Implementing and Managing Microsoft Exchange Server 2003

70-284

This is a demo of the original study guide that consists of 11 numbers of questions and answers with explanation.

Question 1.
You are the exchange administrator of your organization. You are going to upgrade your messaging infrastructure from Microsoft Exchange serve 2000 to Microsoft Exchange server 2003. Your upgrade planning also includes the migrations from Microsoft Windows 2000 server family to Microsoft Windows 2003 server family.

What are the minimum requirements to accomplish these tasks? (Choose all that apply).

A. Domain Controllers of Windows 2000 should be running with minimum of service pack 2.
B. Domain Controllers of Windows 2000 should be running with minimum service pack 3.
C. First, upgrade your Exchange server 2000 to Exchange server 2003 then Windows 2000 server to Windows 2003 server.
D. First, upgrade your Windows 2000 server to Windows 2003 server and then Exchange server 2000 to Exchange server 2003.
E. For front end back end configuration, upgrade your front end servers first.
F. For front end back end configuration, upgrade your back-end servers first.

Answer: B, C, E

Explanation:
Before you upgrade to Exchange Server 2003, make sure that your network and your servers meet the following system-wide requirements:

Domain controllers are running Microsoft Windows 2000 Server Service Pack 3 (SP3) and later, or Microsoft Windows Server 2003.

In a situation where you run Exchange 2000 on a Windows 2000-based computer and you want to upgrade the operating system to Windows Server 2003, you must first upgrade Exchange 2000 to Exchange 2003. You can then upgrade Windows 2000 to Windows Server 2003.

For front-end and back-end servers that are in the same administrative group, you must upgrade the front-end servers to Exchange 2003 (or install Exchange 2003 on the front-end server) before you upgrade the back-end server to Exchange 2003 (or install Exchange 2003 on the back-end server).

Question 2.
You are the Exchange administrator for ITCertKeys. 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: B

Explanation:
The answer B and C are right but because they tell us in the product admin guide You can have Exchange format these messages in either MIME or uuencode, so that non-MAPI clients can read these messages I just select MIME as correct, or this question can be one of those that have two valid answers according MS exams FAQ
Formatting and Automatic Responses

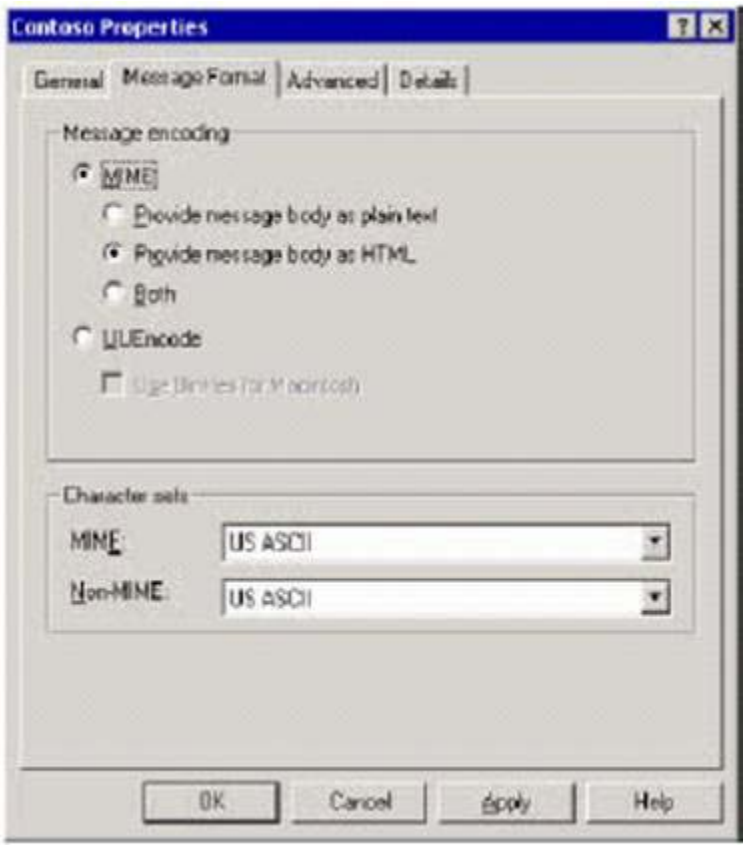
You can use Internet message formats to define SMTP policies that control the format of messages that are sent to the Internet, or to specific external SMTP domains. These policies also control what types of automatic responses, such as out-of-office notifications, can be sent to Internet domains from users in your organization.

