

PASS4SURES.COM

A Composite Solution With Just One Click

Microsoft

70-663 PRACTICE EXAM

**PRO: Designing and Deploying Messaging Solutions with Microsoft Exchange
Server 2010**

SIMPLE QUESTIONS: 271

4 CASE STUDY QUESTIONS: 45

TOTAL QUESTION: 316

Question: 1

Your network contains an Active Directory forest that has a single domain. You have an Exchange Server 2010 organization. You plan to add a new domain to this Active Directory forest and deploy Exchange Server 2010 servers in the new domain. A user named Admin1 is a member of this Active Directory group named Organization Management. Admin1 will deploy the Exchange new domain. You need to identify the minimum permissions required to allow Admin1 to install Exchange Server 2010 servers in the new domain. Which group should you add Admin1 to?

- A. Domain Admins
- B. Enterprise Admins
- C. Exchange Install Domain Servers
- D. Server Operators

Answer: C

Question: 2

Your company has a Exchange Server 2010 organization. You plan to deploy Microsoft Office Outlook and mobile devices for remote users. You need to plan the deployment of Client Access servers to support the automatic configuration of Outlook profiles and -----. What should you include in the plan?

- A. Autodiscover
- B. MailTips
- C. Remote Access Server
- D. Unified Messaging auto attendant

Answer: A

Question: 3

Your network contains an internal network and a perimeter network that are separated by firewall. The perimeter network _____ Server 2010 Edge Transport server. You plan to deploy an internal Exchange Server 2010 organization that meets the following requirements.

- Support EdgeSync synchronization
- Support encrypted delivery of outbound e-mail messages to the Edge Transport server
- Minimize the attack surface of the internal networkWhich TCP ports should you allow from the internal network to the perimeter network?

- A. 3309 and 25
- B. 3309 and 636
- C. 50636 and 25
- D. 50636 and 135

Answer: C

Explanation:

LDAP: Port 50389/TCP

Secure LDAP: Port 50636/UDP

SMTP: Port 25/TCP

Optional: enable RDP: Port 3389/TCP

Question: 4

Your network consists of a single Active Directory site. You plan to deploy Exchange Server 2010. You need to plan the deployment of Exchange Server 2010 servers to meet the following requirements:

- All Mailbox servers must belong to a database availability group (DAG)
- MAPI connections from Outlook clients must be load balanced by using a hardware load balancer
- If a single server fails, users must continue to send and receive e-mail
- The plan must minimize the number of server deployed

What should you include in the plan?

A. Deploy two servers.

On the two servers, deploy the Mailbox server role, the Client Access server role, and the Hub Transport server role.

Configure a Client Access server array.

B. Deploy two servers.

On the two servers, deploy the Mailbox server role, the Client Access server role, and the Hub Transport server role.

Enable Outlook Anywhere on both Client Access servers.

C. Deploy four servers.

On two of the servers, deploy the Mailbox server role and the Hub Transport server role.

On the other two servers deploy the Client Access server role.

Configure a Client Access server array.

D. Deploy four servers.

On two of the servers, deploy the Mailbox server role.

On the other two servers, deploy the Client Access server role, and the Hub Transport server role. Enable Outlook Anywhere on both Client Access servers.

Answer: A

Question: 5

You have an Exchange Server 2010 organization that contains multiple Hub Transport servers. You need to recommend a message hygiene solution to meet the following requirements:

- Block servers that are known to send spam
- Minimize administrative effort

What should you recommend?

A. an IP Block list

B. IP Block list providers

C. recipient filtering

D. sender filtering

Answer: B

Explanation:

IP Block List Providers are part of the connection filtering feature in Exchange. When the IP Block List Providers feature is enabled on a computer, the Connection Filter agent queries the specified IP Block List provider services to determine if the messaging server that has initiated the connection is a host that is known to send spam.

<http://technet.microsoft.com/en-us/library/dd351199.aspx>

Question: 6

Your network contains two Exchange Server 2010 Edge Transport server and five Exchange Server 2010 Hub Transport servers. All e-mail sent from your organization to the Internet is transferred by the Edge Transport servers. You need to recommend a security solution for the organization to meet the following requirements:

- Ensure that users can send encrypted messages to any other organization on the Internet
- Ensure that all Exchange related communication between Hub Transport servers and Edge Transport servers is encrypted.

What should you recommend?

- A. Deploy IPsec.
- B. Deploy SMTP over SSL.
- C. Implement Domain Security.
- D. Implement Security/Multipurpose Internet Mail Extensions (S/MIME)

Answer: D

Explanation:

S/MIME provides a consistent way to send and receive secure MIME data. Digital signatures provide authentication, message integrity, and non-repudiation with proof of origin. Encryption provides data confidentiality. Compression can be used to reduce data size.

<http://www.networksorcery.com/enp/data/smime.htm>

Question: 7

Your company has two data centers. