



70-284

(Installing, Configuring, and Administering Microsoft Exchange 2003 Server)

Document version: 9.30.06

Important Note, Please Read Carefully

techeXams' 70-284 Exam is a comprehensive compilation of questions and answers that have been developed by our team of certified professionals. In order to prepare for the actual exam, all you need is to study the content of this exam questions. An average of approximately 10 to 15 hours should be spent to study these exam questions and you will surely pass your exam. It's our guarantee.

Latest Version

We are constantly reviewing our products. New material is added and old material is revised. Free updates are available for 90 days after the purchase. You should check your member zone at techeXams and update 3-4 days before the scheduled exam date. Here is the procedure to get the latest version:

1. Go to <http://www.techeXams.ws/>
2. Log in the User Center
3. The latest versions of all purchased products are downloadable from here. Just click the links.

Feedback

If you find any possible improvement, then please do let us know. We are always interested in improving the quality of this product. Feedback can be send at: **customer.service@techeXams.ws**

Explanations

This product does not include explanations for all questions at the moment. If you are interested in providing explanations for this exam, please contact **customer.service@techeXams.ws**.

Copyright

techeXams holds the copyright of this material. techeXams grants you a limited license to view and study this material, either for personal or commercial use. Unauthorized reproduction or distribution of this material, or any portion thereof, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.

Disclaimer

Neither this guide nor any material in this guide is sponsored, endorsed or affiliated with any of the respective vendor. All trademarks are properties of their respective owners.

A.	Installing, Configuring, and Troubleshooting Exchange Server 2003
B.	Managing, Monitoring, and Troubleshooting Exchange Server Computers
C.	Managing, Monitoring, and Troubleshooting the Exchange Organization
D.	Managing Security in the Exchange Environment
E.	Managing Recipient Objects and Address Lists
F.	Managing and Monitoring Technologies that Support Exchange Server 2003

Objectives of exam 70-284

Question: 1.

You are the Exchange administrator for Company. 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 Company1 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 servers can send and receive messages to and from the Internet.

Answer: A

Explanation:

Exchange exists on Windows 2000, and 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. This way users can utilize Outlook or OWA to encrypt and answer A is valid.

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 built-in 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: 2.

You are the Exchange administrator for Company. 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 re0.....mains 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: 3.

You are the Exchange administrator for Company. 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 Company 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: 4.

You are the Exchange administrator for 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**

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 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 Company. The network consists of a single Active Directory domain Company.com. All users use Microsoft Outlook and Outlook Web Access to send and receive e-mail.

Company 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 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: 6.

You are the Exchange administrator for Company. 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.

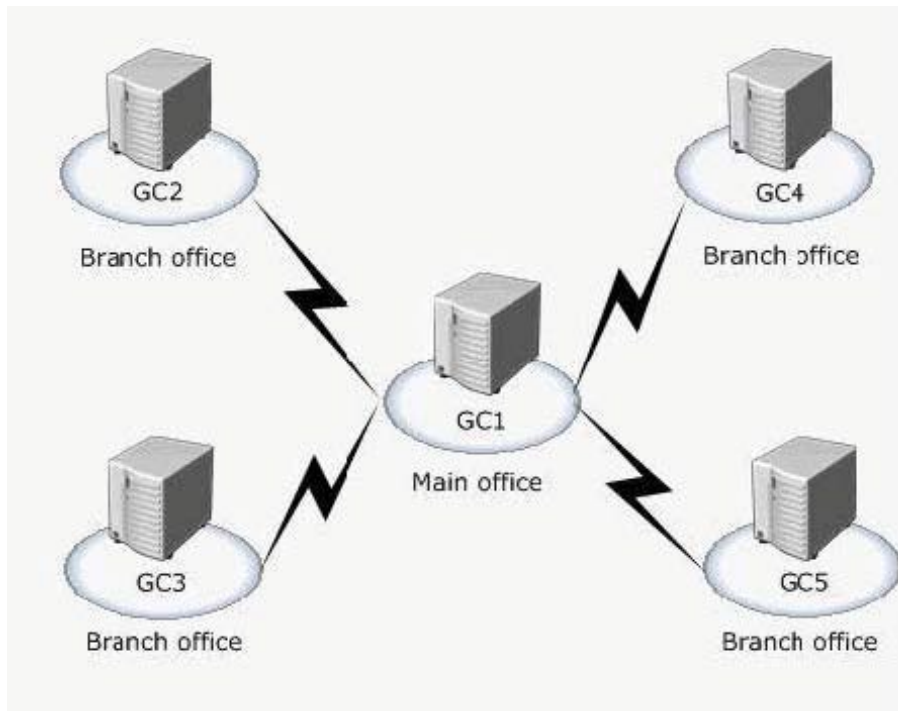
Answer: C

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: 7

You are the Exchange administrator for your company. The network consists of a single Active Directory domain. 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 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 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 in 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 of the business day. What should you do?

- A. First configure the new server in each branch office to point to GC1 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 GC1.
- 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:

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 Company1 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: 8.

