[19:40:59] Process completion time: 0:00:00:01
```

Because you also need the send permission
Exchange Domain Servers group do not have the required permission receive as to use EXMERGE, for this reason you must use Method Two
For Microsoft Exchange Mailbox Merge to work successfully against an Exchange 5.5 Server, the user must be logged into Windows 2000 with the Microsoft Exchange Service Account or have Service Account Admin privilege at the Organization, Site and Configuration levels of the Microsoft Exchange Directory.
References
Exmerge help
How to get "service account" access to all mailboxes in Exchange 262054
When the Mailbox Merge Program Tries to Open the Message Store, the Operation Is Unsuccessful 322312
How to assign service account access to all mailboxes in Exchange Server 2003 821897

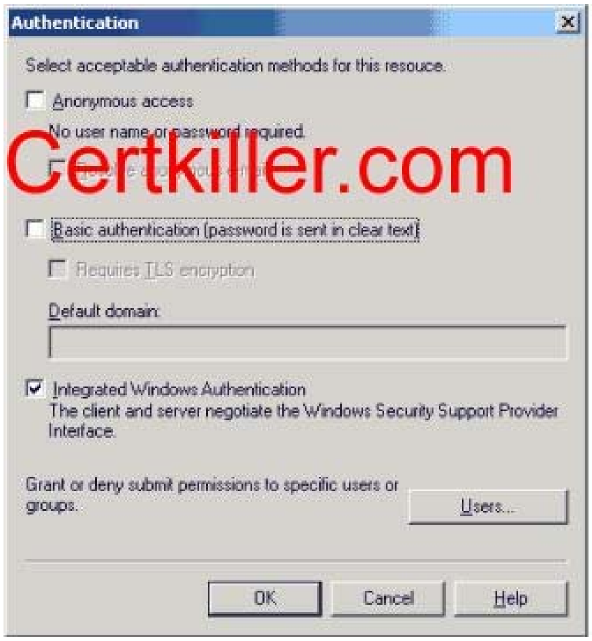
QUESTION 91
You are the Exchange administrator for Certkiller .
The company operates a main office and one branch office.
The network consists of a single Active Directory domain named Certkiller .com.
Exchange Server 2003 is used as the messaging system.
Exchange servers are deployed in two separate Exchange administrative groups.
One administrative group exists in each office.
You manage both offices. An IT administrator manages the users and resources in the branch office.

You need to enable the IT administrator to manage the objects in the Exchange administrative group in the branch office.
The IT administrator must not have the ability to modify permissions for the administrative group.
What should you do?

A. Create a new organizational unit (OU). Place all Exchange servers in the branch office in the new OU. Delegate control over all computer objects in the OU to the IT administrator.
B. Make the IT administrator a local administrator on all Exchange servers in the branch office's administrative group.
C. In the branch office's administrative group, delegate the role of Exchange Full Administrator to the IT administrator.
D. In the branch office's administrative group, delegate the role of Exchange administrator to the IT administrator.

Answer: D
Explanation
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. A user who has Exchange Administrator permissions has the following rights:
Organization Rights:
• All permissions (except for Change permissions) on the MsExchConfiguration container (this object and its subcontainers).
• Deny Receive-As permissions and Send-As permissions on the Organization container (this object and its subcontainers).
Administrative Group Rights:
• Read, List object, and List contents permissions on the MsExchConfiguration container (this object only).
• Read, List object, and List contents permissions on the Organization container (this object and its subcontainers).
• All permissions (except for Change, Deny Send-As, and Deny Receive-As permissions) on the Administrator Group container (this object and its sub-containers).
• All permissions (except for Change permissions) on the Connections container (this object and its subcontainers).
• Read, List object, List contents, and Write properties permissions on the Offline Address Lists container (this object and its subcontainers).
Reference
Working with Active Directory Permissions in Exchange Server 2003

QUESTION 92
You are the Exchange administrator for Certkiller .
The Exchange organization contains a single server that runs Exchange Server 2003.
After a new written company security policy is implemented on the Exchange server, the SMTP virtual server is configured as shown in the Authentication dialog box in the exhibit.



Select acceptable authentication methods for this resouce.

□ Anonymous access

No user name or password required.

□ Resolve anonymous e-mail

□ Basic authentication (password is sent in clear text)

□ Requires TLS encryption

Default domain:

☑ Integrated Windows Authentication

The client and server negotiate the Windows Security Support Provider Interface.

Grant or deny submit permissions to specific users or groups.

External customers now report that they cannot send e-mail to Certkiller from the Internet.
They receive error messages stating that they do not have permission to submit e-mail to your Exchange server.
What should you do?

A. Enable anonymous access.
B. Enable basic authentication.
C. Reconfigure the relay restrictions to allow all IP addresses to relay to the SMTP virtual server.
D. Specify that the NETWORK group has permission to submit messages to the SMTP virtual server.

Answer: A
Explanation
By default, the SMTP virtual server allows only authenticated users to relay e-mail messages. This setting prevents unauthorized users from using your Exchange server to send e-mail messages to external domains. If your server is secured for relay, only authenticated users can send mail to the Internet using your server.
To allow external users to utilize the SMTP connector, you need to permit anonymous user access to SMTP connector.
Reference
Exchange Server 2003 Administration Guide

QUESTION 93
You are the Exchange administrator for Certkiller .
The Exchange organization contains four Exchange Server 2003 computers.
The computer objects for the Exchange servers are contained in an organizational unit (OU) named ExchangeServers.
All client computers run Microsoft Windows NT Workstation 4.0, Windows 2000 Professional, or Windows XP Professional.
Half of the Windows NT Workstation computers are members of a trusted Windows NT 4.0 domain. The computer objects for the client computers are contained in an OU named Clients.

A new written Certkiller policy states that all data communication between the Exchange servers must be encrypted.
The policy does not require communication between client computers and the Exchange servers to be encrypted.
On the ExchangeServers OU, you configure a Group Policy object (GPO) that assigns the Secure Server (Require IP Security) default IPSec policy. You assign the default IPSec policy to all client computers.
Users of Windows NT Workstation computers report that they can no longer send or receive e-mail messages. Users of Windows 2000 Professional computers and Windows XP Professional computers are able to send and receive e-mail messages.
You need to ensure that users on all client computers can send and receive e-mail messages. Your solution must follow company policy.
What should you do?

A. Upgrade all Windows NT Workstation computers to Windows XP Professional.
B. Create and configure a new GPO that assigns the Client (Respond only) IPSec policy, and link the GPO to the Clients OU.
C. Disable the IPSec policy that is linked to the ExchangeServers OU. Configure the Exchange servers to enable SSL for connections to all virtual servers.
D. Modify the IPSec policy that is linked to the ExchangeServers OU to set an IP filter list that specified the IP addresses of the Exchange servers only.

Answer: D

Explanation:
You need to ensure that users on all client computers can send and receive e-mail messages. Your solution must follow company policy Require IP Security means
For all IP traffic, always require security using Kerberos trust. Do NOT allow unsecured communication with untrusted clients. IPSec is disabled by default.
Operating systems older than Microsoft(r) Windows(r) 2000 do not provide built-in support for IPSec. These include Microsoft(r) Windows(r) 98, Windows(r) Millennium Edition, and Microsoft(r) Windows NT(r). If you have computers running these operating systems in your environment, make sure they are not required to use IPSec because the enforcement of IPSec-secured communications denies them access to resources.
The trick in this question is that IPSEC can be used with or without encryption, and the problem is that legacy clients can't understand IPSEC Server (Require Security) policy, they can upgrade all Windows NT Workstation computers to Windows XP Professional that mean answer A or change the policy to Server (Request Security). Also because by default IPSEC policy affect all traffic you will need to filter to affect only to exchange server

---

QUESTION 94
You are the Exchange administrator for Certkiller .
The network consists of an intranet segment and a perimeter network.
A server named ISA1 runs (ISA) Server and connects the perimeter network to the Internet.
The network contains two servers named Exch1 and Certkiller 1.
Both servers run Exchange Server 2003.
Exch1 is connected to the perimeter network and is configured as front-end server.
Exch1 also hosts Microsoft Outlook Web Access. Mail Access.

Certkiller 1 is connected to the intranet and is configured as a back-end server.
Certkiller 1 hosts all user mailboxes.
The firewall between the intranet and the perimeter network is configured to allow RPC communications between Certkiller 1 and Exch1.
A company investigator discovers that confidential e-mail messages are sometimes intercepted when remote users connect to Outlook Web Access on Exch1.
You need to ensure that all Outlook Web Access communications from the Internet are encrypted. Your solution must require the minimum amount of encryption-related processing on Exch1.
What should you do?

A. Configure ISA1 to allow HTTPS traffic between the Internet and Exch1. Instruct employees to connect to Exch1 by using HTTPS instead of HTTP.
B. Configure ISA1 to reverse proxy Outlook Web Access from Exch1. Configure Exch1 and ISA1 to use IPSec encryption when communicate.
C. Install a server encryption certificate on ISA1. Configure ISA1 to reverse proxy Outlook Web Access from Exch1 and to require SSL encryption. Configure ISA1 to transmit unencrypted data to Exch1. Instruct employees to connect to connect to Exch1 by using HTTPS instead of HTTP.
D. Install a server encryption certificate on Exch1. Configure ISA1 to open the HTTPS port for incoming traffic from the Internet to Exch1, and to allow outgoing HTTPS replies from Exch1 to the Internet. Configure the Outlook Web Access virtual server to require SSL encryption for all connections.

Answer: D

Explanation:
You need to ensure that all Outlook Web Access communications from the Internet are encrypted this means: Encrypt traffic between configure Exch1 (Front end server) and Certkiller 1 (backend server) to use IPSec encryption when they communicate and configure ISA.
Incorrect answers:
A: This option does not encrypt front end to back end traffic. You must enforce encryption.
B: You need to Encrypt traffic between configure Exch1 and Certkiller 1.
C: With this option you will have unencrypted data going to Exch1 and users are connecting to Exch1, The option to use ISA in this way is not needed.
Reference
Using ISA Server 2000 with Exchange Server 2003 MS white Paper
Exchange Server 2003 Message Security Guide.doc MS white paper

---

QUESTION 95
You are the Exchange administrator for Certkiller .
The company operates two offices.
Each office has its own intranet.
Each intranet consists of an Active Directory domain.
Both domains are members of the same forest.
Each intranet includes a single server that runs Exchange Server 2003.
Each Exchange server hosts the mailboxes for local users.
The two intranets are connected to the Internet, but not to each other.
New written security polices state that all interoffice e-mail must be secured so that Internet-based

intruders cannot intercept and read it.
You need to ensure compliance with the new polices. Your solution must not affect the way users send email messages to internal or external recipients.
What should you do?

A. Configure each Exchange server to deliver interoffice e-mail messages directly to the other Exchange server.
B. Instruct all users to configure their e-mail client to encrypt all outgoing messages.
C. Configure a VPN between the two offices. Configure the Exchange servers to send interoffice e-mail messages through the VPN.
D. Configure the Exchange servers to use IPSec to encrypt all outgoing SMTP connections.

Answer: C

Explanation:
Because the two intranets are connected to the Internet, but not to each other using a VPN connection will be avoid message interception. This does not provide real encryption, but you can monitor any attempt to break the VPN tunnel.
Incorrect answers

A. This is not valid. You can intercept mail and read it because are in plane text.
B. This requires more steps, like configuring a PKI structure. However you must not affect the way users send e-mail messages to internal or external recipients. External user will not be in your PKI infrastructure.
D. IPSec is used to encrypt all IP traffic not for just SMTP connections. To use IPSec, you will need to set filtering for default IPSec rules to apply only to SMTP traffic. To be able to configure an IPSEC over internet they must use a VPN connection to check their trust PKI certificates if they are not using a Root CA provider with a Public issued CA certificate.
Reference:
MS white paper Exchange Server 2003 Message Security Guide

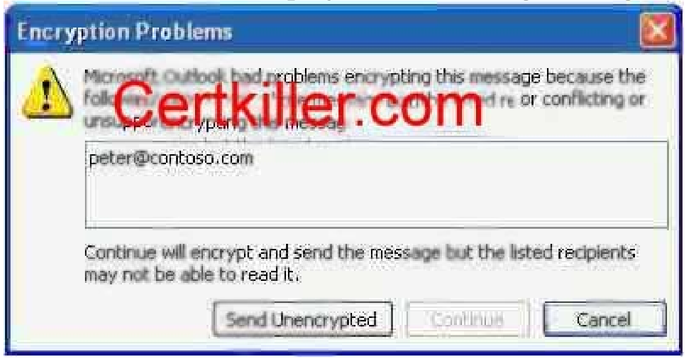
QUESTION 96
You are the Exchange administrator for Certkiller .
The Exchange organization contains two back-end servers and four front-end servers.
All Exchange servers run Exchange Server 2003.
New written security polices require encryption for all Internet connections to the front-end servers.
You try to modify the configuration of each front-end server, but the SSL encryption option is unavailable on each one.
You need to ensure that users can use SSL to secure Internet-based e-mail connections.
What should you do?

A. Obtain and install a server encryption certificate on each front-end server.
B. Obtain and install a server encryption certificate on each back-end server.
C. Install and configure the Key Management Service on a new front-end server.
D. Install and configure Microsoft Certificate Services on each back-end server.

Answer: A

Explanation:
The first step to protecting your OWA traffic is to enable SSL on your Exchange 2000/3 server. To do this you need to get an SSL certificate, install it, and tell IIS to use it for your Exchange server's OWA directory. You can use Microsoft's Certificate Server (included with Windows 2000 Server and higher) to issue your own certificate, or you can buy a commercial certificate from a third-party certificate issuer like VeriSign or Thawte.
Reference.
5-Minute Security Advisor - Configuring Outlook Web Access

QUESTION 97
You are the Exchange administrator for Certkiller .
The network consist of a single Active Directory domain named Certkiller .com.
All Exchange servers run Exchange Server 2003. Microsoft Outlook 2003 is the only e-mail client in use.
New written security polices require encryption for all e-mail messages that contain confidential information.
A domain member named Irene tries to send an encrypted e-mail message to an external user named Peter.
However, Outlook displays the following message:



Microsoft Outlook had problems encrypting this message because the [illegible] or conflicting or [illegible] encrypting the messag[illegible]

peter@contoso.com

Continue will encrypt and send the message but the listed recipients may not be able to read it.

You confirm that Peter has a digital encryption certificate suitable for sending secure e-mail messages.
You need to ensure that Irene can send encrypted e-mail messages to Peter.
What should you do?

A. Instruct Peter to send a digitally encrypted e-mail message to Irene.
B. Instruct Peter to send a digitally signed e-mail message to Irene.
C. Install and configure Microsoft Certificate Services. Instruct Irene to request a personal encryption certificate from the Certificate Services server.
D. Install and configure a server encryption certificate on the Exchange server that contains Irene's mailbox.

Answer: B

Explanation:
The new security polices require encryption for all e-mail messages that contain confidential information but the user has not yet published her certificate. And she is going to send an email to an external user named Peter in the domain contoso.com.
If you use a certificate from your own organization, the user in Contoso.com will get a warning because

Contoso.com does not have a root certificate from Certkiller .com. A possible solution is that Peter send a signed
certificate to Irene, in order that Irene be able to get the public key for Peter.
Outlook 2002/XP/2003 has the ability to sign and encrypt messages for delivery to internal or external recipients. For this encryption you will need a certificate. If you want to deliver signed and/or encrypted e-mail to Internet recipients, you will need to use a recognized certificate (known as a Digital ID) from a third-party vendor.
Once you have a certificate installed on the client, you can begin to send signed and encrypted messages using S/MIME. You can only send encrypted mail to other users if you have access to their public key. This is achieved by having the other user send you a signed message and then adding that user to your contacts. You will now have their public key available.
If you wish to routinely send signed and encrypted messages between users inside your Exchange organization, you should consider using the Key Management service.
This service uses Windows 2003 Certificate Services and provides access to public keys with secure, centralized access to private keys. This gives clients seamless access to signed and encrypted messages, allowing them to send these messages to any other security-enabled recipient in the global address list (GAL).
Reference
Security Operations Guide for Exchange 2000 Server MS Book line

---

QUESTION 98
You are the Exchange administrator for Certkiller .
All Exchange servers run Exchange Server 2003.
Certkiller 's new written security polices require encryption for all internal e-mail messages that contain confidential information.
A domain administrator installs and configures a certification authority (CA) on the network and uses a self-signed certificate to authorize the CA.
Then you use the CA to issue e-mail encryption certificates to all users.
However, when internal users receive encrypted e-mail messages from other internal users, they also receive a message indicating that the encryption is not trusted.
You need to prevent this message from appearing, and you need to ensure that all users can send encrypted messages to each other.
What should you do?

A. Instruct all users to send a digitally signed message to everyone distribution list.
B. Request a domain administrator to create a Group Policy object (GPO) that configures all client computers to trust the CA.
C. Use the CA to create and publish a Certificate Trust List (CTL) on a network share that is accessible to all users.
D. Export the root certificate of the CA to a file. Send the file in e-mail to all users and instruct them to save it on their client computers.

Answer: B

Explanation:
A CTL is a list of trusted certification authorities (CAs) for a particular Web site. You can use CTLs to configure your Web server to accept certificates from a specific list of CAs, and automatically verify client

certificates against this list. Only users with a client authentication certificate that is issued by a CA in the CTL can gain access to the server.