For each domain that is defined in Internet Message Formats, you can set the following properties: Message formatting options that determine how messages sent to this domain are encoded, and which language character set is used to display these messages.

Advanced options that determine when messages are sent in Exchange RTF, how text is formatted, and what types of automatic responses, such as non-delivery reports (NDRs) or out-of-office notifications, are sent to this domain.

Important
Do not send mail exclusively in RTF because many non-Microsoft mail servers cannot read rich-text messages.
Servers that cannot read rich-text messages provide their users with e-mail messages that include a Winmail.dat file attachment. To avoid this problem, ensure that your message settings do not use Exchange RTF exclusively.

You can control how Exchange formats the messages that are sent to the domain or domains on a particular policy. You can have Exchange format these messages in either MIME or uuencode, so that non-MAPI clients can read these messages. Additionally, you can specify the character set that Exchange uses for outgoing messages. By default, all messages use the Western European (ISO-8859-1) character set.



Reference:
Exchange Server 2003 Administration Guide

Question 3.
You are the Exchange administrator for ITCertKeys. 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.

External customers now report that they cannot send e-mail to ITCertKeys 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 verify SMTP virtual server is configured to allow anonymous access In Exchange System Manager, in the Properties dialog box of the SMTP virtual server, on the Access tab, click Authentication.

In the Authentication dialog box (see Figure 5.15), select the Anonymous access check box (if it is not already selected).

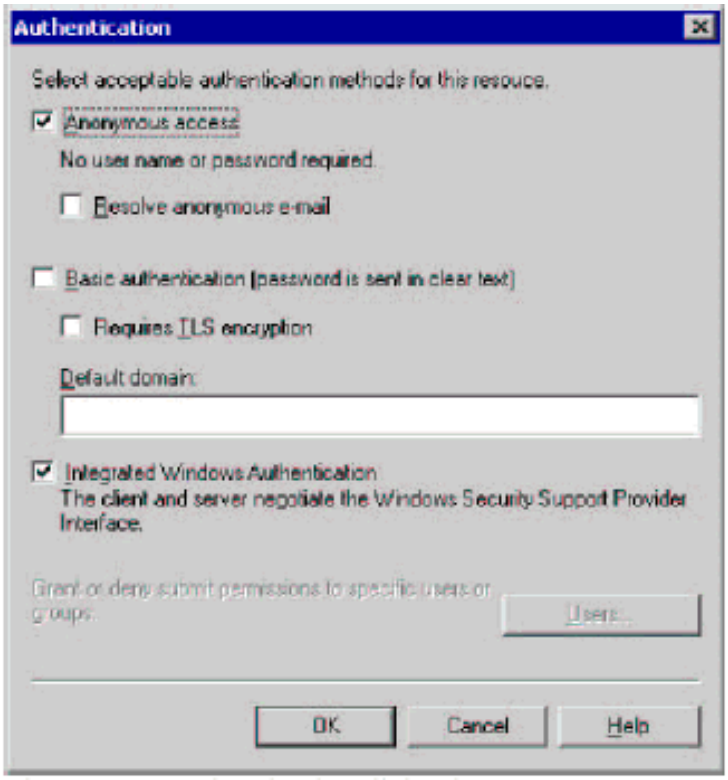


Figure 5.15 Authentication dialog box

To permit use the SMTP connector to external users you need to permit anonymous user access to SMTP connector, just to avoid relay To verify that your SMTP virtual server is not set to open relay In Exchange System Manager, in the Properties dialog box of the SMTP virtual server, on the Access tab, click Relay.

In the Relay Restrictions dialog box (see Figure 5.16), select Only the list below (if it is not already selected), click Add, and follow the instructions to add only those hosts that you want to allow to relay mail to the list.

Note:

If you select All except the list below, your server may be used by unauthorized users to distribute unsolicited email messages on the Internet.

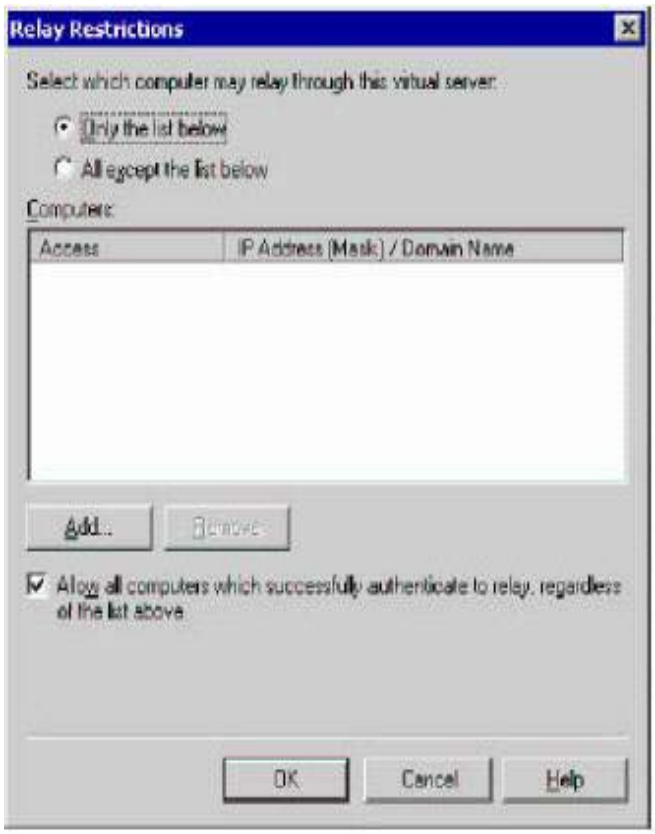


Figure 5.16 Relay Restrictions dialog box
Select Allow all computers which successfully authenticate to relay, regardless of the list above (if it is not already selected).

This setting allows you to deny relay permissions to all users who do not authenticate. Any remote Internet Message Access Protocol version 4 (IMAP4) and Post Office Protocol version 3 (POP3) users who access this server will authenticate to send mail. If you do not have users who access this server through IMAP4 or POP3, you can clear this check box to prevent relaying entirely, thereby increasing security. You can also designate a specific server for IMAP4 and POP3 users, and then clear this check box on all other Internet gateway servers.

Reference:
Exchange Server 2003 Administration Guide

Question 4.
You are the Exchange administrator for your company. 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:
A. Enabling forms based authentication on the SMTP virtual server is required, as this is what will allow the form to be displayed when the user attempts to connect to the OWA server.
B is also required. Attempting to enable Forms Based Authentication will result in the following dialog box:

To enable forms based authentication for Outlook Web Access:

1. Start System Manager: On the Start menu, point to Programs, point to Microsoft Exchange, and then click System Manager. You can manually start the application by following these instructions: On the Start menu, point to Programs, point to Microsoft Exchange, and then click System Manager.
2. Navigate to HTTP. Servers
1. Server
2. Protocols
3. HTTP
3. Right-click a virtual server, and then click Properties.
4. On the Settings tab, in the Outlook Web Access pane, select Enable Forms Based Authentication, and then click OK.

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 anything on the back end server is not helpful. Since all the external clients use the front end servers to communicate, no outside user would ever 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, it will not be explicitly required.

Reference:
Exchange Server 2003 Administration Guide
What's New in Exchange 2003 Exchange Server 2003 Product Help

Question 5.
You are the Exchange administrator for ITCertKeys. The network consists of a single Active Directory domain ITCertKeys.com. All users use Microsoft Outlook and Outlook Web Access to send and receive email.-

ITCertKeys 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 e-mail. 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 permissions 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 concentrator, create a mail-enabled Contract 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 and put their mail address to forward the mail to the mail contact - This explanation is correct, but the correct answer to match this explanation is "B", not "A". A mail-enabled contact, not a mail-enabled user object needs to be created in order to prevent the contractors from having any rights in the organization. contact An Active Directory object that represents a user who is outside of the Exchange organization. For example, a contact may represent a user at another company. A contact in Windows Server 2003 or Windows 2000 is equivalent to a custom recipient in Exchange 5.5 and earlier version.

(Not needed for a complete, accurate description of the answer.)mail-enabled An Active Directory object that has at least one e-mail address defined. If the user is mail-enabled, the user has an associated e-mail address, but does not have an associated Exchange mailbox.

Question 6.
You are the Exchange administrator for ITCertKeys. 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 /disaster recovery command to reinstall Exchange Server 2003 on the active node.

Answer: C

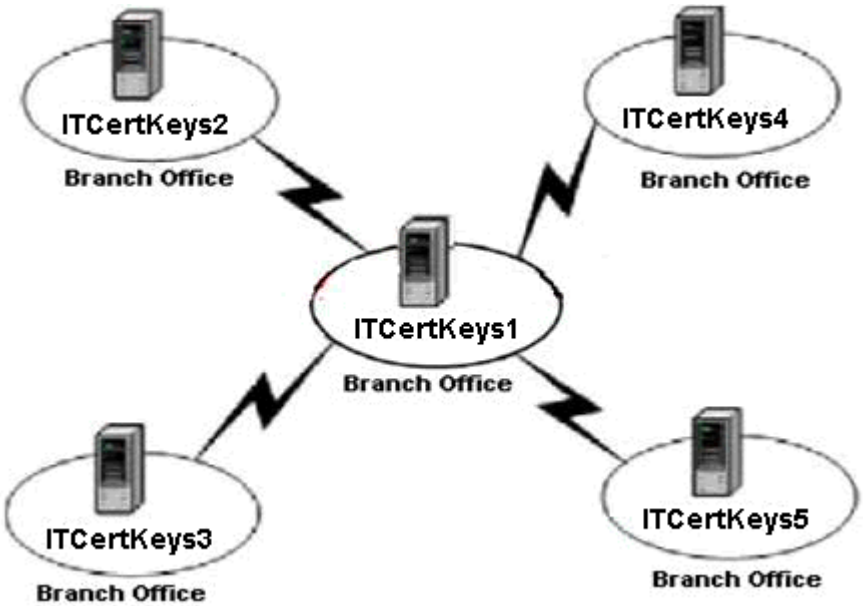
Explanation:
They just tell use that Exchange has been installed in a Cluster but to permit an active passive configuration they need to perform additional task as Create a new cluster resource group for the Exchange server and create a System Attendant resource for the active/passive configuration.
Customizing Your Exchange Cluster Configuration When you deploy Exchange Server 2003 in a cluster, you must accept many default settings. For instance, your Exchange cluster consists of Exchange Virtual Servers that are created using the New Group Wizard. However, this wizard does not allow you to configure all of the possible failover options for your Exchange Virtual Servers. Similarly, the New Resource Wizard, which creates an Exchange System Attendant resource for your Exchange Virtual Server, automatically creates the remaining Exchange resources, like the Exchange store and the MTA, using the default settings for each of these additional resources.

Because initial cluster deployment usually involves so many default settings, you may need to customize your cluster configuration settings. This customization is important not only to achieve your cluster objectives, but also to achieve optimal cluster performance. Improper cluster configuration is the source of many of the Exchange-related issues handled by Microsoft Product Support Services. For this reason, carefully follow the recommendations in this chapter to ensure your clusters perform optimally.

Configuring Exchange Virtual Server Settings
When you create your Exchange Virtual Servers, the default properties that are applied at that time should allow your Exchange cluster to operate adequately. However, you may want to modify these settings to customize your clusters to accommodate your specific Exchange environment.

To change the configuration settings for an Exchange Virtual Server, you use the property settings associated with that Exchange Virtual Server object. These property settings instruct Cluster Service in how to manage your Exchange Virtual Servers.

Question 7.
You are the Exchange administrator for ITCertKeys. The network consists of a single Active Directory domain ITCertKeys.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 ITCertKeys1 through ITCertKeys5.

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 ITCertKeys1, 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 ITCertKeys1 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 ITCertKeys1.
D. On the new server in each branch office, install Exchange by running setup /choosedc and specify the local global catalog server.

Answer: C

Explanation:
They tell us that the schedule can not been modified or forced, Exchange server 2003 installation need to lookup for the CG attributes for Exchange, the new server site can not been installed until the replication occur, but they can use the new Exchange Server 2003 switch /Choose DC and select ITCertKeys1 as the GC to successfully install Exchange, Exchange Server 2003 includes a new switch that is supported by the Exchange 2003 Setup program. This switch is named the /choose DC switch, and you can use it 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 /choose DC switch in combination with other Exchange 2003 Setup switches, including /domainprep.

Reference:
Description of the /Choose DC Switch in Exchange Server 2003 822593
Setup Options for Exchange Server 2003 822893

Question 8.
You are the Exchange administrator for ITCertKeys. The company's network consists of a single Active Directory domain.

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:
In-place upgrade from Exchange Server 5.5 to Exchange 2003 is not supported. Because they ask to us for an in place upgrade they must first to do an upgrade to Exchange 2000 and from Exchange 2000 to Exchange 2003. They do not tell use if the ADC is running or not, for this reason I do not consider answer a, although is a required step to upgrade ADC to Exchange 2003, they ask to us for in place upgrade.

Exchange 5.5 to Exchange 2000 In-Place Upgrade Method
With the in-placed upgrade method, you can take an existing Exchange Server 5.5 SP3 or SP4 server and install Exchange 2000 Server on it. In this way, you upgrade your existing Exchange Server databases and connectors to Exchange 2000 Server. When you use this method, you must perform all prerequisites and testing for the installation of Exchange 2000 Server.

You must upgrade Active Directory Connectors (ADCs) to the version of ADC that is included in Exchange 2003 before you can install the first Exchange 2003 computer in your organization. The installation of the first Exchange 2003 ADC increments all connection agreement version numbers that are hosted on the server.

They do not offer to use this answer
To upgrade from Exchange Server 5.5 to Exchange Server 2003, you must join an Exchange 2003 computer to the Exchange 5.5 site, and then move Exchange resources such as mailboxes to the Exchange 2003 computer. Use the Exchange Server Deployment Tools to migrate from Exchange 5.5 to Exchange 2003. Although Exchange 2000 did support in-place upgrades from Exchange 5.5, moving the resources from Exchange 5.5 to Exchange 2000 is still the recommended upgrade path.

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 9.
You are the Exchange administrator for ITCertKeys. 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 ITCertKeys1 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:
They have the Exchange on Windows 2000 they need ensure that all users have personal digital encryption certificates issued by a commercial certification authority (CA).They can configure external PKI certificates for each user mapped to each user account in this way they can use outlook or OWA to encrypt mail in this case
answer A is valid.

Incorrect Answers:
Answer B is incorrect
OWA with S/MIME Support
The requirements for using OWA with S/MIME support include the following:
. Server The server must be running Exchange Server 2003.
. Client
o The client must be running Windows 2000 or later and Internet Explorer
6.0 Service Pack 1 (SP1) or later.
o The client must have a smart card or a local certificate.
Exchange and Outlook now support the use of the Windows RPC over HTTP feature, allowing Outlook 2003 clients to connect directly to the internal network using HTTPS or HTTP. For more information about configuring RPC over HTTP, see "Configuring Exchange Server 2003 for Client Access," in the book Exchange Server 2003 Deployment Guide (http://www.microsoft.com/exchange/library).

RPC Over HTTP Support in Outlook 2003 Exchange Server 2003 on Windows Server 2003 enables Outlook 2003 users to use RPC over HTTP. Outlook 2003 clients can connect over the Internet to the corporate messaging system. The requirements for RPC over HTTP include the following:

NOTE: Upgrade and Installation: Exchange Server 2003 Requirements
You can run Exchange Server 2003 on the following operating systems:
. Windows Server 2003
. Windows 2000 Server Service Pack 3 (SP3) and later
If your environment contains Windows 2000 domain controllers and global catalog servers, the domain controllers and the global catalog servers that Exchange Server 2003 uses must be running either Windows 2000 SP3 or Windows Server.

Answer C is incorrect
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 built-in features of Outlook and OWA 2003 will accomplish the task with no changes. Therefore, this is not the best answer.
Answer D is incorrect
They do not need to configure POP because this mean a protocol change and they state You must achieve this goal by making the minimum number of changes to the protocols allowed into the intranet from the Internet.

Reference:
Microsoft knowledge base articles
822178 Overview of Dependencies and Requirements for Exchange Server 2003 Features
RPC Over HTTP Support in Outlook 2003
331320 Outlook 11 Performs Slowly or Stops Responding When Connected to Exchange Server 2003 Through HTTP
Overview of Dependencies and Requirements for Exchange Server 2003 Features 822178
Exchange Server 2003 Administration Guide

Question 10.
You are the exchange admin of your company. Your company is running Microsoft exchange server 5.5. You are going to upgrade your exchange server 5.5 to exchange server 2003. Use the basic steps from the left side and arrange them order wise on the right side. Use only the basic steps that are necessary.

Select from Here	Place Here
Upgrade Exchange server 5.5 to exchange server 2000	
Upgrade Exchange server 5.5 to exchange server 2003	
Use exchange server deployment tool to migrate from Exchange 5.5 to Exchange 2003	
Join an Exchange 2003 computer to the Exchange 5.5 site	

Answer:

Select from Here	Place Here
Upgrade Exchange server 5.5 to exchange server 2000	Join an Exchange 2003 computer to the Exchange 5.5 site
Upgrade Exchange server 5.5 to exchange server 2003	Use exchange server deployment tool to migrate from Exchange 5.5 to Exchange 2003

Explanation:
To upgrade from Exchange Server 5.5 to Exchange Server 2003, you must join an Exchange 2003 computer to the Exchange 5.5 site, and then move Exchange resources such as mailboxes to the Exchange 2003 computer. Use the Exchange Server Deployment Tools to migrate from Exchange 5.5 to Exchange 2003. Although Exchange 2000 did support in-place upgrades from Exchange 5.5, moving the resources from Exchange 5.5 to Exchange 2000 is still the recommended upgrade path.

Question 11.

You have installed exchange server 2003 on a Windows 2003 enterprise edition. After installing the Exchange server 2003,

When you try to log on to Outlook Web Access (OWA), you may be prompted for credentials three times, and then you may receive the following error message:

You are not authorized to view this page You do not have permission to view this directory or page using the credentials you supplied.

HTTP 401.1 - Unauthorized: Logon Failed
Internet Information Services

Which of the following steps can be taken to resolve this issue? (Choose all that apply).

A. Re-install the exchange server 2003.
B. Verify Exchange Virtual Directory Settings.
C. Verify Default Web Site Properties.
D. Verify Exchange Recipient Policy.
E. Verify the ADC setting.
F. Verify Connection objects settings.

Answer: B, C, D

Explanation:
You should follow these steps to resolve this error message shown in the questions.
To resolve this issue, follow these steps.

Step 1: Verify Exchange Virtual Directory Settings

1. Start Exchange System Manager. To do this, click **Start**, point to **Programs**, point to **Microsoft Exchange**, and then click **System Manager**.
2. Expand **Servers**, expand ***ServerName***, expand **Protocols**, expand **HTTP**, and then expand **Exchange Virtual Server**.
3. Under **Exchange Virtual Server**, right-click the **Exchange** virtual directory, and then click **Properties**.

   Important Make sure to verify Domain Name System (DNS) settings and to verify the e-mail domain of the user who is experiencing this issue. If the e-mail domain is set incorrectly, you can resolve this problem by setting the e-mail domain correctly.
4. Click the **Access** tab, and then click **Authentication**.
5. Click to select the **Basic authentication** check box, if it is not already selected.
6. In the **Default domain** box, type \ (the backslash character), if it is not already present.
7. Click **OK**, click **OK** again, and then quit the Exchange System Manager snap-in.

Step 2: Verify Default Web Site Properties

1. Expand **Default Web Site**, right-click the **Exchange** virtual directory, and then click **Properties**.
2. On the **Virtual Directory** tab, verify that the **Local Path** box points to the M drive, and then make a note of the path.

3. Verify that the **Application name** box contains the **Exchange** virtual directory application.

   NOTE: When a valid application is displayed in this box, the **Create** button is not displayed. Instead, a **Remove** button is displayed next to the **Application name** box. If a **Create** button is displayed next to the **Application name** box, click it. **Exchange** then appears in the **Application name** box.
4. Click the **Directory Security** tab, and then click the **Edit** button under **Anonymous access and authentication control**.
5. Click to select the **Basic authentication (password is sent in clear text)** check box, if it is not already selected.
6. Under **Authenticated access**, click the **Edit** button.
7. In the **Domain Name** box, type \ (backslash character) if it is not already displayed.
8. Click **OK**, click **OK**, click **OK**, and then quit the Internet Information Services snap-in.

Step 3: Verify Exchange Recipient Policy

1. Start Exchange System Manager.
2. Expand **Recipients**, and then click **Recipient Policies**.
3. In the right pane of the Exchange System Manager window, view the **Properties** pages of the recipient policies to determine if an SMTP address that corresponds to the folder in the M drive (which you noted earlier in step 6 of "Verify Default Web Site Properties") is listed on the **E-Mail Addresses (Policy)** tab.
4. In the left pane of the Exchange System Manager window, click **Recipient Update Services** under **Recipients**.
5. In the right pane, right-click **Recipient Update Service (*Enterprise* Configuration)**, and then click **Rebuild**. Click **Yes** to confirm this operation.
6. Right-click **Recipient Update Service (*Enterprise* Configuration)**, and then click **Update Now**.
7. Right-click **Recipient Update Service (*DomainName.com*)**, and then click **Rebuild**. Click **Yes** to confirm this operation.
8. Right-click **Recipient Update Service (*DomainName.com*)**, and then click **Update Now**.
9. Quit the Exchange System Manager snap-in.
10. Wait for a few minutes to allow the Rebuild operation and the Update operation to complete, and then test Outlook Web Access (OWA) from a client computer.