You are the Exchange administrator for Company. The company's network consists of a single Active Directory domain named Company.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 Server 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.

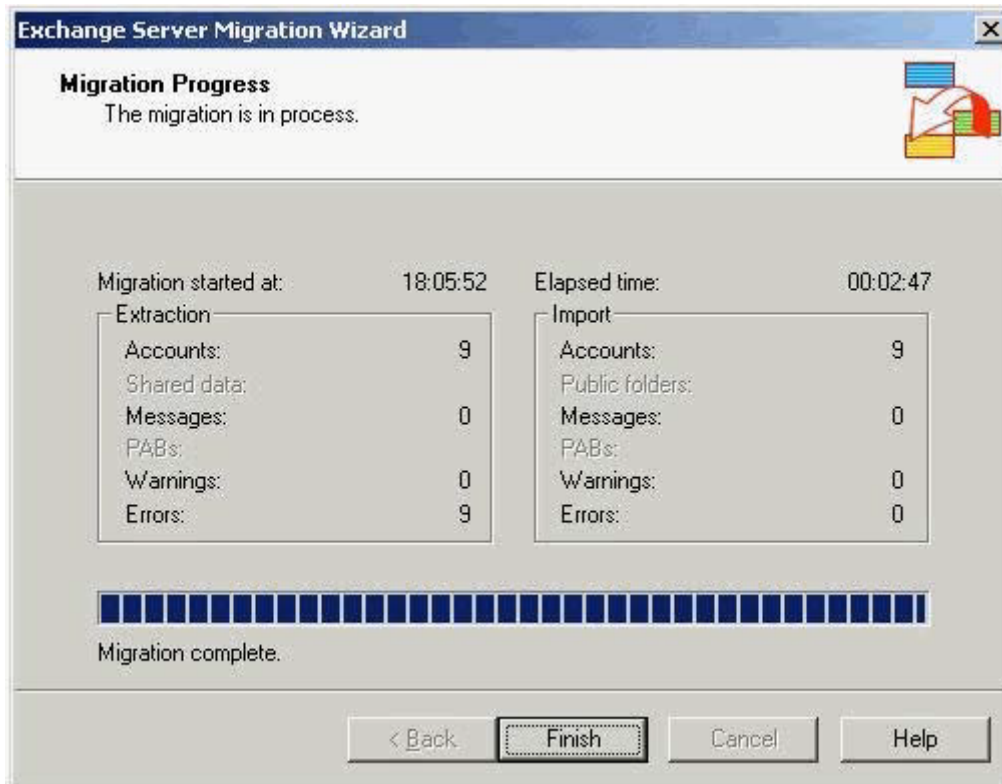
Reference:

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 Company. The network consists of a single Active Directory domain Company.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 Company1. 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.



You verify that the Active Directory user accounts for the IMAP4 users have Exchange mailboxes on Company1. 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 Company1 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 Company1 to the new account. Use the new account to log on to Company1 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 stand-alone application that is installed on your computer during Exchange setup. 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 an 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: 10.

You are the Exchange administrator for Company. 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 search 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: 11.

You are the Exchange administrator for Company. 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: 12.

You are the Exchange administrator for Company3. The Exchange organization contains a single server named Company3. Company3 runs Exchange Server 2003 and hosts all user mailboxes.

Company3 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 Company3.

One afternoon, users report extremely slow response times on Company3. Some users cannot access the server at all. You examine network traffic to Company3 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 Company3. You must minimize the effect of your actions on internal e-mail users.

What should you do?

- A. Stop the SMTP service on Company3.
- B. Reconfigure Company3 to prohibit all POP3 and IMAP connections.
- C. Reconfigure the firewall to prohibit all incoming SMTP traffic.
- D. Reconfigure Company3 to accept only POP3 connections. Instruct users to access Company3 by using POP3 client software.
- E. Configure TCP/IP filtering on Company3 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.

Incorrect answers:

- A. Stopping the SMTP service will also shut down all the internal mail, which violates the last requirement of the exam.
- B. Prohibiting IMAP and POP3 connections will not prevent the incoming SMTP traffic (which 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: 13.

You are the Exchange administrator for Company. The network consists of a single Active Directory domain Company.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 Sara reports that she can no longer access any network files and that her mailbox is not functioning. Other users report that they cannot find Sara's name in the global address list (GAL). You discover that Sara's Active Directory account was deleted 20 minutes ago. You recreate Sara's accounts in Active Directory.

You need to ensure that Sara has access to her most current e-mail message. Your solution must result in the least amount of mailbox downtime for Sara.

What should you do?

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

- B. Create a new mailbox for Sara. Restore the Exchange database to the Recovery Storage Group. Mount the mailbox store. Use Exmerge to merge Sara's old mailbox data into her new mailbox.
- C. Set up a recovery mailbox server. Restore the Exchange database. Use Exmerge to extract Sara's mailbox to a .pst file. Deliver this .pst file to Sara.
- D. Run the Cleanup Agent. Use Mailbox Recovery Center to reconnect Sara's mailbox to her newly created account.