Each Web site on your server can be configured to accept certificates from a different CTL. You may want to do this if you need a different list of trusted CAs for each Web site.

Incorrect answers

A. This requires that each user send mails between them. This is not required by the question.

B. All client computers request a domain administrator to create a Group Policy object (GPO) that configures all client computers to trust the C

A. Therefore; you must use the user policy not the computer policy.

D. Exporting the root certificate to a file and sending the file in e-mail to all users will expose your PKI Root certificate.

Reference

Encryption and Message Security Overview 286159

Quick Start Guide for SMIME for Exchange Server 2003 MS white paper

HOW TO: Configure Certificate Trust Lists in Internet Information Services 5.0 313071

QUESTION 99

You are the Exchange administrator for Certkiller .

The Exchange organization contains 10 Exchange servers.

All Exchange servers run Exchange Server 2003 and Microsoft Windows 2000 Server.

All client computers run Windows XP Professional.

A single Exchange server named Certkiller 1 is allowed to send and receive SMTP traffic to and from the Internet.

User mailboxes are evenly distributed across the other nine Exchange servers.

All Exchange servers host Microsoft Outlook Web Access and are accessible from the Internet by using HTTP only.

You distribute Outlook to all users.

You ensure that all users have personal digital encryption certificates issued by a commercial certification authority (CA). Subsequently, a new written security policy is issued.

The policy requires encryption for all e-mail messages that contain confidential data.

You need to ensure that all local and remote users can send and receive encrypted e-mail messages. You must achieve this goal by making the minimum number of changes to the protocols allowed into the intranet from the Internet.

What should you do?

A. Instruct local users to use Outlook to send encrypted e-mail messages.

Instruct remote users to use Outlook Web Access to send encrypted e-mail messages.

B. Instruct all users to use Outlook to send encrypted e-mail messages.

Configure all client computers to use RPC over HTTP to connect.

C. Instruct all users to use Outlook to send encrypted e-mail messages.

Instruct remote users to establish VPN connections to the Exchange server that contains their mailboxes before they use Outlook.

Configure the network to permit VPN connections to all Exchange servers, configure Routing and Remote Access on all Exchange servers to accept VPN connections.

D. Instruct all users to use Outlook to send encrypted e-mail messages.
Configure Outlook for local users to connect to the Exchange servers as an Exchange client.
Configure Outlook for remote users to connect to the Exchange servers as a POP3 client.
Ensure that all Exchange serves can send and receive messages to and from the Internet.

Answer: A
Explanation
Exchange Server runs on Windows 2000 Server computers. You need to ensure that all users have personal digital encryption certificates issued by a commercial certification authority (CA). You can configure external PKI certificates for each user and map the certificate to each user account. This way users can utilize Outlook or OWA to encrypt their email.
Incorrect Answers
B. The requirements for using OWA with S/MIME support include the following:
The server must be running Exchange Server 2003.
The client must be running Windows 2000 or later and Internet Explorer 6.0 Service Pack 1 (SP1) or later and a smart card or other certificate.
C. VPN connections will encrypt communications to and from Outlook and OWA servers. However, the question requires a minimum number of changes to protocols and configuration. Simply using the builtin features of Outlook and OWA 2003 will accomplish the task with no changes. Therefore, this is not the best answer.
D. POP means a protocol change. Since this violates the requirement of a minimum number of protocol changes, this is not the best answer.
Reference
See "Configuring Exchange Server 2003 for Client Access," in the book Exchange Server 2003 Deployment Guide (http://www.microsoft.com/exchange/library).
Exchange Server 2003 Administration Guide

QUESTION 100
You are the Exchange administrator for Certkiller .
The Exchange organization contains two Exchange Server 2003 computers named Certkiller 1 and Certkiller 2.
Both servers are located on the company's intranet.
An ISA Server computer named ISA1 connects the intranet to the Internet.
Certkiller 1 is not accessible from the Internet.
Certkiller 2 sends and receives all Internet e-mail for all users.
Certkiller 2 is accessible from the Internet only by using SMTP.
Certkiller 2 is the target of a series of Internet-based denial of service (DoS) attacks.
Each attack makes Certkiller 2 unavailable to internal users for a long time.
You need to reduce the impact of future DoS attacks on the Exchange servers.
Your solution must not affect the ability of users to access, send, and receive e-mail.
What should you do?

A. Configure ISA1 to distribute incoming SMTP packets evenly between Certkiller 1 and Certkiller 2.
B. Configure ISA1 to pass all inbound SMTP traffic through the ISA SMTP filter.
C. Configure ISA1 to drop all incoming SMTP packets.
D. Configure Certkiller 2 to perform reverse DNS lookups on all incoming SMTP connections.

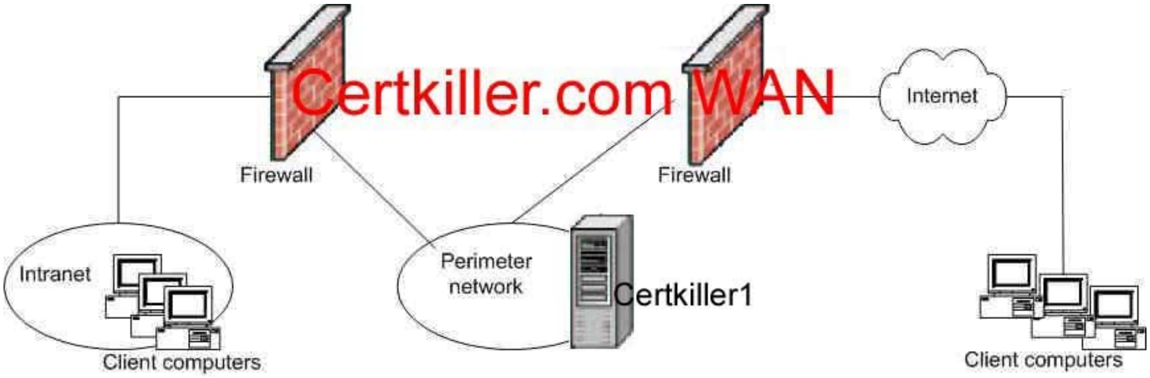
E. Modify your public DNS zone so that both Exchange servers have mail exchanger (MX) resource records with a priority of 10.

Answer: B

Explanation:
ISA Server intercepts all SMTP traffic that arrives on port 25 of the ISA Server computer. The SMTP filter on the ISA Server computer accepts the traffic, inspects it, and passes it on, only if the rules allow it.
The SMTP filter examines SMTP commands sent by Internet SMTP servers and clients. This application layer filter can intercept SMTP commands and check whether they are larger than they should be. SMTP commands that are larger than the limits you configure in the SMTP filter are assumed to be attacks against the SMTP server and can be stopped by the SMTP filter.
Each SMTP command has a maximum length associated with it. This length represents the number of bytes allowed for each command. If an attacker sends a command that exceeds the number of bytes allowed for the command, ISA Server drops the connection and prevents the attacker from communicating with the corporate mail server.
Incorrect Answers:

A. Distributing packets between the servers will not prevent the DDoS attacks from occurring. In fact, the next DDoS attack would be worse, as both servers would then be affected. The DDoS packets would be spread across both servers instead of just one. Therefore, this can't be the correct answer.
C. Dropping all incoming SMTP packets would indeed stop the DDoS attacks. Unfortunately, all incoming mail would also be stopped. This is a violation of the last requirement of the question, so this can't be a correct answer.
D. Reverse DNS lookups will not prevent the attack. It can be used to show where the DDoS attacks are originating. The reverse lookup function will only attach the originating address to the email message. It in-and-of itself will not stop any form of attack. Therefore, this can't be the correct answer.
E. Setting the MX records to have the same value will distribute incoming internet traffic to both servers. This will result in the same problem as "A". The next DDoS attack would be worse since the attack is spread across two systems.
Reference
ISA Server 2000 Feature Pack 1
Using ISA Server 2000 with Exchange Server 2003
Using the ISA Server 2004 SMTP Filter and Message Screener

QUESTION 101
You are the Exchange administrator for Certkiller .
The Exchange organization contains a single Exchange Server 2003 computer named Certkiller 1.
Certkiller 1 is connected to a perimeter network.
The relevant portion of the network is configured as shown in the exhibit.



Certkiller 1 hosts Microsoft Outlook Web Access and all user mailboxes.
To access Certkiller 1, intranet users use Outlook, and Internet users use Outlook Web Access. Certkiller 1 is the target of a series of HTTP-based denial of service (DoS) attacks from the Internet. Each attack makes Certkiller 1 unavailable to all users for a long time.
You need to implement a solution that will protect Certkiller 1 from DoS attacks.
You need to ensure that Inter users can use Outlook Web Access to access their e-mail.
Even during an attack, Certkiller 1 must be available to intranet users.
Your solution must not compromise the security of the internal network.
What should you do?

A. Move Certkiller 1 to the intranet. Configure both firewalls to allow HTTP traffic from the Internet to pass to Certkiller 1.
B. Move Certkiller 1 to the intranet. Install a new server that runs Exchange Server 2003 on the perimeter network. Name the server Certkiller 2 and configure it as a front-end server that hosts Outlook Web Access.
C. Configure the internal firewall to block all HTTP traffic from the Internet. Configure the external firewall to block all HTTP traffic from the intranet.
D. Install a new server that runs Exchange Server 2003. Move half of the mailboxes from Certkiller 1 to the new Exchange server.

Answer: B

Explanation:
In a two firewall setup, the best solution is to have all mailboxes on the internal network, and only required ports through the internal firewall to the Exchange server. Installing another Exchange Server on the perimeter and allowing only OWA access will prevent Certkiller 1 from being attacked directly, and will enable the users of Certkiller 1 to work even if the OWA server comes under attack.
Incorrect answers:

A. Allowing HTTP traffic to pass to the internal network would not stop the DDoS attacks. The firewall would in fact be useless if all internet traffic was allowed to pass right to the internal network.
C. Blocking all HTTP traffic would prevent the OWA users from accessing their mail remotely.
D. Moving half of the mailboxes to a new Exchange server would alleviate half the problem. However, OWA users would not be able to connect to the new mailbox (it has no associated MX record), the users on Certkiller 1 would still receive DDoS attacks, and the servers would still be sitting in the perimeter network and open to compromise.

QUESTION 102

You are the Exchange administrator for Certkiller .
The Exchange organization contains a single Exchange Server 2003 computer named Certkiller A.
The company employs 1,000 users.
Six hundred of the users are remote users who access Certkiller A by using POP3 and IMAP4 clients over the company Internet connection.
On Monday morning, the company ISP informs you that 1 million unsolicited e-mail messages were sent from your network over the preceding two days.
Such activity violates the terms of service of your ISP.
The problem must be resolved immediately.
You verify that the e-mail messages were not sent by any users on your network.
You suspect that an external intruder used Certkiller A to send the e-mail messages.
You need to ensure that this problem cannot happen again.
Your solution must not affect the ability of company users to send and receive legitimate e-mail messages.
What should you do?

A. Configure Certkiller A to prohibit SMTP relaying.
B. Configure Certkiller A and Active Directory to permit only authenticated users to send e-mail messages to user groups and distribution lists in the domain.
C. Configure Certkiller A to permit SMTP relaying only for authenticated users. Instruct all remote users to configure their e-mail clients to authenticate when they send e-mail messages.
D. Configure the network so that only outgoing SMTP traffic and replies to incoming SMTP traffic are allowed to leave the network.

Answer: C

Explanation:
You have POP3 and IMAP4 clients who rely on SMTP for message delivery. These clients may have legitimate reasons for sending e-mail messages to external domains. To work around this issue, create a second SMTP virtual server that is dedicated to receiving e-mail messages from POP3 and from IMAP4 clients. You can configure this additional SMTP virtual server to use authentication that is combined with Secure Sockets Layer (SSL) based encryption, and then configure it to permit relaying for authenticated clients.
Note: By default, the Default SMTP Virtual Server in Exchange 2003 is configured to prevent relaying of email messages through the virtual server.
Incorrect answers:

A. Prohibiting SMTP relaying would prohibit to your remote users from sending or receiving mail, as they must relay since they are outside the organization.
B. Allowing only authenticated users to send and receive in the domain would not work because the e-mail in question went outside the organization. The unsolicited e-mail did not go to users and groups in the domain. Even if it did, this answer is not optimal since this would also prevent external clients from sending valid e-mail to the organization.
D. Configuring the network in this way would prevent users from sending e-mail into the organization.
Reference
HOW TO: Prevent Unsolicited Commercial E-Mail in Exchange 2003 KB 821746

QUESTION 103

You are the Exchange administrator for Certkiller .
The network consists of a single Active Directory domain named Certkiller .com.
Exchange Server 2003 is used as the messaging system.
The default recipient policy is configured to generate SMTP addresses based on the format of givenname_surname@ Certkiller .com, in which givenname is the user's given name or personal name and surname is the user's surname or last name.
A user named Jack Edwards marries and changes her name to Jack King.
You need to ensure that Jack's new e-mail address and associated friendly name appear in her out bound e-mail address.
Tess's original e-mail address must remain valid for inbound e-mail.
Which two actions should you perform? (Each correct answer presents part of the solution. Choose two)

A. Change the pre-Microsoft Windows 2000 user logon name to Tess_King.
B. Change the user principal name (UPN) attribute to Tess_King@ Certkiller .com.
C. Change the last name attribute to King.
D. Change the display name attribute to Jack King.

Answer: C, D

Explanation:
In the default Recipient Policy, the string used is %r._%g.%s where %r is a replacement variable, %g stands for given name, and %s stands for surname. These names are taken from AD's First Name and Last Name attributes. In order for the new e-mail address to be used for Tess, the last name attribute must be changed. When this happens, the new e-mail address will be generated. In addition, changing the display name attribute will change her friendly name to the new address. This is needed as this attribute is what Exchange uses to display the friendly name.
Incorrect Answers:

A. The pre-MS Windows 2000 logon name is only used for authentication on Windows 3.5x and Windows NT 4 domains. Changing this will not change any of the attributes that is used in Exchange.
B. Changing the UPN attribute will not change her address in Exchange. Note the default Recipient Policy string used above. Since this does not use the UPN name to generate its SMTP address, this can't be used to change her name now.

QUESTION 104

You are the Exchange administrator for Certkiller .
All Exchange servers run Exchange Server 2003.
Users report that a large number of unsolicited e-mail messages are delivered directly to their company e-mail addresses.
You need to reduce the number of unsolicited e-mail messages received by company users, without affecting their ability to send and receive legitimate e-mail messages.
You cannot install any additional software on the Exchange servers.
What should you do?

A. Configure the Exchange servers to perform reverse DNS lookups for all incoming SMTP connections.
B. Write an Exchange server-side script that performs reverse DNS lookups on all incoming SMTP connections and rejects connections when the reverse lookup fails.
C. Enable the junk mail feature on all e-mail client applications. On client applications that do not have junk mail features, install mail-filtering software.
D. Configure size limits for all mailboxes so that new mail cannot be received when the mailbox exceeds its size limit.
E. Enable client-side mail filtering to delete all e-mail messages that do not contain the full e-mail addresses of the appropriate recipient.

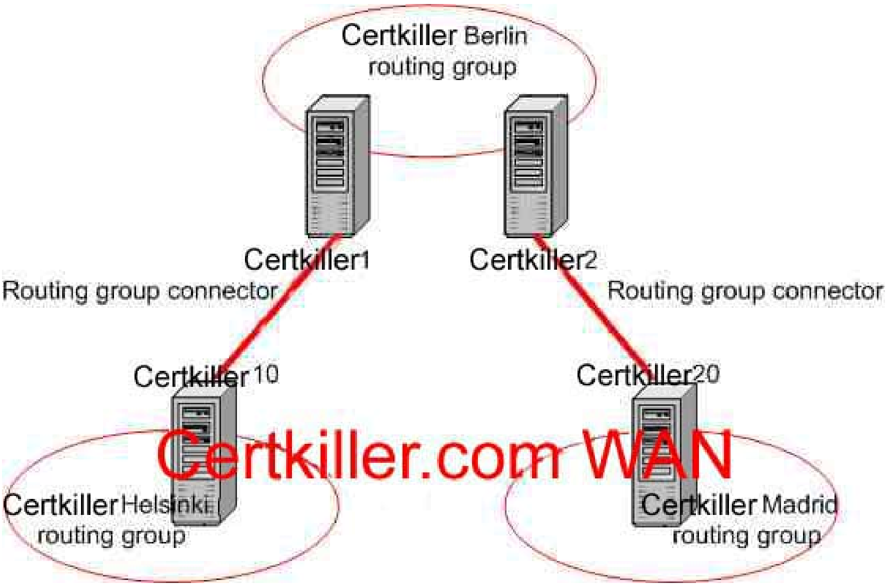
Answer: C

Explanation:
Of the options available, enabling junk mail filters on clients' machines or installing it for clients that do not have the capability is the best solution.
Incorrect choices:

A. Reverse DNS lookup simply adds a tag to the message header stating where the DNS lookup came from. It will not stop incoming messages from being delivered in any way, shape or form except if the sender domain is not valid.
B. Typically unsolicited (or spam) e-mail has a valid DNS lookup. It is relayed from a valid server to you. Therefore, a script to reject connections where reverse DNS fails would not work since the reverse lookup would succeed in those cases.
D. Configuring limits would stop ALL mail once the limit is reached. Since in large part the mailbox would be filled with unsolicited mail, there would be two issues to resolve instead of one.
E. Enabling client side filtering to delete messages can cause problems if the user is part of a group. In many cases, the group membership is not explicitly defined upon delivery. This would cause all mail coming to the user from these groups to be deleted without ever being seen.
References:
Exchange Server 2003 Help -> Reverse DNS lookups
MS KB article How to configure connection filtering to use Real time Block Lists (RBLs) and how to configure recipient filtering in Exchange 2003 823866
MS White Paper Exchange Server 2003 Message Security Guide
MS press BOOK Secure Messaging with Microsoft Exchange Server 2003
MS white paper Exchange 2003 Intelligent Message Filter Deployment Guide

---

QUESTION 105
You are the Exchange administrator for Certkiller .
The Exchange organization contains three routing groups named Berlin, Helsinki, and Madrid.
Each routing group contains one or more Exchange Server 2003 computers.
In the Berlin routing group, Certkiller 1 functions as the bridgehead server for a routing group connector to the Helsinki routing group, and Certkiller 2 functions as the bridgehead server for a routing group connector to the Madrid routing group.
The topology of the Exchange organization is shown in the following table.



Users report intermittent problems with slow delivery of e-mail messages between the Helsinki and Madrid routing groups.
You attempt to use Message Tracking Center on Certkiller 10 to track the flow of a message sent from a mailbox on Certkiller 10 to a mailbox on Certkiller 20.
Even through the message is delivered; you can see its progress only as far as Certkiller 1.
You need to be able to track messages sent from Certkiller 10 to Certkiller 20.
What should you do?

A. Enable message tracking on Certkiller 2 and Certkiller 20.
B. Run Message Tracking Center from the console on Certkiller 20.
C. Create a direct routing group connector between the Helsinki and Madrid routing groups.
D. Configure Certkiller 1 and Certkiller 2 as bridgehead servers for the routing group connector between the Madrid and Berlin routing groups.
E. Configure Server1 and Server2 as bridgehead servers for the routing group connector between the Helsinki and Berlin routing groups.

Answer: A

Explanation:
You can't expect to track a message if it passes invisibly between servers. In an Exchange Server organization, you can search for a message only when you've already configured the Exchange Server machines to generate message-tracking log files for you to interrogate.
Tracking is simple when a message remains on one server, more complicated when the message passes across multiple servers en route to its final destination and even more complex when the message passes out across the Internet or across another messaging system. Exchange 2003 can't force every email system on the planet to generate and maintain tracking data in a common format and make that data available to any program that might request the data. Therefore, your options are restricted to tracking messages as they pass between servers within one Exchange Server organization.
When you enable tracking, every Exchange Server machine can maintain a set of message-tracking logs. Each server creates a new log daily and names the log according to the date in yyyymmdd format (e.g., 20000725.txt).

The logs reside on a network share called server_name.log (in Exchange 2003) or tracking.log (in Exchange Server 5.5, Exchange Server 5.0, and Exchange Server 4.0). Prefixing the name of the Exchange Server system creates the full name of the share.
Reference:
How To Troubleshoot for Exchange Server 2003 Transport Issues 821910

QUESTION 106
You are the Exchange administrator for Certkiller .
The network consists of a single Active Directory domain named Certkiller .com.
All network servers run Microsoft Windows Sever 2003. Exchange Server 2003.
Exchange Server 2003 is used as the messaging system.
The accounting department hires a consultant on a temporary basis.
The consultant needs to access the department's file server.
The department needs to ensure that the consultant's external e-mail address appears in the global address list (GAL) and that mail sent to him is sent to his external e-mail address.
You need to create an Active Directory object in the domain to fulfill these requirements.
Which type of object should you create?

A. A mail-enabled Contact object
B. A mail-enabled User object
C. A mailbox-enabled User object
D. A mailbox-enabled InetOrgPerson object

Answer: B

Explanation:
A mail-enabled object is a Windows 2003 Active Directory object that has at least one e-mail address defined.
An example of a mail-enabled object is an Exchange 2003 contact that has an e-mail address defined.
Incorrect Answers:

A. A contact object does not have any rights in the domain. Since the user will need rights to the department's file server, this cannot be the correct answer.
C. A mailbox-enabled object is a Windows 2003 Active Directory object that has one or more Exchange Server mailboxes associated with it. This user will need to have his external e-mail address associated with his account and NOT an Exchange address.
D. The InetOrgPerson object is a class (or collection of related fields) and not an object. This class would not be used to define a user in this manner. It is used in LDAP queries.
Reference:
KB article 275636 - Creating Exchange Mailbox-Enabled and Mail-Enabled Objects in Active Directory

---

QUESTION 107
You are the Exchange administrator for Certkiller .
The network consists of a single Active Directory domain named Certkiller .com.
Exchange Server 2003 is used as the company wide messaging system.
The Exchange organization contains one administrative group and one routing group.
The company has one office in Hong Kong and another in Osaka.

The Hong Kong office has 2,000 users.
The Osaka office has 500 users.
The two offices are connected by a VPN that uses a highly utilized Internet connection.
The Osaka office contains a single Exchange server
Hong Kong office contains four Exchange servers.
Each office has one mail-enabled global security group that contains all users in that office.
These groups are named All Hong Kong and All Osaka.
When users in Osaka send e-mail messages to the All Hong Kong group, some recipients receive the messages after a few minutes, but other recipients receive them after a few hours.
You need to ensure that e-mail messages sent to the All Hong Kong group are delivered to all users as efficiently as possible.
What should you do?

A. Convert the All Hong Kong group to a mail-enabled universal security group.
B. In each office, create a separate routing group and place the local Exchange servers in that group. Create routing group connectors to send messages between the two groups.
C. Configure the All Hong Kong group to use an expansion server in the Hong Kong office.
D. Configure the All Hong Kong group to use an expansion server in the Osaka office.

Answer: B

Explanation:
Sending messages when there is only one routing group means that the server will attempt to send the message directly, rather than tunneling the message through a bridgehead connection. When this is the case, the messages will hang in the outbound queue until a path to the destination server is clear. Creating routing groups and connectors will send the messages to the dedicated bridgehead servers. Note that this is the Microsoft recommended configuration between Exchange servers when the links are slow or unreliable.
Incorrect Answers:

A. Converting the group to a universal group will not resolve the situation. The messages will still attempt to go directly from server to server over the over utilized link. Some messages will arrive quickly, and others will still be delayed as the link saturation increases and decreases.
C. Using an expansion server in the Hong Kong office will not help the situation, and in fact could make it worse. Since there is no bridgehead server, messages will leave the new server and attempt to connect to the destination directly. Without the traffic control capability of the bridgehead server, the link will become even more utilized.
D. No bridgehead means no any traffic regulation between sites, and this will result in further delays in message delivery.

QUESTION 108
You are the Exchange administrator for Certkiller .
The network consists of a single Active Directory domain named Certkiller .com.
All Exchange servers run Exchange Server 2003.
Microsoft Outlook is the only e-mail client in use.
The domain contains 1,000 Contact objects that represent customers, vendors, and independent contractors.

The domain also contains 5,000 mailbox-enabled user accounts for company users.
Users report that they are often unable to distinguish between external recipients and internal recipients when they address e-mail.
Management requests that you provide a way to separate internal e-mail addresses from external e-mail addresses in the Outlook Select Names dialog box.
You need to ensure that all user accounts and Contact objects appear in Outlook.
You also need to ensure that users can easily distinguish between internal and external e-mail addresses.
Your solution must require the minimum amount of administrative effort to maintain the external e-mail addresses.
What should you do?

A. Create a universal distribution group named External. Add all Contact objects to the External group.
B. Create new address lists for internal and external recipients. Configure the filters on each view to display only the appropriate objects.
C. Create a new organizational unit (OU) named External. Move all Contact objects to the new OU.
D. Create an Outlook Address Book that contains all external recipients. Delete all Contact objects form the domain and distribute the new address book to all internal users.

Answer: B

Explanation:
You must create multiple Global Address Lists. The address lists typically have different user accounts listed in them based on the Lightweight Directory Access Protocol (LDAP) filter that you create. By default, all the users in the Exchange 2003 organization can view all the defined Global Address Lists.
By creating different views you can easily maintain the external e-mail addresses in one; and internal e-mail addresses in other

---

QUESTION 109
You are the Exchange administrator for Certkiller .
The network consists of a single Active Directory domain named Certkiller .com.
A server named Exch1 runs Exchange Server 2003 and hosts all user mailboxes.
Exch1 also sends and receives SMTP e-mail messages to and from the Internet.
Exch1 is protected by a firewall that connects the intranet to the Internet.
Users report that they receive a large number of unsolicited e-mail messages every day.
You discover that all users receive the same unsolicited e-mail messages, which are sent to a universal distribution group in the domain.
You need to ensure that distribution groups cannot be used to send e-mail messages from the Internet to company users.
Your solution must not affect the ability of company users to send and receive legitimate e-mail messages.
What should you do?

A. Convert the universal distribution groups to universal security groups.
B. Configure the distribution groups so that messages are only accepted from authenticated users.
C. Configure Exch1 to reject incoming SMTP traffic from external IP addresses.
D. Configure Exch1 to send and receive SMTP traffic to and from the firewall. Configure the firewall to reverse publish the SMTP port on Exch1.

Answer: B

Explanation:
The universal group is used for mail distribution in your organization. To stop receiving spam, you can configure the distribution group to accept mail for authenticate users only.
Incorrect answers

A. Converting universal group to security group on its own will not protect your against unsolicited mail.
C. If you configure Exch1 to reject incoming SMTP traffic from external IP addresses, you will not receive mail from anybody.
D. Although not recommended, you can position the Exchange Server 2003 front-end server acting as the RPC proxy server inside the perimeter network. In this scenario, you configure your Exchange servers as in Scenario 1. However, you will need to make sure to open the ports required by RPC over HTTP on your internal firewall, in addition to those already required for an Exchange front-end server. The ports for RPC over HTTP are TCP 6001, 6002, and 6004.
Reference:
MS white paper Exchange Server 2003 RPC over HTTP Deployment Scenarios
MS white paper Exchange Server 2003 Client Access Guide
MS white paper Exchange 2003 Front-End Back-End Topology
MS white paper Exchange Server 2003 Message Security Guide
MS white paper Microsoft Exchange Intelligent Message Filter Deployment Guide

---

QUESTION 110
You are the Exchange administrator for Certkiller .
The Exchange organization contains two servers that run Exchange Server 2003.
All users send and receive e-mail messages by using Microsoft Outlook.
All users in the customer service department are members of a global group named CS_GG.
Management plans to implement a new process for customer service.
Customers will request service by sending e-mail messages to a specified address.
Customer service users will receive and reply to these messages.
In the source address field, each reply must display CustomService as the alias.
Replies must not display the personal e-mail addresses of customer service users.
You create a mail-enabled distribution group named CustomService and add all customer service users to this group.
Members of the CustomService distribution group now receive all e-mail requests for customer service.
However, when they send replies, the replies display their personal e-mail addresses as the return address.
You need to enable the customer service users to reply by using the CustomService e-mail address instead of their personal e-mail address.
What should you do?

A. Modify the permissions on the CustomerService distribution group so that CS_GG has Send As permissions on the distribution group.
B. Modify the CustomerService distribution group to accept messages only from authenticated users.
C. Delete the CustomerService distribution group. Create a mail-enabled user account named

CustomerService. Modify the permissions on the CustomerService mailbox so that CS_GG has permissions to send on behalf of the mailbox.
D. Modify the permissions on the CustomerService distribution group so that CS_GG has Send To permissions on the distribution group.

Answer: A

Explanation:
The CustomerService group is mail enabled; meaning that it has a mailbox. Assigning the Send As permission to the CS_GC membership will enable the CS_GC users to send mail as the CustomerService "user". Note that since the group is mail enabled, there is a single mailbox for the group that has been defined. Understand that the "Send As" permission allows users to send mail as another user. In this case, the "user" is actually a group.
Incorrect answers:
B. Accepting messages only from authenticated users is designed to prevent people outside the organization from sending messages to the organization. It will not affect messages sent by already authenticated users, and hence will have no effect on the problem described.
C. The CS_GC group can't be given permission to "Send on Behalf". Only other users can be given this permission. Therefore, this answer is not correct.
D. There is no "Send To" permission. Therefore, this answer can be eliminated.
References:
Implementing, Managing, and Maintaining Microsoft Exchange Server 2003 MOC Course book 2400B, Pages 04-35,36
Microsoft Exchange Help -> Users and Computers -> Exchange 2003 General Tab -> Delivery Options

---

QUESTION 111
You are the Exchange administrator for Certkiller .
The company operates a main office and one branch office.
The network consists of a single Active Directory domain named Certkiller .com.
The domain contains three servers that run Exchange Server 2003 in single Exchange organization.
Two Exchange servers are located in the main office and are members of the Main Office administrative group.
The Third Exchange server is located in the branch office and is a member of the Branch Office administrative group.
User and group accounts for users in the main office are located in the Main Office organizational unit (OU).
User and group accounts for users in the branch office are located in the Branch Office OU.
A new administrator is hired to perform the following administrative tasks:
• Create and delete user accounts for branch office users.
• Add and remove users from mail-enabled groups for branch office users.
• Create and delete mailboxes on the Exchange server in the branch office.
• View and manage queues on the Exchange server in the branch office.
You need to ensure that the new administrator can perform the required tasks. You must assign only the minimum level of necessary permissions.
Which two actions should you perform? (Each correct answer presents part of the solution. Choose two)

A. Configure the permission on the Branch Office OU to grant full control of the OU to the new

administrator.
B. Add the new administrator to the Account Operators group in the domain.
C. Configure the permissions on the Branch Office OU to enable the new administrator to manage user and group accounts in the OU.
D. Add the new administrator to the Server Operators group on the Exchange server in the branch office.
E. Configure the permissions on the Branch Office administrative group to assign Exchange View Only Administrator permission to the new administrator.
F. Configure the permissions on the Branch Office administrative group to assign Exchange Administrator permissions to the new administrator.

Answer: C, F

Explanation:
Permissions over specific objects do need to be delegated to specific sets of administrators. The new administrator needs permissions on the branch offices OU to manage AD accounts, also because he needs to create and manage exchange mail box, he needs to be an exchange administrator.
References:
Overview of Exchange Administrative Role Permissions in Exchange 2003 KB article 823018
MS white paper Design Considerations for Delegation of Administration in Active Directory
MS white paper Working with Active Directory Permissions in Microsoft Exchange 2003

QUESTION 112
You are the Exchange administrator for Certkiller .
The Exchange organization contains two Exchange routing groups.
Each routing group contains four Exchange Server 2003 computers.
One Exchange server in each routing group hosts a routing group connector.
The company's Service Level Agreement (SLA) states that internal e-mail service should not be disrupted by the failure of a single Exchange server.
You need to ensure that e-mail messages are delivered between the two routing groups even if one of the Exchange servers fail.
You want to achieve this goal by using the minimum amount of administrative effort.
What should you do?

A. In each routing group, configure an additional SMTP virtual server on one Exchange server that is not used by the routing group connector.
B. In each routing group, create an SMTP connector that forwards all mail for the SMTP address space of "*" to the bridgehead server in the other routing group.
C. On the properties of each routing group connector, add an SMTP virtual server from another Exchange server.
D. On an Exchange server that does not host the routing group connector, create an additional routing group connector and use the same local and remote SMTP virtual servers that are used by the existing routing group connector.

Answer: D

Explanation:

A Routing Group is a collection of "well-connected" Exchange Server computers. Messages sent between any two servers within a Routing Group are routed directly from source to target. Full mesh 24 x 7 Connectivity is assumed. Any messages sent from a server in one Routing Group to a server in another Routing Group must be routed to a bridgehead in the source Routing Group and over to a bridgehead in the destination Routing Group.
Incorrect answers:

A. Creating additional SMTP virtual Servers does not give any redundancy, as no connection is established if the link fails. In addition, another virtual SMTP server would not use the default connections, and hence not do anything other than simple sit there.
B. Creating a SMTP link in each group that forwards all SMTP traffic to the other bridgehead server would work, but is more administration, and if the bridgehead server goes down, this link would collapse as well.
C. Adding an SMTP virtual server from another server utilizes the same link for connectivity, and hence has the same problem: If the link goes down, then there is no backup. Therefore, there is no redundancy as required by the question.
References
KB article 231731 XADM: Administrative Groups and Routing Groups
KB 251825 XADM: Uninstalling Last Server in Routing Group Does Not Clean Up the RG Connectors from Other RGs
KB article 266744 XADM: How to Create a Routing Group
KB article 267992 XADM: How to Configure a Routing Group Connector

---

QUESTION 113
You are the Exchange administrator for Certkiller .
The Exchange organization contains three Exchange Server 2003 computers that run Microsoft Windows Server 2003.
Each Exchange server is used by a separate business unit.
Each business unit is located in a separate routing group.
The routing groups are connected by routing group connectors.
These routing group connectors are used to deliver internal e-mail messages.
Each business unit has its own connection to the Internet.
The network connections between the business unit servers are at almost 100-percent utilization.
You need to ensure that each business unit uses its own Internet connection to deliver Internet e-mail messages.
Your solution must not affect the delivery of Internal e-mail messages.
What should you do?

A. Configure the SMTP virtual server on each server to forward all mail to the SMTP smart host that belongs to the ISP for the server's business unit.
B. Configure the SMTP virtual server on each server to use the IP address of an external DNS server. Use the DNS server provided by each business unit's respective ISP.
C. In each routing group, create an SMTP connector that defined an SMTP address space of * and restrict the connector scope to the routing group.
D. In each routing group, create an SMTP connector that defined an SMTP address space of the ISP's domain used by the business unit. Configure the SMTP connector to allow messages to be relayed to that domain.

Answer: C

Explanation:
In each routing group, configure an SMTP connector and limit its scope to only that group - Prevents other groups from using the link as well as forwarding all requests that are not handled locally through that connector. (Note that the connectors between business units will probably have preference since "*" is the most generic match, and the business unit connectors will match local resources before this connector, so only internet traffic will get routed out.)
Incorrect answers:

A. Configuring the SMTP virtual server to forward to smart host can't work because ALL SMTP traffic would be routed there, not just the internet traffic as prescribed
B. Configuring the SMTP virtual server to forward to the ISP's DNS server can't work because ALL SMTP traffic would be routed there, not just the internet traffic as prescribed
D. Since the scope is not limited any request made to the internet can use this link, regardless of its origin. Therefore, if another group's internet link was down, all of their routing would go through this ISP, which is a clear violation of the requirements of the question that state, "Each business unit uses its own internet connection to deliver internet email messages."

QUESTION 114
You are the Exchange administrator for Certkiller .
The Tokyo office has six servers that run Exchange Server 2003.
The Osaka office has four servers that run Exchange Server 2003.
The servers are all in a single routing group.
The WAN administrator reports a large amount of e-mail traffic on the network connection between the Tokyo and Osaka offices.
The traffic is interfering with critical line-of-business database applications that must run during business hours.
The database servers are in the Tokyo office, but many of the users are in the Osaka office.
The large amount of WAN traffic is caused by e-mail messages that have large attachments.
You need to ensure that large e-mail messages are delivered between offices only after business hours.
What should you do?

A. Define global size limits for inbound and outbound messages.
B. Define message size limits on all SMTP virtual servers in both offices.
C. Create a routing group that contains the Exchange servers in the Osaka office. Create an SMTP connector to connect the Osaka and Tokyo routing groups that schedules the ETRN connection time.
D. Create a routing group that contains the Exchange servers in the Osaka office. Create a routing group connector between the routing groups in the Osaka and Tokyo offices that uses a specified delivery time for oversized messages.

Answer: D

Explanation:
Using a Routing Group Connector that has a specified delivery time for oversized messages is the Microsoft

recommended way of connecting between routing groups that are in the same organization
Incorrect answers:
A, B. Message size limits on inbound and outbound SMTP servers Global Limits would help the problem, but would prevent large messages from passing. Also, using only one group, there is a lot of unnecessary traffic generated between servers.
C. SMTP connectors are designed for networks that are not well connected. This does not seem to be the case here.

QUESTION 115
You are the Exchange administrator for Certkiller .
The network consists of a single Active Directory domain Certkiller .com.
All users use Microsoft Outlook and Outlook Web Access to send and receive e-mail.
Certkiller hires 50 independent contractors.
All contractors work off site.
None of them have user accounts in the domain. Internal users communicate with the contractors by email.
However, users report that they cannot find e-mail addresses for the contractors in Outlook or in Outlook Web Access.
You need to ensure that all users can look up the e-mail addresses of the contractors in the global address list (GAL).
Your configuration must not give the contractors any permission on any company resources.
What should you do?

A. For each contractor, create a mail-enabled User object in Active Directory.
Configure the User object to forward e-mail messages to the contractor's e-mail address.
B. For each contractor, create a mail-enabled contact object in Active Directory.
Configure the Contact object to use the contractor's e-mail address.
C. Create an Outlook distribution list that includes all contractors.
Send the distribution list to all internal users in e-mail
D. Create an Outlook contact for each contractor's e-mail address.
Send all Outlook contacts to all internal users in e-mail.

Answer: B
Explanation
To see the contractors email you just need to create a contact object for each contractor. The contact object will contain their mail address will allow users to forward the email to the correct mail contact.
Incorrect answers:

A. The contractors must not be allowed any access to the company resources. If a user object is created, they will have some permissions on the domain unless other precautions are taken.
C. A distribution list for the contractors can't be created since they do not have any information in Active Directory. In order for the contractors to show up for a Distribution List, they must first be created as users or as contacts.
D. This answer will not list the contractors in the GAL. In addition, it would be very labor intensive and is not a centralized solution.
Reference
Exchange Server 2003 Administration Guide

QUESTION 116
You are the Exchange administrator for Certkiller .
The network consists of a single Active Directory domain that contains three domain controllers. All domain controllers and member servers are located in a single subnet that is separate from the subnet that contains client computers.
The Exchange organization contains one Exchange Server 2003 computer named Certkiller 1. Certkiller 1 hosts all user mailboxes. Microsoft Outlook is the only e-mail client in use.
You install a new, redundant network adapter on Certkiller 1 and on each domain controller.
Each new network adapter has its own IP address.
You connect all four new network adapters to the server subnet.
Users immediately begin to report intermittent problems when they try to send e-mail messages or view the global address list (GAL).
They receive the following error message: "Network problems are preventing connection to the Microsoft Exchange Server computer.
Contact your system administrator if this condition persists."
You confirm that all client computers can use the ping command to connect to all servers by name and to all network adapters by IP address.
You need to ensure that all users can send e-mail and view the GAL.
What should you do?

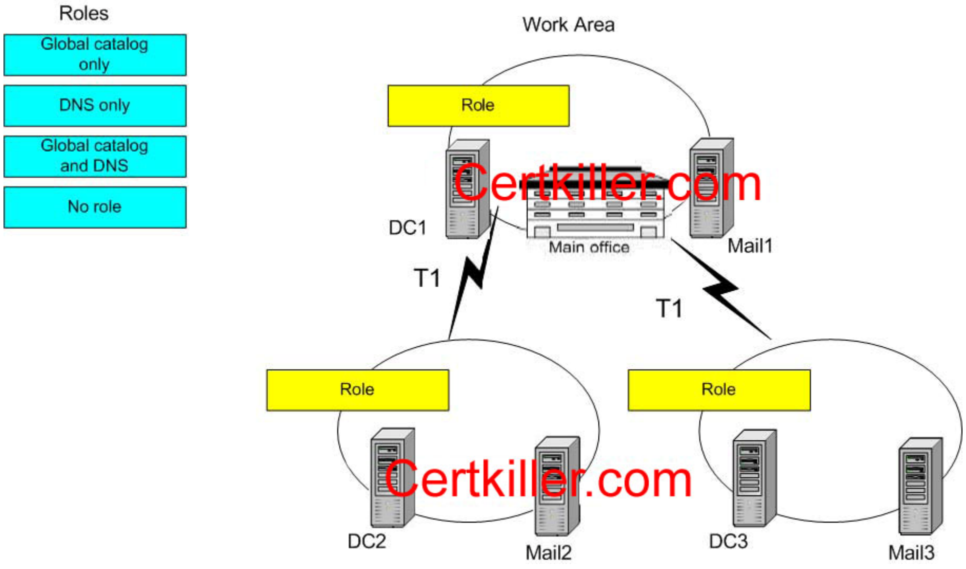
A. Reconfigure the network adapters on Certkiller 1 so that IP filtering allows SMTP and RPC traffic on both network adapters.
B. On the domain controllers, reconfigure the network adapters so that file and print sharing is bound to all network adapters on all domain controllers.
C. On the domain controllers, modify the permissions on the SYSVOL share to assign the Full Control permission to the Everyone group.
D. Reconfigure the Active Directory structure so that the IP addresses used by servers are located in one site and the IP addresses used by client computers are located in another site.

Answer: B

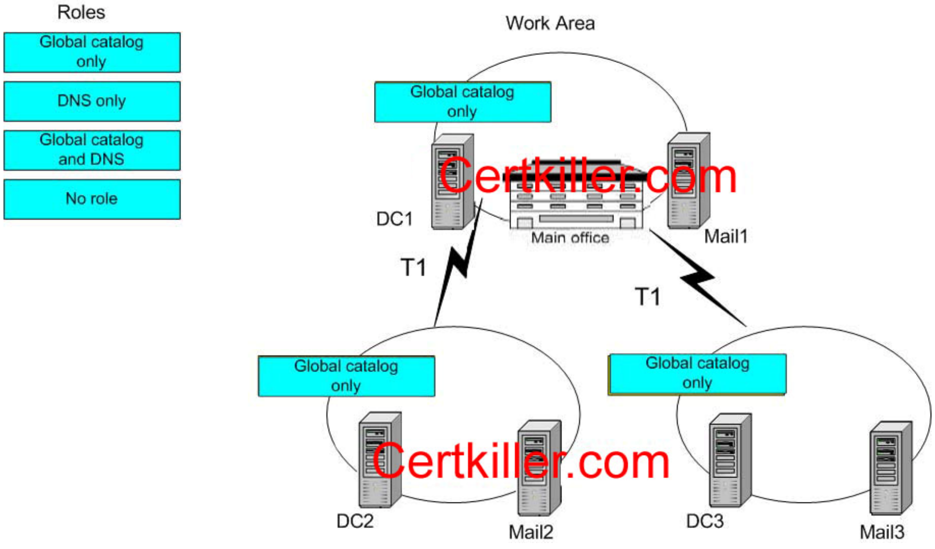
Explanation:
Disabling File and Print Sharing can cause Event 8032 messages. When you add a second network card to a DC you must check that File and Print sharing is bound ONLY to the intranet adapter, and that the intranet adapter is First in the binding order.

QUESTION 117
You are the Exchange administrator for Certkiller .
The company operates a main office and two branch offices.
The network consists of a single Active Directory domain and a single Exchange organization.
All Exchange servers run Exchange Server 2003.
Each office contains one domain controller and one Exchange server.
Domain controllers are named DC1 through DC3.
Exchange servers are named Certkiller 1 through Certkiller 3.
DC1 is configured as a global catalog server.

DC1 runs the DNS Server service and hosts and Active Directory-integrated DNS zone.
DC1 is used by all network computers for DNS name resolution.
DC2 and DC3 are configured as domain controllers only.
Users report intermittent problems when they try to send e-mail messages or access the global address list (GAL).
You discover that the T1 lines between the main office and the branch offices sometimes fail for one hour or longer.
You need to configure the network so that all Exchange servers can start normally and all users can send e-mail messages and access the GAL, even if a single T1 line fails.
What should you do?
To answer, drag the appropriate domain controller roles to the correct office locations in the work area.



Answer:



Explanation:
They told us DC2 and DC3 are configured as domain controllers DC1 is configured as a global catalog server

and Each office contains one domain controller and one Exchange server.
They ask You need to configure the network so that all Exchange servers can start normally and all users can send e-mail messages and access the GAL, even if a single T1 line fails to avoid problem when the line is dropped Each office should have a Global Catalog server.
The logical answer is to add a GC to each site but because also T1 line fails is a better option to use a GC that also run DNS service to be able to resolve the names when T1 fail, Exchange DSACESS is DNS dependent to determinate where is the SRV record for Global catalog, making just to the other DC Global catalog will be not enough to solve the issues when line fail because each 15 minutes Exchange reconstruct it link state table based on DNS query to GC to see if still alive or not

---

QUESTION 118
You are the Exchange administrator for Certkiller .
The Exchange organization contains 10 servers that run Exchange Server 2003.
All users send and receive e-mail messages by using Microsoft Outlook.
Certkiller has many different departments and a total of 10,000 users.
For each department, management asks you to create one address list that contains all users in that department. Management also asks you to create a confidential address list.
The membership of the confidential address list will consists of several users from every department.
For each department, you create an address list that uses the department attribute.
Now you need to create the confidential address list. You must ensure that members of the Managers group are the only users who can identify the members of the list by using Outlook. You must not affect any existing e-mail functionality.
What should you do?

A. Modify the permissions on the user accounts of individuals in the confidential address list so that only the Managers group has permission to send e-mail messages to these accounts.
Create a confidential address list that includes the required user accounts.
B. Modify the permissions on the user accounts of the individuals in the confidential address list so that only the Managers group has permission to view these accounts.
Create a confidential address list that includes the required user accounts.
C. Configure the department attribute as Confidential for the user accounts of individuals in the confidential address list.
Create an address list that uses the department attribute.
Modify the permissions on the address list so that only the Managers group has permission to view its membership.
D. Configure a custom attribute as Confidential for the user accounts of individuals in the confidential address list.
Create an address list that uses the custom attribute.
Modify the permissions on the address list so that only the Managers group has permission to view its membership.

Answer: D

Explanation:
In order to prevent affecting the current e-mail functionality, the use of a custom attribute is required. There are 15 custom attributes available in Exchange 2003 for defining things such as special memberships. Enabling and

grouping based on these attributes will not affect any other distribution lists.
Incorrect answers:

A. Modifying permissions on individual accounts will change the memberships of the existing groups. Other users will not be able to send mail to these modified users, and this would disrupt the existing email functionality.
B. Modifying permissions so only managers will be able to see the accounts will also disrupt the existing functionality, as anytime a user wants to send to anyone in this group (whether they want to send to the whole group or not does not matter) they will not be able to see them. Remember that the purpose of the confidential group is not to hide the members from getting normal mail, but to hide the fact that these people are in a confidential group.
C. Configuring the Departmental attribute in this way will prevent the users in the group from receiving normal departmental mail. This will disrupt the normal e-mail functionality. In addition, the users will not be seen by their own departments.
Reference
Exchange 2003 Admin HELP

QUESTION 119
You are the Exchange administrator for Certkiller .
The network consists of a single Active Directory domain named Certkiller .com.
Exchange Server 2003 is used as the companywide messaging system.
Network administrators create a new child domain.
They also create a new user accounts in the child domain and configure the accounts to use mailboxes located on the Exchange servers in the parent domain.
Users in the new domain report that they receive an error message when they open Microsoft Outlook to access their Exchange mailboxes.
The message state states that the mailbox name cannot be matched to a name in the address list.
You discover that none of the user accounts in the child domain have e-mail addresses.
You need to ensure that users in the child domain can access their mailboxes.
What should you do?

A. Run the setup /domainprep command in the child domain. Create a Recipient Update Service for the child domain.
B. Create a new storage group on an Exchange server. Move all mailboxes for the child domain users to a new mailbox store in the storage group.
C. Create a new e-mail address recipient policy. Apply the policy to only Exchange recipients that have mailboxes.
D. In the child domain, create a user account named ExchangeProxyAccount. Delegate Exchange Full Administrator permissions in the Exchange organization to this account.

Answer: A
Explanation
Network administrators create a new child domain. They also create a new user accounts in the child domain and configure the accounts to use mailboxes located on the Exchange servers in the parent domain.
Exchange uses the Recipient Update Service primarily to generate and update default and customized address lists, and to process changes made to recipient policies. This service ensures that when new recipient policies or

address lists are created, their content is applied to the appropriate recipients in the organization. The Recipient Update Service also applies existing policies to new recipients that are created after the policy or address list has already been established. In this way, information is kept current with minimal administrative overhead.

You must have at least one Recipient Update Service for each domain in your organization, and it must be run from an Exchange 2003 or Exchange 2000 server. For domains that do not have these Exchange servers, the Recipient Update Service must be run from an Exchange server outside of the domain. You can set up more than one Recipient Update Service for a domain, if there are multiple domain controllers. Each Recipient Update Service must read from and write to a unique domain controller.

Note

If you do not have a Recipient Update Service for a domain, you cannot create recipients in that domain.

QUESTION 120

You are the Exchange administrator for Certkiller .

The Exchange organization contains a single Exchange Server 2003 computer.

The network connects to the Internet via an ISP to send and receive e-mail messages.

All internal users connect to the Exchange server by using HTTP.

No SMTP connector is configured.

You monitor the performance and utilization of the Exchange server on an ongoing basis.

There is normally very little SMTP traffic to and from the server.

You notice a sudden increase in the workload of the server.

When you investigate, you discover a very large increase in the number of SMTP connections that are being made to and from the server.

There is no corresponding increase in the number of messages that are sent or received by internal users.

You need to reduce the workload of the Exchange server to normal levels.

What should you do?

A. Restart the SMTP service.

B. Add an additional SMTP virtual server.

C. Disable the SMTP relay on the SMTP virtual server.

D. Configure an SMTP connector to connect to a smart host at the ISP.

Answer: C

Explanation:

The server is being used as a relay agent for an attack. Prohibiting the relay will cause the SMTP requests to cease. This is not going to cause a problem as all current clients use HTTP to connect to the server.

Incorrect answers:

A. The service is functioning correctly. Since local clients use HTTP, the SMTP service is rarely used; the sudden increase can't be coming from internal clients.

B. Since internal clients do not use SMTP, adding another SMTP server will only make the problem worse, as now the attacker can use two servers instead of one!

D. Configuring an SMTP connector to connect to a smart host at the ISP will not have any effect on the problem as the issue is not with the connection, but with the incoming traffic. The most important part of the question states that the internal users all connect via HTTP, and there is a sudden increase in SMTP traffic. This can't be caused by your connection to your ISP.

QUESTION 121
You are the Exchange administrator for Certkiller .
The Exchange organization contains a single server that runs Exchange Server 2003.
Microsoft Outlook 2002 and Outlook Express are the only e-mail clients in use on the intranet. External users retrieve e-mail by using Outlook Web Access.
Some users report that they receive error messages when they send e-mail to recipients outside of the company.
The error messages state that one of the recipients was rejected by the Exchange server.
You discover that this error occurs only for users of Outlook Express.
Users of Outlook 2002 can send messages to the same recipients without error.
You need to ensure that users of Outlook Express can successfully send e-mail messages to all recipients inside and outside of the company.
Your solution most not exposes the Exchange server to unnecessary security risks.
What should you do?

A. Configure the SMTP virtual server to allow relays only from IP addresses on the intranet.
B. Configure the POP3 virtual server to accept connections only from IP addresses on the intranet.
C. Configure the SMTP virtual server to accept connections only from IP addresses on the intranet.
D. Configure the SMTP connector to allow messages to be relayed to the domains on the property page of the connector's address space.

Answer: B

Explanation:
Outlook 2002 will connect to Exchange 2003 using MAPI, Outlook express will connect using POP
Exchange connection schema are based on protocols
Incorrect answers:

A. The issue only applies to Outlook Express. Outlook users do not have the issue. Therefore, the problem must be with POP3, and not with SMTP.
C. The issue only applies to Outlook Express. Outlook users do not have the issue. Therefore, the problem must be with POP3, and not with SMTP.
D. They specify that any solution most not exposes the Exchange server to unnecessary security risks this option will work but it will also open up the server to an attack by relaying messages without regard to location or authenticity.

QUESTION 122
You are the Exchange administrator for Contoso.
The newly deployed Exchange organization contains a single Exchange Server 2003 computer named Mail1
Contoso intranet does not have a full-time Internet connection.
A demand-dial router connects the intranet to the company's ISP.
The ISP gives Contoso a user account and static IP address.
The ISP agrees to queue Contoso e-mail on its SMTP server so that MAIL1 can retrieve the queued email.
You discover that Mail1 is not receiving e-mail from the Internet.

You need to ensure that Mail1 can retrieve e-mail that is stored at the ISP.
What should you do?

A. Configure an SMTP connector that sends the HELO command.
B. Configure an SMTP connector to forward all outbound messages to the ISP's SMTP server and to issue an ETRN command.
C. Configure your SMTP virtual server to use the ISP's SMTP server as a smart host.
D. Configure your SMTP virtual server to use the same DNS server that is used by the ISP's SMTP server as an external DNS server.

Answer: B
Explanation
Using the SMTP connector without a Full-Time Internet Connection
Many smaller companies cannot afford a full-time connection to the Internet. Unfortunately, SMTP was originally designed under the assumption that all SMTP servers will be online all the time. Later, a new command for SMTP was developed called TURN, but it was implemented only with limited success, partially due to security concerns.
RFC 1985 now defines the SMTP command ETRN (Enhanced TURN), which allows an SMTP client to connect to an SMTP server that has been queuing mail for the client and issue the ETRN command. The SMTP server will then deliver any queued messages to the SMTP server client.
Reference
How to use SMTP connectors to connect routing groups in Exchange 2003 KB 822941

QUESTION 123
You are the Exchange administrator for Certkiller .
The Exchange organization contains a single server that runs Exchange Server 2003.
The Exchange server supports POP3, IMAP4, and MAPI clients.
Company employees use various client software applications for e-mail.
POP3 users report that they receive a Winmail.dat attachment on every e-mail message that they receive.
The attached file contains only random characters.
You need to ensure that POP3 users do not receive Winmail.dat attachments.
What should you do on the POP3 virtual server?

A. Configure the character set to US ASCII.
B. Configure the message encoding format to MIME.
C. Configure the message encoding format to UUENCODE.
D. Disable support of rich-text formatting.

Answer: D

Explanation:
The Message Format tab in Exchange Server 2003 is used to configure the way that MAPI messages are converted when retrieved by a Post Office Protocol version 3 (POP3) client. You can choose the MIME encoding type and the character set. You can also choose whether to send messages to POP3 clients in Exchange Rich Text format, Standard Text format, or both. The Exchange Rich Text format will not be used if HTML formatting is selected in Outlook. You should only select the Exchange Rich Text format option if every

client that will be connecting to this virtual server supports Exchange Rich Text Format. Incompatible clients will display blank messages with unviewable file attachments called winmail.dat. The winmail.dat file contains all the rich text formatting information for the message.
Incorrect Answers:

A. Many mail systems that do not use the US ASCII character set for text. Enforcing this format will result in any email server that uses a non US ASCII character set to generate the same winmail.dat file.
B. When the MIME encoding format is used, disallowed characters are replaced with plain text where possible, but no winmail.dat file is generated. If a POP3 client can't utilize rich text formatting, this file remains in the message, and contains unprintable characters.
C. UUEncode takes a binary file and converts to 7 bit ASCII. This is used in news groups to convert a binary file such as a photograph to ASCII text.
Reference
Exchange Server 2003 Administration Guide; Exchange Server 2003 Help File

---

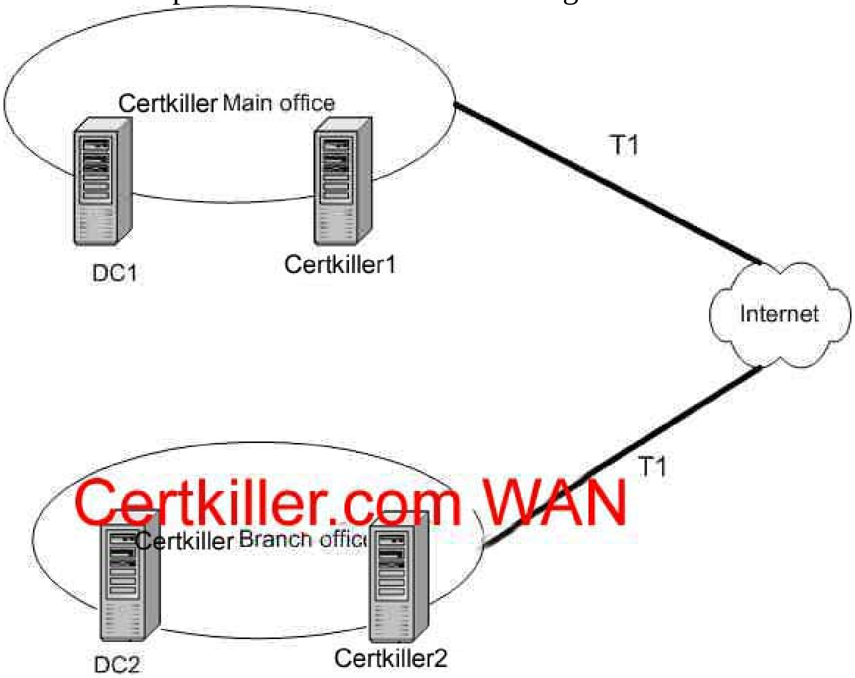
QUESTION 124
You are the Exchange administrator for Certkiller .
The company's network consists of a single Active Directory domain named Certkiller .com.
The Exchange organization contains two servers, the company's server and a subsidiary company's server.
Certkiller 's server runs Exchange Server 2003 and the subsidiary's server runs Exchange Server 5.5.
Both Exchange servers are located in the same Active Directory site and in the same routing group.
Active Directory Connector (ADC) is configured with a two-way connection agreement between the company and the subsidiary.
The company's management decides to sell the subsidiary.
You delete the subsidiary user mailboxes from the Exchange 5.5 server.
You discover that the deletions do not replicate to Active Directory.
You need to ensure that the deletions are replicated to Active Directory.
What should you do?

A. Configure the connection agreement as a one-way connection agreement from Exchange to Microsoft Windows.
B. Configure the connection agreement as a one-way connection agreement from Microsoft Windows to Exchange.
C. Configure the connection agreement to delete the objects from Active Directory when replicating deletions from the Exchange 5.5 directory.
D. Configure the connection agreement to delete the objects from the Exchange 5.5 directory when replicating deletions from Active Directory.
E. Configure the connection agreement so that it is not the primary connection agreement for the connected Exchange organization.
F. Configure the connection agreement so that it is not the primary connection agreement for the connected Microsoft Windows domain.

Answer: C
Explanation
They tell us Active Directory Connector (ADC) is ALREADY configured with a two-way connection

agreement between the company and the subsidiary. They need to check their ADC settings in order tell to Active Directory that the mailboxes have been deleted:
Incorrect answers:
A, B. There is currently a connector in place. There is no need to establish another one.
D. Configuring the connection agreement to delete objects in Exchange is not needed since the objects were deleted in Exchange 5.5 in the first place. The changes need to be replicated to Active Directory.
E, F. There is only one connection agreement in place. Therefore, it has to be the primary one. There is no way to tell the only agreement that is it not primary. In addition, changing the agreement to not be primary will not change how replication is handled across it.

QUESTION 125
You are the Exchange administrator for Certkiller .
The company operates a main office and one branch office.
Both offices are connected to the Internet.
A VPN provides interoffice connectivity.
The relevant portion of the network is configured as shown in the exhibit.



The network consists of a single Active Directory domain Certkiller .com.
Each office contains one domain controller and one server that runs Exchange Server 2003.
The domain controllers are name DC1 and DC2.
The Exchange servers are named Certkiller 1 and Certkiller 2. In each office, all user mailboxes are hosted on the local Exchange server.
Microsoft Outlook is the only e-mail client in use.
When users in the branch office send e-mail messages, they report that Outlook sometimes requires several minutes to resolve user names to e-mail addresses.
The problem occurs intermittently, but it affects all users in the branch office.
These users experience no delays when they open e-mail messages and attachments.
Users in the main office no not experience any delays when they open e-mail messages or when user names resolve to e-mail addresses.

You need to improve the performance of Outlook name resolution in the branch office.
What should you do?

A. Configure DC2 as a global catalog server.
B. Configure the interoffice VPN to pass LDAP traffic.
C. Configure the client computers in the branch office to authenticate to DC2.
D. Modify Active Directory to place both office networks in the same site.

Answer: A
Explanation
DS1 is the only Catalog server. Adding a GC to the branch office will enable Exchange to look up the attributes of the user it needs, and hence resolve the issue. The problem was intermittent due to traffic on the network. When traffic was high, response was slow.

QUESTION 126
You are the Exchange administrator for Certkiller . Certkiller operates a main office in Toronto and five branch offices in Europe.
The network consists of a single Exchange organization that contains three servers that run Exchange Server 2003.
All three Exchange servers are located in the main office.
Microsoft Outlook is the only e-mail client application in use.
All client computers run Microsoft Windows XP Professional, Windows 2000 Professional, or Windows 98.
You deploy a new Exchange Server 2003 computer in the main office.
You move 25 percent of user mailboxes to the new Exchange server.
Some users in a branch office now report that they cannot open Outlook.
They receive an error message indicating that their Exchange server cannot be located.
You discover that the only users who experience this problem are users whose computers run Windows 98 and whose mailboxes are located on the new Exchange server.
You need to ensure that all users can successfully access Outlook.
What should you do?

A. Configure Outlook on the affected computers to use the new Exchange server.
B. Configure the new Exchange server to register with a WINS server.
C. Add a host (A) resource record and a mail exchanger (MX) resource record for the new Exchange server to the DNS zone.
D. Configure the other three Exchange servers with an Lmhosts file entry for the new Exchange server.

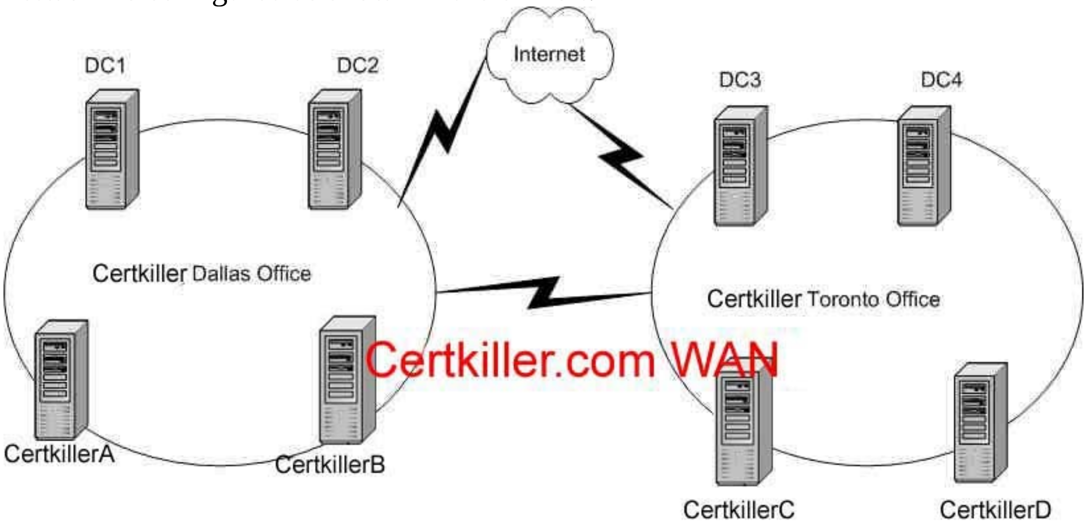
Answer: B

Explanation:
Windows 98 does not use DNS natively for name resolution. It uses WINS for NetBIOS name lookups. Adding a WINS address for the Exchange server should resolve the problem.
Incorrect Answers:

A. Outlook should not need to be modified. All clients other than Win98 clients can connect successfully.

Assuming that all users are using the same version of Outlook, this can't be the problem.
C. Configuring an MX record will not resolve the problem. As all other users are able to connect, and all connections are occurring within the organization, the MX record is not needed.
D. Configuring the servers with an LMHosts file will not help the clients connect. It is designed to do NetBIOS to IP address lookups on a computer that can't do those lookups for itself. As the server is not having a problem, adding an LMHosts file to the server will not resolve the problem.

QUESTION 127
You are the Exchange administrator for Certkiller . The network consists of a single Active Directory domain named Certkiller .com. The company operates an office in Dallas and an office in Toronto. Both offices are part of a single routing group and a single Exchange organization. The relevant portion of the network is configured as shown in the exhibit.



DC1 through DC4 are domain controllers.
Certkiller A through Certkiller D are Exchange Server 2003 computers.
The SMTP virtual server on Certkiller A is configured as a bridgehead server for an SMTP connector in the Dallas office.
The SMTP virtual server on Certkiller C is configured as a bridgehead server for an SMTP connector in the Toronto office.
The two SMTP connectors are configured with the same cost.
New e-mail polices state that that all outbound and inbound Internet e-mail must be distributed equally between the two Internet connections. Outbound Internet e-mail already complies with the new policies. However, all inbound Internet e-mail is received through the Internet connection in Dallas.
You need to ensure that inbound Internet e-mail also complies with the new polices.
What should you do?

A. Configure an additional host (A) resource record and mail exchanger (MX) resource record for the Certkiller .com domain on the Internet DNS servers. Configure the MX record with the same priority value as that of the existing MX record.
B. Configure an additional host (A) resource record and mail exchanger (MX) resource record for the Certkiller .com domain on the Internet DNS servers. Configure the MX record with a priority value that is higher than that of the existing MX record.
C. Add the Certkiller .com namespace to the SMTP connector in Toronto.

D. Increase the cost of the SMTP connector in Toronto.

Answer: A

Explanation:
To evenly distribute incoming e-mail from outside the organization, a new MX record must be created, pointed to the Toronto server (Certkiller C). The MX record must have the same value as the existing record. If this is not the case, messages will be delivered to the connector with the lower cost.
Incorrect Answers:
B. Creating a new MX record will enable another path for inbound messages to flow. However, assigning a higher cost to it will prevent the connection from ever being used unless the original link goes down.
Since the messages are not distributed evenly, this can't be the correct answer.
C. Adding the namespace to the SMTP connector in Toronto will forward all outbound mail destined for Toronto to go there without passing through the internet. Since the question states that the incoming mail is already functioning as intended, this step can't be correct.
D. Increasing the cost of the SMTP connector in Toronto will not have any noticeable effect. The connector is designed to handle mail flow between the two sites, and will not affect incoming mail from the internet.

QUESTION 128
You are the Exchange administrator for Certkiller .
The company has a business partnership with Trey Research.
Each company has its own Active Directory domain.
The domains are named Certkiller .com and treyresearch.com, respectively. Certkiller and Trey Research are in the same Exchange organization.
The organization contains three servers that run Exchange Server 2003.
One Exchange server is configured with an SMTP connector for all Internet e-mail.
Most users have SMTP addresses of alias@ Certkiller .com.
However, some users have SMTP addresses of alias@treyresearch.com.
The alias@treyresearch.com users report that they cannot receive e-mail messages from the Internet.
However, they can send and receive e-mail messages internally.
They can also send e-mail messages to Internet recipients.
You need to ensure that all users can send and receive Internet e-mail messages.
What should you do?

A. Create a recipient policy that adds the alias@treyresearch.com SMTP address for all Trey Research users.
B. Add the user principal name (UPN) suffix for treyresearch.com to the forest.
C. Add the treyresearch.com namespace to the SMTP connector at Certkiller .com.
D. Add a mail exchanger (MX) resource record to the treyresearch.com domain on the appropriate DNS servers.

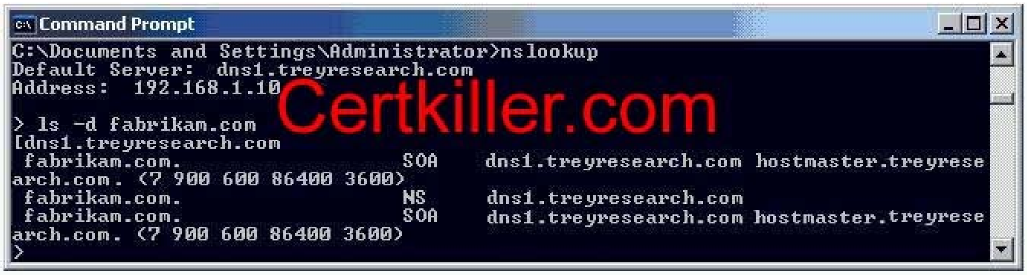
Answer: D

Explanation:
All mail is flowing correctly with the exception of inbound mail for treyresearch.com. The only possible

explanation for this is that the external DNS servers do not know how to handle incoming mail for this domain. The way to resolve this is to add an MX record to the external DNS server for the treyresearch.com domain.
Incorrect Answers:

A. Adding alias@treyresearch.com to the recipient policy will add another SMTP address to the list of possible mail addresses. This will not allow users to receive mail on that address. Even if it did, the answer would still be incorrect since only a few users are using Treyresearch, and these users already have this as an SMTP address.
B. Adding a UPN suffix will not affect e-mail flow in any way. It is used to help streamline domain naming in a forest. Therefore, this can't be the correct answer.
C. Adding the treyresearch namespace to the SMTP connector will not resolve the problem, as the SMTP connector is used only for connections between sites, and has no effect on incoming e-mail from outside the organization.

QUESTION 129
You are the Exchange administrator for Certkiller .
The network consists of a single Active Directory domain named Certkiller .com.
The Exchange organization contains three servers that run Exchange Server 2003.
One Exchange server is configured with an SMTP connector for all Internet e-mail.
The SMTP connector is configured to use DNS for e-mail delivery.
Certkiller 's DNS server is named DNS1. Certkiller .com.
Certkiller enters into a business partnership with Fabrikam, Inc.
This company has its own Active Directory domain, which is named fabrikam.com.
This company's DNS server is named DNS1.fabrikam.com.
Users report that they cannot send Internet e-mail messages to recipients at Fabrikam, Inc. However, they can send Internet e-mail messages to other recipients, and they can receive Internet e-mail messages from users at Fabrikam, Inc.
You use nslookup command to view the DNS information for fabrikam.com. The output is shown in the exhibit.



```
C:\Documents and Settings\Administrator>nslookup
Default Server:  dns1.treyresearch.com
Address:  192.168.1.10

> ls -d fabrikam.com
[dns1.treyresearch.com
 fabrikam.com.                  SOA    dns1.treyresearch.com hostmaster.treyrese
arch.com. (7 900 600 86400 3600)
 fabrikam.com.                  NS     dns1.treyresearch.com
 fabrikam.com.                  SOA    dns1.treyresearch.com hostmaster.treyrese
arch.com. (7 900 600 86400 3600)
>
```

You need to ensure that users can send Internet e-mail messages to Fabrikam, Inc. Your solution must not affect other e-mail delivery.
What are two possible ways to achieve this goal? (Each correct answer presents a complete solution. Choose two)

A. Delete the fabrikam.com zone from DNS1. Certkiller .com.
B. Configure the SMTP connector to use an SMTP server at fabrikam.com as a smart host for e-mail delivery.
C. Add the mail exchanger (MX) and host (A) resource records for fabrikam.com to the fabrikam.com zone on DNS1. Certkiller .com.

D. Configure DNS1.treyresearch.com with a conditional forwarder for fabrikam.com.
Configure the forwarder record to use DNS1.fabrikam.com.
E. Add the Certkiller .com address space to the SMTP connector.

Answer: C, D

Explanation:
C. Adding an MX record for Fabrikam to the DNS1. Certkiller .com will enable the Exchange Server to find the Fabrikam domain from within Certkiller and will allow internet mail to travel to Fabrikam from Certkiller .
D. Configuring DNS1 as a forwarder to Fabrikam will enable all requests for the Fabrikam domain from Certkiller to be sent to Fabrikam for resolution. Since Fabrikam has records for its own MX servers for internet mail, the messages will be delivered.

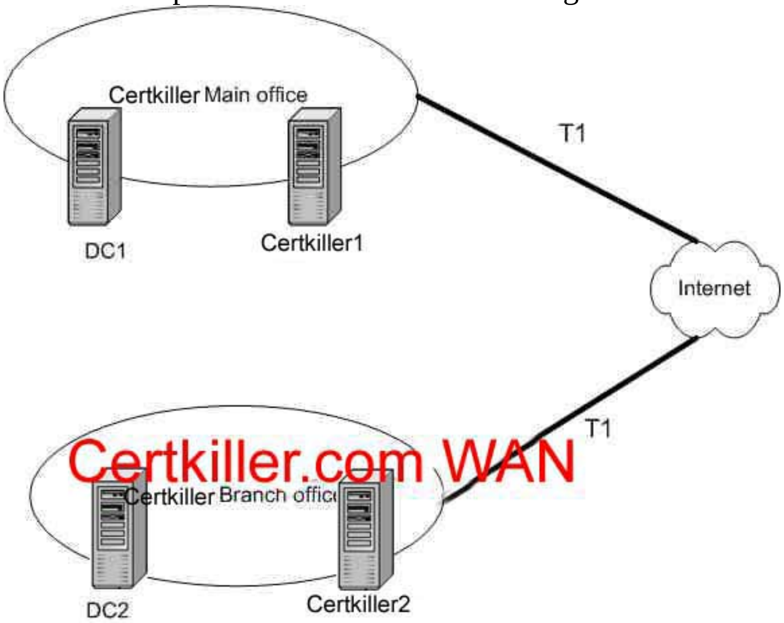
QUESTION 130
You are the Exchange administrator for Certkiller .
The network consists of a single Active Directory domain named Certkiller .com.
The domain contains a single domain controller named DC1.
The Exchange organization contains a single Exchange Server 2003 computer named Certkiller 1 that hosts all user mailboxes. Certkiller opens a new branch office.
The new office is connected to the main office by means of VPN connection.
The branch office contains a domain controller named DC2 and an Exchange Server 2003 computer named Certkiller 2.
The VPN connection is configured to allow all network traffic only between DC2, Certkiller 2, and the main office.
The branch office contains five users.
You create mailboxes for these users on Certkiller 2.
The users report that they can access their e-mail by using Microsoft Outlook 2002, but that they cannot display the Global Address List (GAL).
The users also report that Outlook cannot resolve e-mail addresses when they send e-mail messages.
You need to ensure that the branch office users can perform these tasks.
What should you do?

A. Configure the VPN to permit global catalog queries between the branch office network and the main office network.
B. Configure Certkiller 2 to force the selection of DC1 as a global catalog server.
C. Configure the VPN to permit LDAP traffic (port 389) from the branch office network to the main office network.
D. Configure Certkiller 2 to have a static TCP/IP route from the branch office network to the main office network.

Answer: A
Explanation
By default traffic to query a DC Global catalog (port 3268) is not permit with a normal VPN configuration. Therefore you will need to setup your VPN Filter rule to permit 3268 port traffic to query a catalog global DC to search for address book.

Incorrect Answers
B. Force DSaccess to query DC1 with not solve nothing, because is a traffic problem for LDAP global catalog queries.
C. This is a tricky answer. LDAP is used by Active Directory, Active Directory Connector, and the Microsoft Exchange Server 5.5 directory. Global Catalog queries are LDAP queries, but this queries go for 3268 port not port 389. The Windows 2000 Active Directory global catalog (which is really a domain controller "role") listens on TCP port 3268. When you are troubleshooting issues that may be related to a global catalog, connect to port 3268 in LDP
D. To have an static route just permit to avoid to configure one protocol as OSPF for routing
Reference
XGEN: TCP/UDP Ports Used By Exchange 2000 Server 278339
Port Requirements for the Microsoft Windows Server System 832017
XCCC: Exchange 2000 Windows 2000 Connectivity through Firewalls 280132
VPN servers and firewall configuration Windows Server 2003 Help

QUESTION 131
You are the network administrator for Certkiller .
The company operates a main office and a one branch office.
Both offices are connected to the Internet and use a VPN for interoffice communications.
The relevant portion of the network is configured as shown in the exhibit.



The network consists of a single Active Directory domain named Certkiller .com.
Each office has one domain controller.
Each office also has one Exchange Server 2003 computer, which hosts all mailboxes for users in that office.
Users in the branch office report that sending e-mail messages from Certkiller 2 sometimes requires several minutes.
However, the problem does not occur consistently.
You discover that a large quantity of LDAP queries is passed from the branch office to DC1.
You verify that DC2 is configured as a global catalog server.
You need to reduce the LDAP traffic sent across the VPN.

What should you do?

A. Promote Certkiller 2 to domain controller.
B. Configure Certkiller 2 to force the selection of DC2 as a global catalog server.
C. Add the fully qualified domain name (FQDN) and IP address of DC2 to the Hosts file on Certkiller 2.
D. Modify Active Directory to place both office networks in the same site.

Answer: B
Explanation
Exchange use Dsaccess service to find a set of available directory service servers. For each available directory service server, DSAccess opens LDAP connections dedicated solely on behalf of each process that is using DSAccess. DSAccess updates these LDAP connections with directory service state information (Up, Slow, or Down) that it detects, and channels requests based on this state information. The set of LDAP connections to those available domain controllers and global catalogs and their associated states forms the profile of the process. For reliability and scalability, DSAccess supports a load-balancing mechanism to distribute user context directory service requests in a round-robin fashion among these LDAP connections.
Only one Recipient Update Service is active within each Active Directory domain; the others remain idle. The Recipient Update Service is fully integrated with the Exchange System Attendant (Mad.exe). According to the schedule you've set or by means of the Update Now option, the service contacts a local domain controller and proceeds to update address lists based on the rules set.
By default DSAccess is configured to perform the "automatically discover servers"
Certkiller 2 is not included in the same site as DC1 and DSAccess is already configured with DC1 as the configuration server for the Certkiller .com domain. It is thus querying to DC1 server across the wan link and generating a large quantity of LDAP queries
To fix this issue you can change dcsaccess order and point to DC2 by changing the automatically discover server to manually although is not a MS recommended practice
Incorrect Answer
A Can FIX the problem but is not a good option
C If Certkiller 2 can resolve DC1 you can suppose that resolve DC2, but the problem is not resolve the name is resolve who the global catalog and configuration domain controller for Exchange
D If you put both DC's in the same site, Exchange mad.exe will be still querying to DC1 as Configuration Domain Controller
References
Understanding and Troubleshooting Directory Access MS Book Online
Microsoft Exchange 2000 Server Service Pack 2 Deployment Guide
Event ID 2080 from MSExchangeDSAccess KB article 316300

QUESTION 132
You are the network administrator for Certkiller .
Certkiller operates a main office and one branch office.
The network consists of a single Active Directory domain named Certkiller .com.
The two offices are connected by a dedicated frame-relay line.
Each office contains one domain controller.
Each domain controller runs the DNS Server service and hosts and Active Directory-integrated zone.
In each office, all computers are configured to use the local DNS server for DNS name resolution.
Each office contains one Exchange Server 2003 computer, which hosts all user mailboxes for that office.

The domain controller and the Exchange server in the main office are named DC1 and Certkiller A, respectively.
The domain controller and the Exchange server in the branch office are named DC2 and Certkiller B, respectively.
Monday morning, users in the branch office report that they cannot connect to Certkiller B.
You discover that no Exchange services will start on Certkiller B.
When you restart Certkiller B, the services fail to start.
You discover that the frame-relay line between the two offices is in a state of failure.
After restoring the frame-relay line, you restart Certkiller B.
All Exchange services start successfully.
You need to ensure that failures in the frame-relay line will not prevent either Exchange server from starting normally.
What should you do?

A. Configure Certkiller B to have a static route to DC2.
B. Configure Certkiller B to force the selection of DC1 as a global catalog server.
C. Modify the Active Directory configuration so that DC2 is a global catalog server.
D. Remove all existing Active Directory connection objects, and manually create a new connection object between DC1 and DC2.

Answer: C

Explanation:
The Exchange services will fail if a global catalog can't be contacted. Enabling a GC on the domain controller in the remote office will enable the functionality of the Exchange server even if the link fails.
Reference
XADM: The Information Store Service May Fail to Start and an Error Message May Be Displayed KB 303186
How to Troubleshoot Exchange Server 2003 System Attendant When It Does Not Start 821907

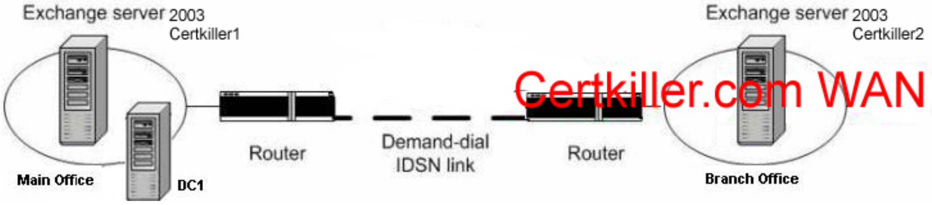
QUESTION 133
You are the Exchange administrator for Certkiller .
The network consists of a single Active Directory domain named Certkiller .com.
The domain contains four domain controllers named DC1 through DC4.
DC1 holds all operations master roles and is the only global catalog server.
The network also includes three Exchange Server 2003 computers, which run Microsoft Windows Server 2003.
The Exchange servers collectively contain 8,000 user mailboxes.
Certkiller acquires another company and migrate 7,500 new users to Certkiller .
The new users work in a separate branch office that contains two new domain controllers.
The branch office is connected to Certkiller 's main office by a T1 line.
The new domain controllers are not configured as global catalog servers, and they do not host any operations master roles.
You distribute the mailboxes for the new users evenly across the three existing Exchange servers. All users now report that e-mail access is extremely slow.
Users in the branch office report that e-mail is often so slow that it is unusable.
All users report that address book resolution is extremely slow and that sometimes it fails.

You need to ensure that all users have responsive e-mail service.
Which two actions should you perform? (Each correct answer presents part of the solution. Choose two)

A. Configure an additional domain controller in each office as a global catalog server.
B. Configure one domain controller in the branch office to host the PDC emulator role.
C. Install the two new Exchange servers in the branch office. Move all mailboxes for branch office users to the new Exchange servers.
D. Install an additional domain controller in the branch office. Configure the new domain controller as a DNS server. Configure all client computers in the branch office to use the new domain controller for DNS name resolution.
E. Install an additional Exchange server in the main office. Move all mailboxes for branch office users to the new server. Disable POP3, HTTP, and IMAP access on the new server.

Answer: A, D
Explanation
They have too many users to be handled by one Global Catalog, configuring a new dc for branch offices will solve part of the problem, configuring a DNS to be queried by branch offices solve the name resolution issue.
Reference
Designing and Deploying Directory and Security Services guide
Planning Operations Master Role Placement
How to Troubleshoot Query-Based Distribution Groups 822897

QUESTION 134
You are the Exchange administrator for Certkiller .
All network computers are members of a single Active Directory domain named Certkiller .com.
The relevant portion of the network is configured as shown in the exhibit.



DC1 is a domain controller.
Certkiller 1 and Certkiller 2 run Exchange Server 2003.
Users at each office use the local Exchange server for e-mail.
Users at the branch office report that when they create e-mail messages, there are occasionally problems resolving e-mail addresses to names.
When these problems occur, an administrator at the branch office restarts Certkiller 2.
If the administrator tries to restart Certkiller 2 immediately, the Exchange services fail to start.
If the administrator waits 10 minutes before restarting Certkiller 2, the Exchange services usually start correctly and the problems disappear.
When these problems occur, users can still log on to their client computers. You receive no response when you attempt to ping Certkiller 1 from Certkiller 2.
You need to prevent these e-mail problems and server problems from occurring.
What are two possible ways to achieve this goal? (Each correct answer presents a complete solution. Choose two)

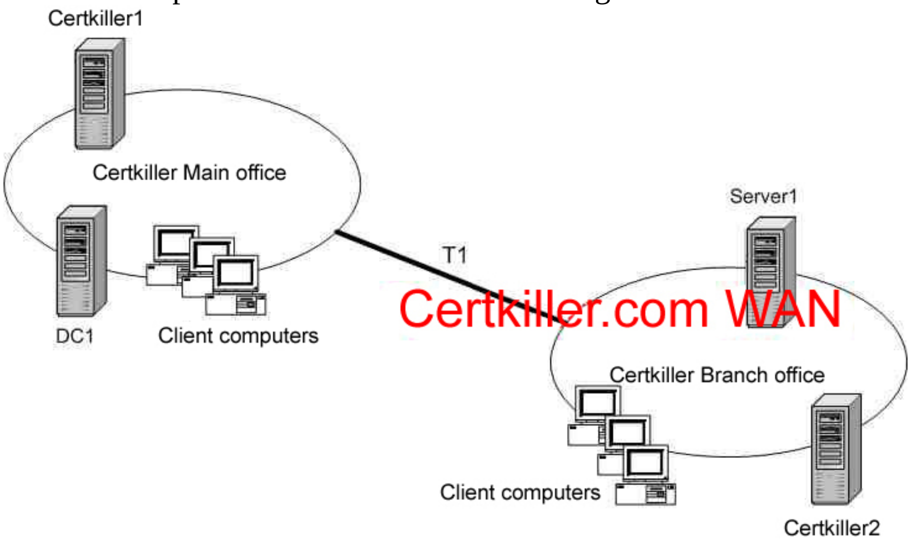
A. Install a backup frame-relay line between the main office and the branch office.
B. Configure the routers between the main office and the branch office to place a high priority on LDAP traffic.
C. Create a VLAN that places both offices networks in a single logical IP address range.
D. Install a domain controller at the branch office. Configure the new domain controller to host the global catalog.
E. Configure Certkiller 2 as a front-end server only. Move all user mailboxes to Certkiller 1.

Answer: A, D

Explanation:

A. Adding an additional frame relay line will help since the issue lies with the Global Catalog not responding in a timely manner. When the administrator reboots the server immediately, the probable cause for it not coming back successfully is that the WAN link is saturated and Exchange can't contact a Global Catalog. Adding a line will lessen the load and allow the contact of the GC.
D. Adding a Global Catalog server to the branch office will allow the name attributes to be looked up quicker and locally in the GC. Since the resolution would not be dependent upon the WAN connection, the name resolution would occur, and if the Exchange server had to be restarted, it could be using the local GC as its contact.

QUESTION 135
You are the Exchange administrator for Certkiller .
The Exchange organization contains a single Exchange Server 2003 computer named Certkiller 1.
A domain controller named DC1 runs the DNS and hosts an AD integrated DNS zone.
All client computers run Microsoft Windows XP Professional. Outlook 2003 is e-mail client in use.
The branch office network contains a member server named Server1 that runs Windows Server 2003 and the DNS Service.
At the main office, you install Exchange Server 2003 on a new server named Certkiller 2.
You ship Certkiller 2 to the branch office, where it is connected to the local network.
Certkiller 2 is configured to use Server1 for DNS name resolution.
The relevant portion of the new network configuration is shown in the exhibit.



When you start Certkiller 2 for the first time in the branch office, some Exchange services fail to start.
You find the following message in the application event log on Certkiller 2:
Process MAD.EXE. Dsaccess could not find any Global Catalog servers in the enterprise. Promote one or more of your Domain Controllers to a Global Catalog to allow DSAccess to function properly.
You confirm that DC1 is configured as a global catalog server, and that all computers in the branch office can connect to DC1 by using its IP address.
You need to solve this problem and ensure that all Exchange services start without error.
What should you do?

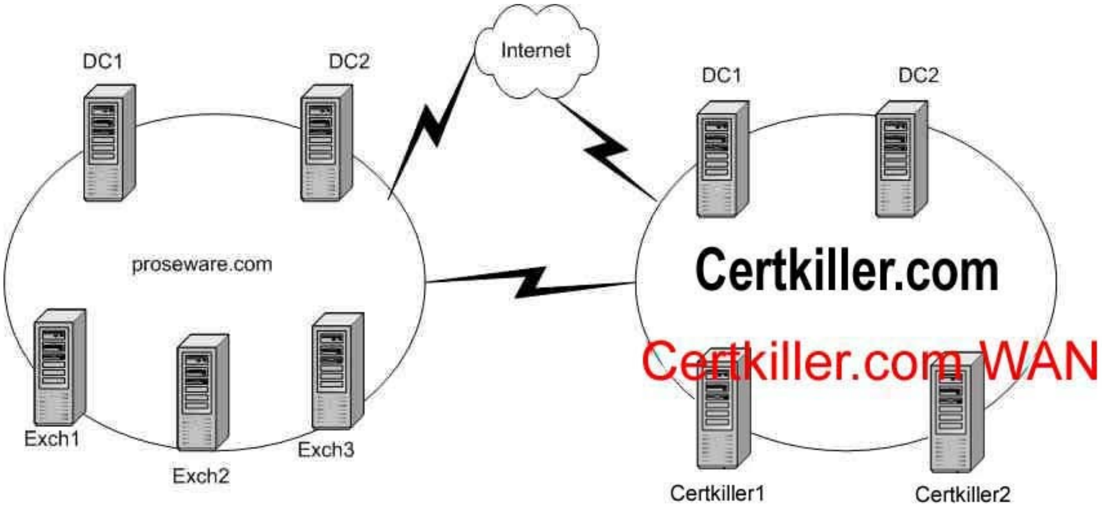
A. Configure Server1 to host a secondary DNS zone and to use DC1 as its primary.
B. Configure the routers between the two office networks to use static routes.
C. Configure the DNS zones on Server1 and DC1 to allow dynamic updates.
D. Configure Certkiller 2 to use static host file entries that point to DC1 and Certkiller 1.

Answer: A

Explanation:
Because Certkiller 2 is configured to use Server1 for DNS name resolution, the cause of the problem locating the
global catalog is that server1 is running the DNS service but is not holding any DNS configured zone and is therefore acting like any client querying to its primary DC as a DNS client but the DNS server can't resolve to the client that queried it; Certkiller 2 is querying to Server1 for the global catalog but can't find a SVR record for
DC1
Providing the host file entries to DC1 and Certkiller 1 will enable name resolution for DC1 but not a DSACCESS service query to a Domain controller with the Global Catalog role. If they configure the zones in Server1, it will be able to resolve the names and services to any server that query server1
Incorrect Answers:
B. Providing static routes would avoid network traffic because the router does not need to use any protocol to construct their router tables.
C. Configuring the zones on DNS1 to allow dynamic updates will have no effect here since the problem lies in Certkiller 2 not being able to contact a GC and not with it registering its dynamic IP address.
D. Configuring a host file to Certkiller 1 with a record for DC1 will not work, this provided only host name resolution but not provide access to a Global Catalog

---

QUESTION 136
You are the Exchange administrator for Proseware. Inc.
The company has a business partner named Certkiller . Each business partner has its own office, and a separate Active Directory forest is deployed in each office.
The relevant portion of the network is configured as shown in the exhibit.



The Proseware, Inc, network consists of a single Exchange organization that contains three servers named Exch1, Exch2, and Exch3.
All three servers run Exchange Server 2003.
Exch1.proseware.com is configured as an SMTP bridgehead server for all Internet e-mail.
The Certkiller network consists of a single Exchange organization that contains two servers named Certkiller 1 and Certkiller 2. Both servers run Exchange Server 2003.
Certkiller 1. Certkiller .com is configured as an SMTP bridgehead server for all Internet e-mail.
The IP configuration of Certkiller 1.litware.com is shown in the following table.

Exchange server	**DNS server**	**IP address**
Certkiller 1. Certkiller .com	Internal	10.10.50.20
Certkiller 1. Certkiller .com	Internet	131.107.196.20

An SMTP connector is configured to use DNS to deliver e-mail from Proseware, Inc., to Certkiller . All email between the two offices is sent across a WAN connection. Users report that e-mail delivery frequently fails or takes an unacceptably long time. You discover that the WAN connection between the two offices is unreliable.
You need ensure that e-mail services use the WAN connection when it is available and that services continue even of the connection becomes unavailable.
What should you do?

A. Configure the SMTP connector on Exch1.proseware.com to use a smart host for e-mail delivery. Configure the smart host as 131.107.196.20.
B. Configure the SMTP connector on Exch1.proseware.com to use a smart host for e-mail delivery. Configure the smart host as 10.10.50.20.
C. Add a host (A) resource record and a mail exchanger (MX) resource record for Certkiller 1. Certkiller .com to the Internet DNS server. Configure the MX record with a priority value that is higher than that of the existing MX record.

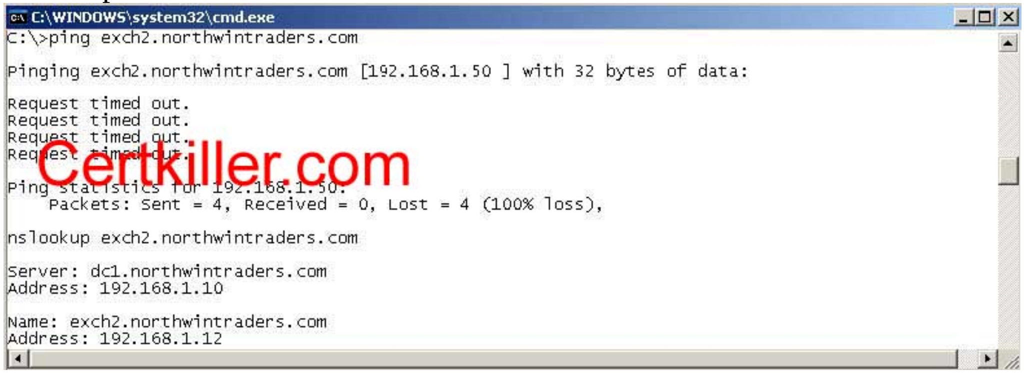
D. Add a host (A) resource record and a mail exchanger (MX) resource record for Certkiller 1. Certkiller .com to the internal DNS server. Configure the MX record with a priority value that is higher than that of the existing MX record.

Answer: C

Explanation:
You need to configure an MX record for Certkiller 1. You will need to assign a different MX priority, like 20. In
this way smtp connector will use default value 10 to flow messages if connection fail smtp will try second value to flow mail.
Incorrect Answers

A. This does not solve the problem because they still using a smart host over SMTP, and in this way still using unreliable connection.
B. If a smart host of 10.10.50.20 is configured you will configure the internal network card.
D. If you configure a DNS MX record for internal network card you are wrong, configuring your MX record because in this way you use your internal network card not your external to flow mail.

QUESTION 137
You are the Exchange administrator for Northwind Traders.
The network consists of a single Active Directory domain that contains a single Exchange organization.
The Exchange servers are named Exch1, Exch2, and Exch3.
All three run Exchange Server 2003 and host user mailboxes.
You discover that users who have mailboxes on Exch1 cannot send e-mail messages to users who have mailboxes on Exch2.
All other e-mail messages flow normally.
You run the ping and the nslookup commands on Exch1.
The output from the commands is shown in the exhibit.



```
C:\>ping exch2.northwintraders.com

Pinging exch2.northwintraders.com [192.168.1.50 ] with 32 bytes of data:

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

Ping statistics for 192.168.1.50:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

nslookup exch2.northwintraders.com

Server: dc1.northwintraders.com
Address: 192.168.1.10

Name: exch2.northwintraders.com
Address: 192.168.1.12
```

You need to ensure that e-mail messages can be sent between all Exchange servers in the Exchange organization.
What should you do?

A. Remove the entry for Exch2 from the Hosts file on Exch1.
B. Remove the entry for Exch2 from the Lmhosts file on Exch1.
C. Manually add the new IP address for Exch2 to the DNS zone for your domain.

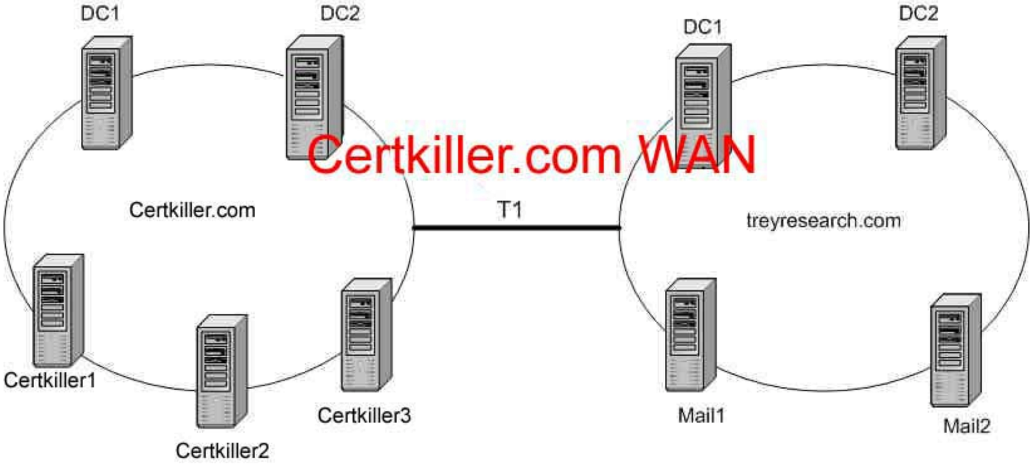
D. Force a re-registration of the DNS resource records on Exch2.

Answer: A

Explanation:
Using the LMHOSTS file is one method of name resolution for NetBIOS names in TCP/IP networks. Hosts file is used for host name to IP resolution and returns the IP address for the specified host name.

QUESTION 138

You are the Exchange administrator for Certkiller .
The network consists of a single Active Directory domain named Certkiller .com.
The domain contains two domain controllers.
Each domain controller runs Microsoft Windows Server 2003 and is configured as a DNS server. The network contains a single Exchange organization that contains three servers named Certkiller 1, Certkiller 2, and Certkiller 3.
All three servers run Exchange Server 2003.
Certkiller merges with a company named Trey Research.
Trey Research's network consists of a single Active Directory domain treyresearch.com.
Trey Research has a single Exchange organization that contains two servers named Mail1 and Mail2.
Both servers run Exchange Server 2003.
A T1 connection is configured between the two company networks. The relevant portion of the resulting network configuration is shown in the exhibit.



You configure a secondary DNS zone for the treyresearch.com zone on the DNS servers at Certkiller .
You configure an SMTP connector with an address space of treyresearch.com.
The SMTP connector is configured to use DNS for message delivery.
You send a test e-mail message to a user at Trey Research.
The message is not delivered and you receive a non-delivery report (NDR).
You need to ensure that you can send e-mail messages from Certkiller to Trey Research across the T1 connection.
What are two possible ways to achieve this goal? (Each correct answer presents a complete solution. Choose two)

A. Configure the SMTP virtual server used by the SMTP connector to use one of the DNS servers at Certkiller .com as an external DNS server.

B. Add mail exchanger (MX) resource records for treyresearch.com on the DNS servers at Trey Research.
C. Configure the SMTP connector to use Mail1.treyresearch.com as a smart host.
D. Remove the secondary zone for the treyresearch.com DNS domain. Configure a conditional forwarder on Certkiller 's DNS servers to forward all name resolution queries for hosts in treyresearch.com to the DNS servers on the Trey Research network.
E. Remove the secondary zone for the treyresearch.com DNS domain. Add a stub zone for the treyresearch.com DNS domain on the DNS servers at
A. Datum Corporation.

Answer: B, D

Explanation:
B. In pure Exchange AD organizations, MX record must be manually added to DNS, by adding an MX record when smtp content reach Trey Research network will query for their MX record to send the mail
D. By configuring a DNS stub zone of treyresearch.com, Certkiller .com DNS will know which dns is authoritative for reyresearch.com and will forward any query to them
Incorrect answers:

A. If they have not an MX record for their Exchange server this will not work, also this will cause NDR for their own domain
B. Smart host in connectors can handle message delivery on a per-domain basis not for different domains s paces
C. By having a secondary zone you can't add an MX record for Exchange server's in treyresearch.com domain
Reference
MS article 821911, How to Configure Exchange Server 2003 to Use a Smart Host IP Address

---

QUESTION 139
You are the Exchange administrator for Certkiller .
The network consists of two subnets.
All client computers are located in one subnet.
All servers are located in a central data center that uses a single IP subnet.
The data center contains the hosts shown in the following table.

Host name	**Role**	**IP address**
Router1	Router	10.1.1.1
Router2	Router	10.1.1.2
Router3	Router	10.1.255.1
DC1	Domain controller	10.1.10.1
DC2	Domain	10.1.10.2

	controller	
Certkiller 1	Mail server	10.1.11.1
Certkiller 2	Mail server	10.1.11.2

You install Exchange Server 2003 on a new computer in the data center.
The computer is named Certkiller 3.
After installation, the network administrator makes some changes to the TCP/IP settings of Certkiller 3 as shown in the following table.

Parameter	**Value**
IP address	10.1.1.3
Subnet mask	255.255.255.0
Default gateway	10.1.1.2

You discover that Certkiller 3 cannot communicate with any of the other servers. You test network connectivity on Certkiller 3 by using the ping command. When you attempt to ping DC1, you receive the following error message: "Destination host unreachable".
You need to ensure that Certkiller 3 can communicate with all computers on the network.
What should you do?

A. Change the IP address of Certkiller 3 to 10.1.10.3.
B. Change the IP address of Certkiller 3 to 10.1.11.3.
C. Change the subnet mask of Certkiller 3 to 255.255.0.0.
D. Change the default gateway of Certkiller 3 to 10.1.1.1.

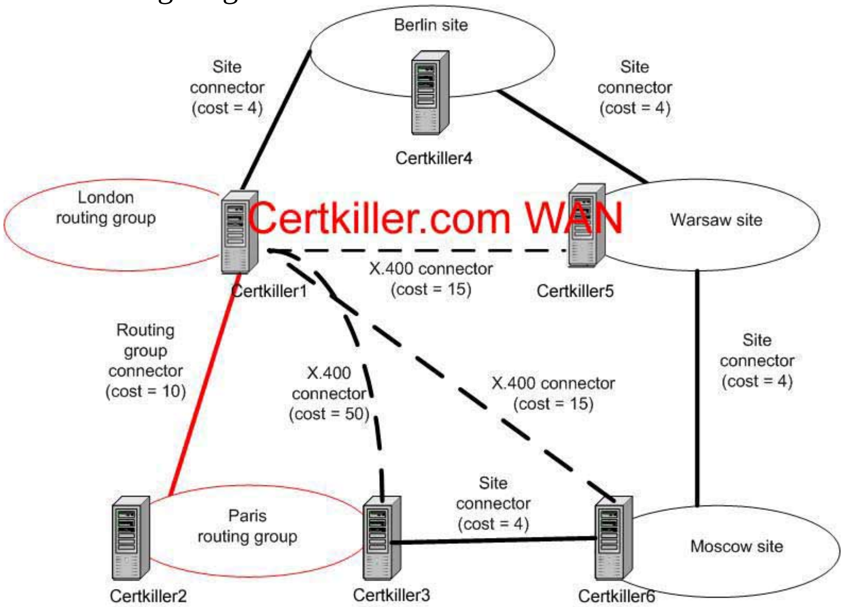
Answer: C

Explanation:
The new server can't connect to the other servers due to the fact that it is on the 10.1.1.x subnet. In order to allow the other servers to see this server, it must be placed in the same subnetwork. The only way to do this from the choices listed is to change the subnet mask to 255.255.0.0.
Incorrect Answers:
A, B. Changing Certkiller 3's IP address to 10.1.10.3 or 10.1.11.3 will not resolve the problem because the server is physically connected to another network. In order for this solution to work, the default gateway would also have to be changed.
D. By reassigning the default gateway, the server is effectively being moved to another subnet. If the IP address is not changed to match, the server will still not be able to connect.

QUESTION 140

You are the Exchange administrator for Certkiller .

The Exchange organization is shown in the exhibit.


Berlin site
Site connector (cost = 4)
Site connector (cost = 4)
Certkiller4
London routing group
Certkiller.com WAN
Warsaw site
Certkiller1
X.400 connector (cost = 15)
Certkiller5
Routing group connector (cost = 10)
X.400 connector (cost = 50)
X.400 connector (cost = 15)
Site connector (cost = 4)
Site connector (cost = 4)
Paris routing group
Moscow site
Certkiller2
Certkiller3
Certkiller6

In the Paris routing group, Certkiller 2 runs Exchange Server 2003, and Certkiller 3 runs Exchange Server 5.5.

Certkiller 2 is configured as the bridgehead server for all routing group connectors in the Paris routing group.

Certkiller 3 is configured as the bridgehead server for the X.400 connector in the Paris routing group.

Mailboxes for all Paris users are in Certkiller 3.

Certkiller 2 is shut down for repairs.

Users who have mailboxes on Certkiller 1 report that there is an unusual delay in the delivery of messages to Paris recipients.

You discover that messages between London users and Paris users are being forwarded to the servers in the following sequence: Certkiller 1, Certkiller 4, Certkiller 5, Certkiller 6, and Certkiller 3.

You need to ensure that messages are delivered as quickly as possible between the London and Paris routing groups.

You do not want to alter the normal flow of messages between any of the other sites or routing groups.

What should you do?

A. Increase the cost of all site connectors to 25.

B. Decrease the cost on the routing group connector between London and Paris to 5.

C. Decrease the cost of the X.400 connector between the London and Paris routing groups to 20.

D. Modify the routing group connector between the London and Paris routing groups to add Certkiller 3 to the list of London routing group

Answer: D

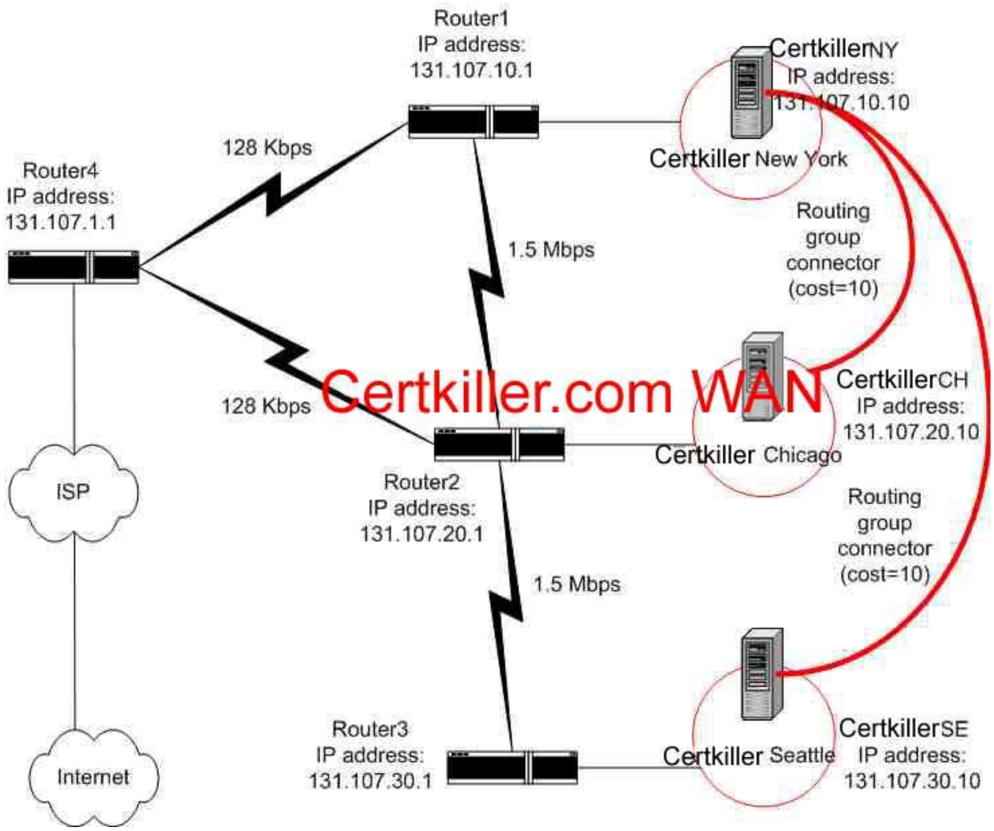
Explanation:

There must be a routing group connector between routing groups if you want to be able to send mail between

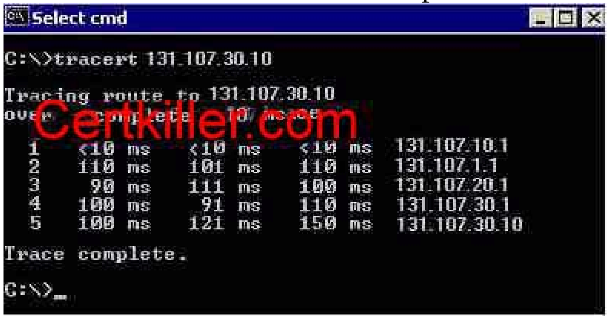
them. In this case we have two links. They told us that Certkiller 2 is shut down for repairs. Certkiller 2 is also the bridgehead server for all routing group connectors in the Paris routing group.
If Certkiller 2 is down, the new server in routing group is Certkiller 3. The only way to go form London to Paris will be based on cost. If we add Certkiller 3 to the list of London routing group connector and because this server
is Exchange 2003, and because by default the cost will be 10 the mail will be flow through Certkiller site connector between Certkiller 1 and Certkiller 4
Incorrect answers:

A. Increasing the cost of all connectors to 25 will disrupts the normal flow of mail for all other sites
B. Decreasing cost of routing group connector between London and Paris to 5 would not help as the other server in Paris is not a bridgehead server and does not automatically accept connections. (In 5.5, bridgehead connections did not exist, but there would be an explicit site connector, and that connector does not exist here.) Even if it did, the given value of 10 would have still work, and mail would not take the circular route that is currently the problem.
C. Decreasing the cost of the London to Paris routing group cost to 20 would still be higher than the link costs of the current route combined, and would be higher than the x.400 connection between London-Moscow-Paris.

QUESTION 141
You are the Exchange administrator for Certkiller .
The Exchange organization contains three routing groups named New York, Chicago, and Seattle. Each routing group contains a single Exchange Server 2003 computer.
The three Exchange servers are named Certkiller NY, Certkiller CH, and Certkiller SE.
The relevant portion of the network is configured as shown in the exhibit.



Users report slow delivery of large e-mail messages between mailboxes on Certkiller NY and Certkiller SE.
You verify that all WAN links and servers are functioning properly.
Certkiller NY can resolve the name Certkiller SE by using DNS.
You run the tracert command to perform a test on Certkiller NY and obtain the following results.



```
C:\>tracert 131.107.30.10

Tracing route to 131.107.30.10
over [illegible]

  1    <10 ms    <10 ms    <10 ms  131.107.10.1
  2    110 ms    101 ms    110 ms  131.107.1.1
  3     90 ms    111 ms    100 ms  131.107.20.1
  4    100 ms     91 ms    110 ms  131.107.30.1
  5    100 ms    121 ms    150 ms  131.107.30.10

Trace complete.

C:\>_
```

You need to increase the speed of e-mail delivery between Certkiller NY and Certkiller SE.
What should you do?

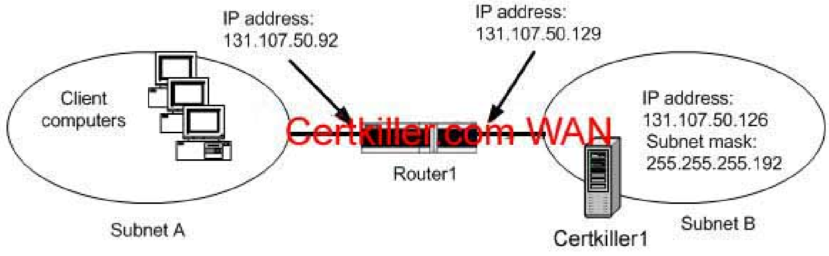
A. Create a routing group connector between the Chicago and Seattle routing groups.
B. Create an SMTP connector in the New York routing group. Specify the Seattle routing group on the Connected Routing Groups tab, and specify 131.107.30.10 as a smart host.
C. Request the ISP to remove the IP route to the 131.107.30.0 network on Router4 as the ISP.
D. Request the network administrator to create an IP route to the 131.107.30.0 network on Router1 in the New York subnet.
E. Increase the cost of the routing group connector between the New York and Chicago routing groups to 20.
F. Decrease the cost of the routing group connector between the New York and Seattle routing groups to 5.

Answer: D

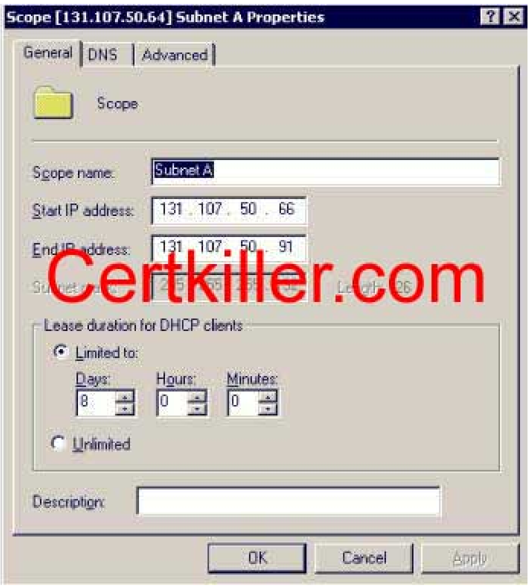
Explanation:
The main problem is that the routing from 131.107.10.1 is going through the much slower 131.107.1.1 interface before continuing to Seattle. An IP route explicitly stating the correct route for messages headed for Seattle should be created at the point where the message route is incorrect. In this case, it's 131.107.10.1.
Incorrect Answers:

A. Creating a routing group connector between Chicago and Seattle will not improve the situation. The routing Group connector between New York and Seattle is already in place. Adding another hop for the Exchange traffic to travel would not improve the situation.
B. Creating an SMTP connector in New York may cause a lot more traffic, as any SMTP traffic from New York would flow all the way to Seattle before being routed where it needs to go. In most cases, this would not be Seattle. Further, the route taken would still go through the slow links, as even though there is a routing group connector, it will still take the same physical route to the destination.
C. There is no route currently for the 131.107.30.0 network on that router. Therefore, this route can't be removed.
E. Increasing the cost of the routing group connector to 20 will not have any effect. According to the tracert, the problem is not that the mail is hitting the Chicago server before moving on. The problem is that it is hitting a 128K link between the ISP and its internal routers instead of taking the quicker internal routers only.
F. Decreasing the cost of the routing group connector between New York and Seattle will have no effect. The route being taken is not as direct as it needs to be for the messages to arrive as quickly as possible.

QUESTION 142
You are the Exchange administrator for Certkiller .
The network consists of two subnets.
The relevant portion of the network is configured as shown in the following diagram.



Subnet A contains 25 client computers that receive their TCP/IP configuration from a DHCP server.
Subnet A scope on the DHCP server is shown in the exhibit.



Scope [131.107.50.64] Subnet A Properties

Scope name: Subnet A

Start IP address: 131 . 107 . 50 . 66

End IP address: 131 . 107 . 50 . 91

Subnet mask: 255 . 255 . 255 . 192 Length: 26

Lease duration for DHCP clients

● Limited to:

Days: 8 Hours: 0 Minutes: 0

○ Unlimited

Description:

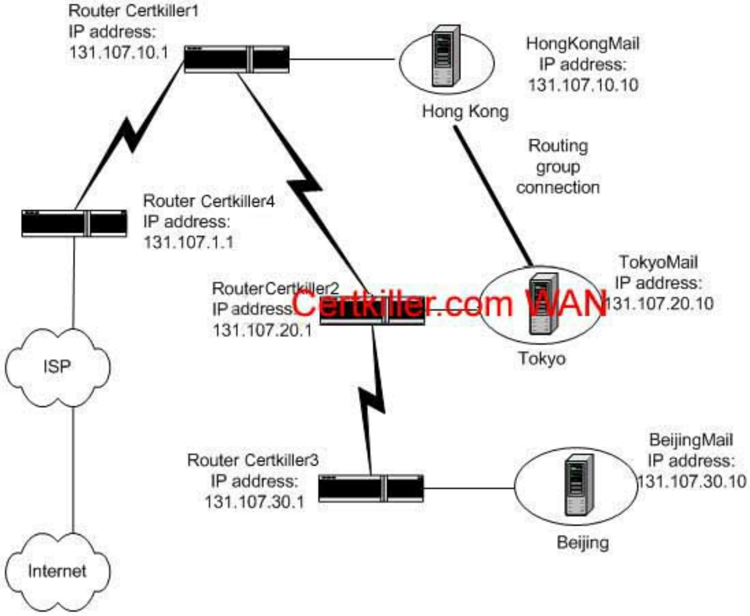
Subnet B contains only a single Exchange Server 2003 computer named Certkiller 1.
Users in subnet A report that they cannot connect to Certkiller 1.
You run the ping 131.107.50.126 command on a client computer in subnet A.
You receive the following error message: "Request times out".
You need to ensure that the client computers in subnet A can connect to Certkiller 1.
What should you do?

A. Change the IP address of Certkiller 1 to 131.107.50.130.
B. Change the subnet mask of Certkiller 1 to 255.255.255.224.
C. Change the IP address of the subnet A interface on Router1 to 131.107.50.65.
D. Change the subnet mask of the client computers in subnet A to 255.255.255.224.
E. Change the default gateway of the client computers in subnet A to 131.107.50.129.

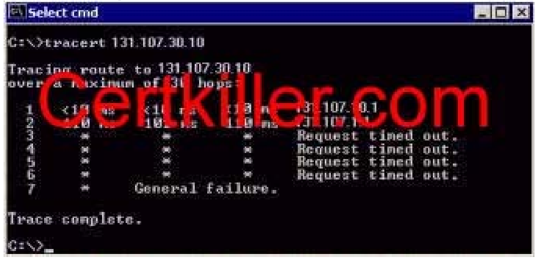
Answer: A
Explanation
Certkiller 1 should have the same network ID as the network card of the router in Subnet B. Currently, the DCHP
range is 131.107.50.66 to 131.107.50.91. The two servers' IP addresses and the two routers' IP addresses are outside of DHCP scope. This means that they have static IP addresses. Therefore we can manually change the IP address for Certkiller 1 to 131.107.50.107.
Incorrect Answers
B If we change the subnet mask to 255.255.255.224, we would only be able to support 30 hosts per subnet.
C IP is not in the correct range.
D If we change the subnet mask to 255.255.255.224, we would only be able to support 30 hosts per subnet.
E There is no need to change default gateway. Routing in correctly enabled.

QUESTION 143
You are the Exchange administrator for Certkiller . The Hong Kong and Tokyo offices each have a routing group that contains an Exchange Server 2003 computer. The two Exchange servers are named HongKongMail and TokyoMail.
You add a new office names Beijing to the network. The Beijing office has a routing group that contains

an Exchange Server 2003 computer named BeijingMail. The relevant portion of the network is configured as shown in the exhibit.



You test the connectivity from HongKongMail to BeijingMail by running the ping command, but you receive no response. You can ping TokyoMail from HongKongMail and you can ping TokyoMail from BeijingMail. You perform a test on HongKongMail by running the tracert command, and you receive the following result.



```
C:\>tracert 131.107.30.10

Tracing route to 131.107.30.10
over a maximum of 30 hops:

  1   <10 ms   <10 ms   <10 ms  131.107.10.1
  2   110 ms   101 ms   110 ms  131.107.1.1
  3     *        *        *     Request timed out.
  4     *        *        *     Request timed out.
  5     *        *        *     Request timed out.
  6     *        *        *     Request timed out.
  7     *     General failure.

Trace complete.

C:\>_
```

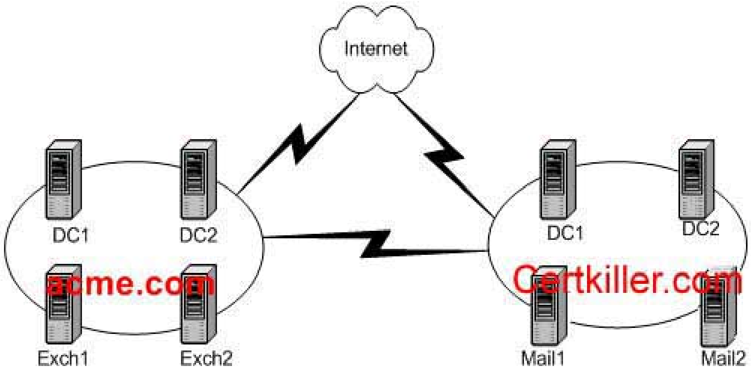
You need to enable network connectivity between HongKongMail and BeijingMail. All changes will be implemented by the network administrator.
Which action should you ask the network administrator to perform?

A. On HongKongMail, create a static IP route to 131.107.30.10.
B. On Router1, create an IP route to the 131.107.30.10.
C. On Router1, create an IP route to the 131.107.30.0 network.
D. On Router4, create an IP route to the 131.107.30.0 network.

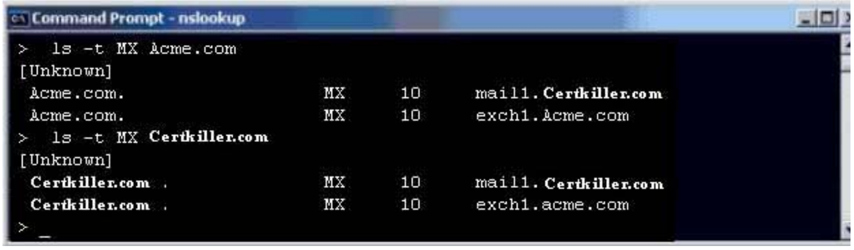
Answer: C
Explanation
The tracert command shows us that the first HOP IP address 131.107.10.1, whjich is the IP address for Router1, and the second Hop IP address 131.107.1.1, which the router connected to the Interent (Router4)
This indicates that router one does not have a default route to reach the Beijing network 137.107.30.x and BeijingMail Server IP 131.107.30.10.
In this case we need to add a route to the Beijing network on router1.

Reference
Basic Routing

QUESTION 144
You are the Exchange administrator for Acme. Certkiller has a business partnership with Certkiller .
The two companies share a single network and a single Exchange organization.
Each company has its own Active Directory domain named Certkiller .com.
The domains are named acme.com and Certkiller .com, respectively. Both domains are contained in a single forest.
The relevant portion of the network configuration is shown in the Network exhibit.



A new e-mail design document states the following requirements:
• All inbound Internet e-mail messages for acme.com must be delivered to Exch1.acme.com.
If this server is not available, the e-mail messages must be delivered to
Certkiller 1. Certkiller .com.
• All inbound Internet e-mail messages for Certkiller .com must be delivered to
Certkiller 1. Certkiller .com. If this server is not available, the e-mail messages must be delivered to Exch1.acme.com.
You discover that mail1. Certkiller .com and Exch1.acme.com receive equal numbers of Internet e-mail messages that are intended for acme.com. mail1. Certkiller .com and Exch1.acme.com also receive equal numbers of Internet e-mail messages that are intended for Certkiller .com.
You use the nslookup command to view the Internet mail exchanger (MX) resource records for the two domains. The output is shown in the Nslookup exhibit:



```
>  ls -t MX Acme.com
[Unknown]
 Acme.com.                    MX      10      mail1.Certkiller.com
 Acme.com.                    MX      10      exch1.Acme.com
>  ls -t MX Certkiller.com
[Unknown]
 Certkiller.com .             MX      10      mail1.Certkiller.com
 Certkiller.com .             MX      10      exch1.acme.com
> _
```

You need to ensure that the e-mail messages for each domain are delivered as stated in the e-mail design document.
Which two actions should you perform? (Each correct answer presents part of the solution. Choose two)

A. Set the priority for the Exch1.acme.com MX record in acme.com to 20.
B. Set the priority for the Exch1.acme.com MX record in Certkiller .com to 20.
C. Set the priority for the mail1. Certkiller .com MX record in acme.com to 20.

D. Set the priority for the mail1. Certkiller .com MX record in Certkiller .com to 20.
E. Remove the MX record for Exch1.acme.com from the Certkiller .com zone.
F. Remove the MX record for mail1. Certkiller .com from the acme.com zone.

Answer: B, C
Explanation
In this case with a MX cost of 10 mail will be routed to his domain until the connector fail and use the next on cost 20, this apply to both domains
Exchange 2003 provides load balancing in the form of a round-robin DNS between servers, both sources and targets. A round-robin DNS is a mechanism that directs incoming requests to servers on a rotating basis. This is done by looping through a list of IP addresses belonging to the servers in the configuration. When an e-mail client attempts to access a mailbox on an Exchange server, the client is given the first IP address on the list. The second client request is given the second IP address in the list, and so on. If there are four servers on the roundrobin
list, all four IP addresses are used before the first IP address is used again, and the loop starts over. In addition, Exchange 2003 offers improvements over the Exchange 5.5 Site Connector if one of the source bridgehead servers is down
Exchange connectors automatically try not to use that server until it comes back up. If there are multiple connectors with the same cost, each server picks a random connector and uses it for a period of time. Over multiple servers, this functionality simulates round-robin behavior.
Reference
Exchange server Resource Kit
Chapter 7 - Migrating Transports, Connectors, and Hubs

QUESTION 145
You are the Exchange administrator for Certkiller .
The network consists of a single Active Directory domain Certkiller .com that contains two domain controllers.
Each domain controller runs Microsoft Windows Server 2003 and is configured as a DNS server. Each DNS server is configured with root hints for resolving Internet host names.
The Exchange organization contains two servers that run Exchange Server 2003.
One Exchange server is configured with two network adapters and two SMTP virtual servers.
One SMTP virtual server is configured for internal e-mail, and the other is the bridgehead server for an SMTP connector that delivers all Internet e-mail messages.
The Internet SMTP virtual server is configured to use a DNS server at an ISP as an external DNS server.
The firewall configuration for Certkiller is modified to permit only domain controllers to make DNS queries to the Internet. Users report that they can no longer send e-mail messages to recipients on the Internet.
However, they can receive e-mail messages from the Internet.
You need to ensure that users can use the Internet to send and receive e-mail messages.
What should you do?

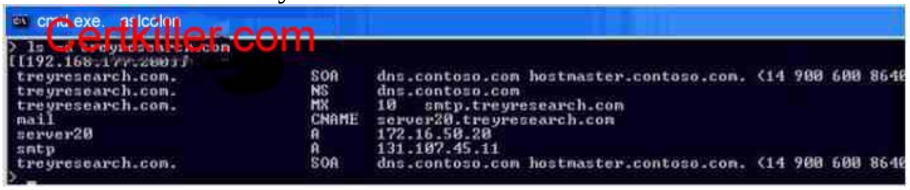
A. Reconfigure the network adapter used by the Internet SMTP virtual server to use the DNS server at the ISP.
B. Reconfigure the Internet SMTP virtual server to not use an external DNS server.
C. Configure the Internet SMTP virtual server to use a smart host to deliver e-mail messages.

Use the fully qualified domain name (FQDN) of an SMTP server managed by the ISP as the smart host.
D. Configure the SMTP connector to use a smart host to deliver e-mail messages.
Use the fully qualified domain name (FQDN) of an SMTP server managed by the ISP as the smart host.

Answer: D
Explanation
They already have Internet SMTP virtual server configured to use a DNS server at an ISP as an external DNS server. The problem is this case is DNS queries Each DNS server is configured with root hints for resolving Internet host names also the firewall configuration is modified to permit only domain controllers to make DNS queries to the Internet. Because in the ISP DNS they have a MX for the company domain, they can receive mail from Internet. But, in order send email, an SMTP connector for the domain must be able to resolve or forward DNS queries to external domain or in this case to forward DNS resolution to the ISP DNS server.
Incorrect answer

A. This network adapter is already configured to use a DNS server at an ISP as an external DNS server.
B. If you reconfigure the Internet SMTP virtual server to not use an external DNS server, the SMTP virtual servers will be unable to resolve the internet e-mail addresses.
C. When you use the Forward all mail through this connector to the following smart host option over a connector this option overwrite the Internet SMTP virtual server setting to use a smart host. You should use this option to route mail through a smart host that assumes responsibility for DNS name resolution and mail delivery.
Reference
Part 10 - Exchange Architecture
How to Configure the SMTP Connector in Exchange 265293

QUESTION 146
You are the Exchange administrator for Trey Research. The internal network is connected to the Internet through a Network Address Translation (NAT) router. The registered DNS zone named treyresearch.com is hosted at an external ISP named Contoso.com. Contoso.com used the DNS domain name contoso.com for network resources. Contoso.com manages the content of treyresearch.com zone.
The content of the treyresearch.com zone is shown in the exhibit.



```
> ls [illegible] treyresearch.com
[[192.168.177.200]]
 treyresearch.com.              SOA    dns.contoso.com hostmaster.contoso.com. (14 900 600 8640
 treyresearch.com.              NS     dns.contoso.com
 treyresearch.com.              MX     10   smtp.treyresearch.com
 mail                           CNAME  server20.treyresearch.com
 server20                       A      172.16.50.20
 smtp                           A      131.107.45.11
 treyresearch.com.              SOA    dns.contoso.com hostmaster.contoso.com. (14 900 600 8640
>
```

A computer named Server20 is the only computer in Trey Research that is accessible from the Internet. Server20 runs Exchange Server 2003 and is used as the bridgehead server for all SMTP traffic between the internal network and the Internet. Three other Exchange servers host user mailboxes.
Trey Research employs 50 technicians who work on site at customer locations. At the customer locations, the technicians connect to the Internet through a HTTP proxy only.
You want these technicians to access their mailboxes by using Microsoft Outlook Web Access, so you instruct them to connect to the URL http://mail.treyresearch.com/exchange.
The technicians report that they receive an error message when they attempt to connect to the URL from any computer at customer locations. However, the technicians can use the URL to connect successfully to Outlook Web Access when they are logged on to a computer on the internal network at the Trey Research location. There are no other problems relating to other messaging traffic between the internal

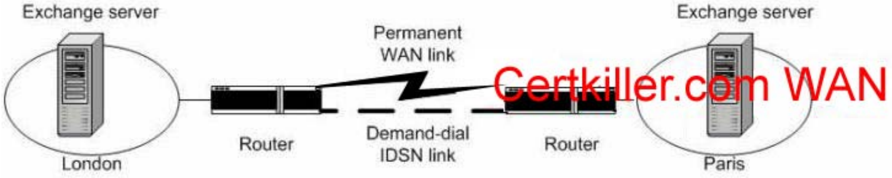
network and the Internet.
You need to enable the technicians to access their mailboxes from customer locations.
What should you do?

A. Instruct the technicians to use the URL http://smtp.treyresearch.com/exchange when they need to access their mailboxes.
B. Instruct the technicians to use the URL http://server20.treyresearch.com/exchange when they need to access their mailboxes.
C. Configure Routing and Remote Access on Server20. Instruct the technicians to make a VPN connection to Server20 when they need to access their mailboxes.
D. Configure the HTTP virtual server on Server20 to use TCP port 8080. Instruct the technicians to use the URL http://mail.treyresearch.com:8080/exchange when they need to access their mailboxes.

Answer: B

Explanation:
They show in the mail DNS mail a CName record for server20.treyresearch.com. CNAME is a dns alias for a record that point to another record that will be used for lookup service
TRICK: You will need to use Exchange 2000 SP2, or higher, there was a bug in previous versions, that do not permit to do this

QUESTION 147
You are the Exchange administrator for Certkiller . The relevant portion of the network is configured as shown the following diagram.



The network serves two offices, one in London and one in Paris. Each office contains a single Exchange Server 2003 computer in its own routing group. The routing groups are connected by a routing group connector.
The only network traffic between the two offices is e-mail messages. There is a permanent WAN link that connects the two offices. The WAN link is connected to a hardware router in each office. The two hardware routers each also have an ISDN dial-up interface. Demand-dial routing is defined between the two offices.
You view network utilization statistics in the Paris office, and you discover that traffic from the Paris Exchange server frequently causes the ISDN link to connect. There is little utilization of the permanent WAN link between the two offices. The WAN link has been very reliable and has suffered no downtime.
You need to ensure that the ISDN link is used only when the permanent WAN link fails.
What should you do in the Paris office?

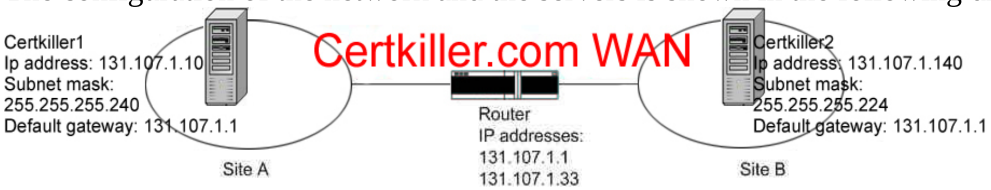
A. Request the network administrator to remove the IP route that uses the ISDN link from the routers.
B. Request the network administrator to reconfigure the routers, so that the IP route that uses the ISDN link is assigned a higher cost than the permanent WAN link.
C. Request the network administrator to reconfigure the routers, so that the IP route that uses the ISDN link

is assigned a lower cost than the permanent WAN link.
D. On the Exchange server, create a TCP/IP static route to the London Exchange server.
E. On the Exchange server, replace the routing group connector with an SMTP connector that uses the ETRN command.
F. On the Exchange server, replace the routing group connector with an SMTP connector that uses the London Exchange server as a smart host.

Answer: B

Explanation:
When you assign a higher cost to a route, that route will only be used if the primary line fails.

QUESTION 148
You are the Exchange administrator for Certkiller .
The network consists of two sites. Each site has its own IP subnet.
Each site contains a computer that runs Exchange Server 2003.
The two Exchange servers are named Certkiller 1 and Certkiller 2.
The configuration of the network and the servers is shown in the following diagram.



Users in each site have mailboxes on the Exchange server in their own site.
Users in site A report that they can connect successfully to Certkiller 1, but that e-mail sent to users in Site B is not delivered.
You test connectivity between the sites by using the ping command. When you attempt to ping Certkiller 1 from Certkiller 2, you receive the following error message: "Destination host unreachable".
You need to ensure that mail delivery occurs between the two Exchange servers.
What should you do?

A. Reconfigure the subnet mask on Certkiller 1 to be 255.255.255.224.
B. Reconfigure the default gateway address on Certkiller 1 to be 131.107.1.33.
C. Reconfigure the subnet mask on Certkiller 2 to be 255.255.255.240.
D. Reconfigure the default gateway address on Certkiller 2 to be 131.107.1.33.

Answer: D

Explanation:
Site A IP address 131.107.1.10 mask 255.255.255.240, their 3 first bytes are fixed
240 means in binary -> 1111.0000 (jump 24^16) router goes to 131.107.1.0-15, 131.107.1.16-31, 131.107.1.32-47, where 131.107.1.0-15 is own subnet in this segment the IP address 131.107.1.0 is the network address and IP address 131.107.1.15 is broadcast address, rest of IP are for HOST in this case exchange 131.107.1.10 and 131.107.1.1 router
Site B network address is 131.107.1.32 mask 255.255.255.240 go from 131.107.1.32 to 131.107.1.47 where 131.107.1.32 is the network address and 131.107.1.47 broadcast address the other IP are for host in this case 131.107.1.40 for exchange and 131.107.1.33 for router

QUESTION 149

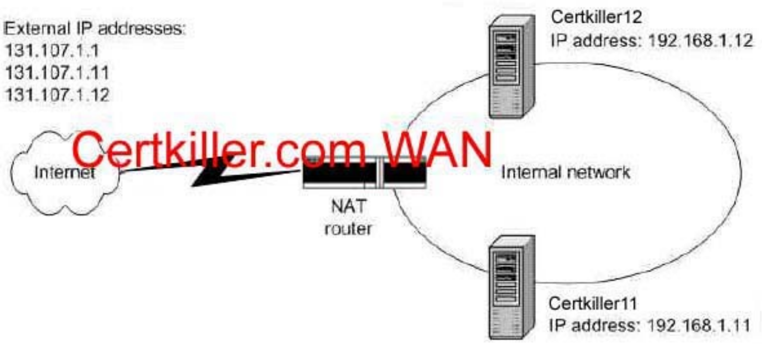
You are the Exchange administrator for Certkiller . The New York and Chicago offices each have a routing group that contains an Exchange Server 2003 computer.

The two Exchange servers are named NewYorkMail and ChicagoMail.

You add a new office named Seattle to the network.

The Seattle office has a routing group that contains an Exchange Server 2003 computer named SeattleMail.

The relevant portion of the network is configured as shown in the exhibit.



The internal network is accessible from the Internet only through a Network Address Translation (NAT) router.

The NAT router has filters that limit the types of network connections allowed onto the internal network.

The filters allow access by using all protocols that can be used for Exchange client computers to retrieve e-mail messages from mail servers on the internet network.

External IP address	**Internal IP address**	**Purpose**
131.107.1.1	None	External IP address of router
131.107.1.11	192.168.1.11	Makes Certkiller 11 accessible from Internet
131.107.1.12	192.168.1.12	Makes Certkiller 12 accessible from Internet

Users report that they cannot retrieve e-mail messages when connected remotely over the Internet.

They establish a VPN connection to Certkiller 11 and then attempt to connect to 131.107.1.1 by using their mail client.

They receive an error message stating that the server cannot be found.

You need to provide users with the correct IP address to configure when they user their mail client to retrieve e-mail messages on Certkiller 12 over the Internet.

Which IP address should users connect to after their VPN connection is established?

A. 131.107.1.11
B. 192.168.1.11

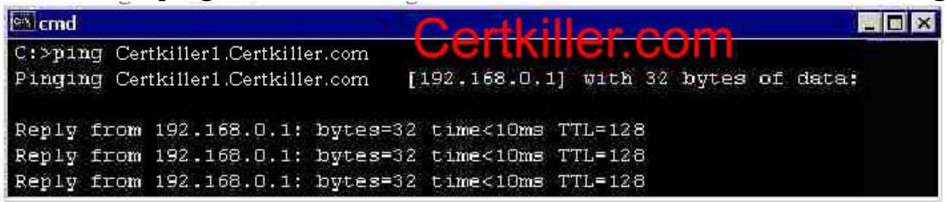
C. 131.107.1.12
D. 192.168.1.12

Answer: D
Explanation
They establish a VPN connection to Certkiller 11 that means they need access to 192.168.1.11, they then try to connect to 131.107.1.1 that means need to access the router they need to access to Certkiller 12 192.168.1.12
They give to us the solution in the table

131.107.1.12	192.168.1.12	Makes Certkiller 11 accessible from Internet

Nat translation for public IP 131.107.1.12 is internal 192.168.1.12 that is Certkiller 12 IP

QUESTION 150
You are the Exchange administrator for Certkiller .
The network consists of two Active Directory domains
• Certkiller .com
• manufacturing. Certkiller .com
The domain controllers in each domain are configured as DNS servers and host the DNS zone for their local domain name.
The DNS servers in each domain are configured to forward unresolved queries to DNS servers in the other domain.
All computers are configured to use a DNS server in their own domain as their preferred DNS server.
The Exchange organization consists of two Exchange sites named Certkiller and Manufacturing.
Each site contains an Exchange Server 5.5 computer running Microsoft Windows NT Server 4.0.
The Exchange server in the Certkiller site is named Nt Certkiller 1 and belongs to the Certkiller .com domain.
The Exchange server in the Manufacturing site is named Nt Certkiller 2 and belongs to the manufacturing. Certkiller .com domain.
You install a new Exchange Server 2003 computer named Certkiller 1 in the Certkiller site.
You make Certkiller 1 a member of the Certkiller .com domain.
You modify theX.400 connector between the Manufacturing site and the Certkiller site to use Certkiller 1 as the destination server for the connector.
You discover that test messages sent between the Manufacturing site and the Certkiller site are not delivered.
To test connectivity, you unsuccessfully attempt to connect to the URL http:// Certkiller 1/exchange from Nt Certkiller 2.
You run the ping command from Nt Certkiller 2 and receive the following results.



```
C:>ping Certkiller1.Certkiller.com
Pinging Certkiller1.Certkiller.com    [192.168.0.1] with 32 bytes of data:

Reply from 192.168.0.1: bytes=32 time<10ms TTL=128
Reply from 192.168.0.1: bytes=32 time<10ms TTL=128
Reply from 192.168.0.1: bytes=32 time<10ms TTL=128
```

You need to ensure that Nt Certkiller 2 can consistently connect to Certkiller 1.

What should you do?

A. Configure the DNS servers that host the manufacturing. Certkiller .com zone to perform conditional forwarding of all queries for hosts in the Certkiller .com zone.
B. Configure the DNS servers that host the manufacturing. Certkiller .com zone to host a secondary zone for Certkiller .com.
C. Configure Nt Certkiller 2 to use a DNS server in the Certkiller .com domain as an alternate DNS server.
D. Configure the DNS settings on Nt Certkiller 2 to append the DNS suffixes manufacturing. Certkiller .com and Certkiller .com to all host name queries.

Answer: A

Explanation:
Rather than having a DNS server forward all queries it cannot resolve to forwarders, the DNS server can forward queries for different domain names to different DNS servers according to the specific domain names that are contained in the queries. Forwarding according to these domain-name conditions improves conventional forwarding by adding a second condition to the forwarding process.
A conditional forwarder setting consists of a domain name and the IP address of one or more DNS servers. To configure a DNS server for conditional forwarding, a list of domain names is set up on the Windows Server 2003-based DNS server along with the DNS server IP address. When a DNS client or server performs a query operation against a Windows Server 2003-based DNS server that is configured for forwarding, the DNS server looks to see if the query can be resolved by using its own zone data or the zone data that is stored in its cache, and then, if the DNS server is configured to forward for the domain name that is designated in the query (a match), the query is forwarded to the IP address of a DNS Server that is associated with the domain name. If the DNS server has no domain name listed for the name that is designated in the query, it attempts to resolve the query by using standard recursion.
Reference
Conditional Forwarding in Windows Server 2003 304491