Answer: D

Explanation:

By default Exchange keep any mailbox deleted seven days, to recover a single mailbox to recover a single mailbox you just need to recreate a deleted USER ACCOUNT, run the cleanup agent and reconnect the mailbox to the new account.

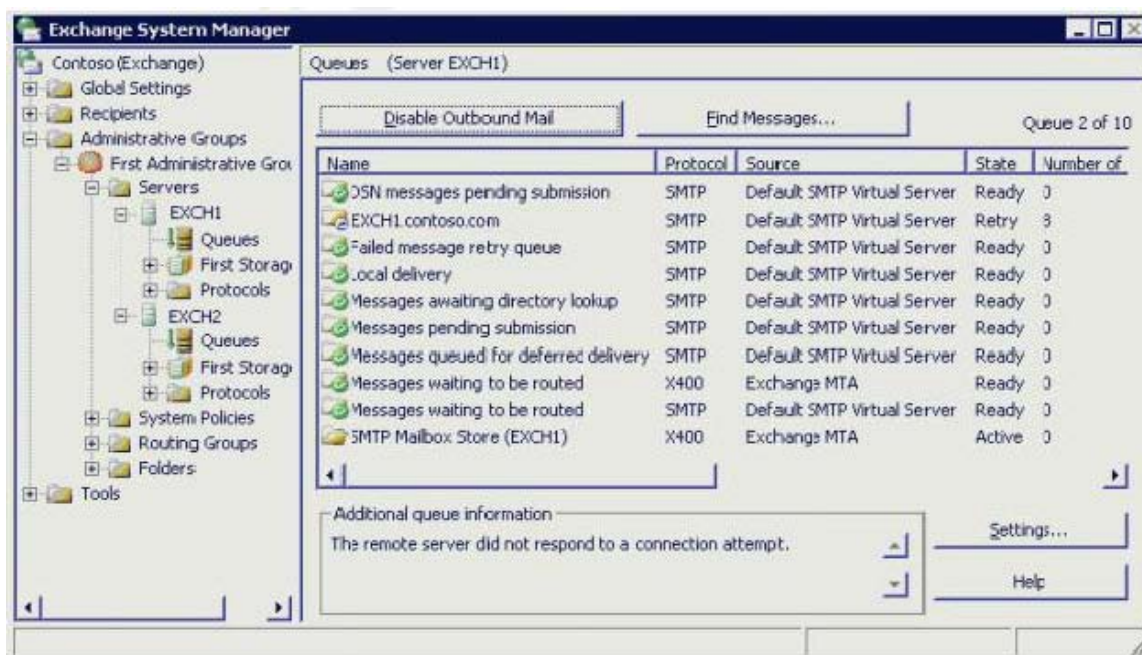
Reference:

HOW TO: Recover or Restore a Single Mailbox in Exchange Server 2003 823176

Question: 14.

You are the Exchange administrator for Company. The network consists of a single Active Directory domain named Company.com. The Exchange organization contains two servers named Exch1.Company.com and Exch2.Company.com. Both servers run Exchange Server 2003.

Users who have mailboxes on Exch1.Company.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.Company.com can send e-mail messages to mailboxes on the same server. However, e-mail messages sent to mailboxes on Exch1.Company.com are not delivered. You open Queue Viewer on Exch2.Company.com. The queue information is shown in the exhibit.



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.Company.com to accept only authenticated connections.
- B. Start the SMTP service on Exch1.Company.com.
- C. Configure a mail exchanger (MX) resource record for Exch1.Company.com on the DNS server that is authoritative for Company.com.
- D. Start the IMAP4 and POP3 services on Exch1.Company.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 organization. Exchange use SRV records to locate a Global Catalog through DSaccess component.

D. There is no problem with POP or IMAP protocols. Exchange Server uses MAPI by default

Reference:

How to Use Queue Viewer to Troubleshoot Mail Flow Issues 823489

Question: 15.

You are the Exchange administrator for Company. The Exchange organization contains a single Exchange Server 2003 computer named CompanySrv 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 lose any permissions. Therefore, the administrator needs to perform an authoritative restore for the user 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 would have to be created to attach the email account to, and since this is not done, this is not a correct answer.
- 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 no account. However, controllers would restore will restore other domain cont

e associated m other domain -authoritative overwritten by any

Free Exam 70-284 Questions

Question: 16.

You are the Exchange Server 2003 active/p CompanySrvB. The CompanySrvA is the failures that cause it CompanySrvB. You need to change troubleshoot the ca

s an Exchange SrvA and S).
 rmittent hardware EVS fails over to

online while you

- A. In Cluster Admin Remove Company
- B. In Cluster Admin the option to prev
- C. Create a new cl Select CompanySrv that CompanySrvA
- D. Create a new cl the option to prev

ompanySrvB.

ompanySrvB. Select e new cluster group. er, and ensure

cluster group. Select

Answer: B

Get complete **70-284 exam questions and answers** by visiting URL
["http://www.techexams.ws/exams/70-284.do"](http://www.techexams.ws/exams/70-284.do)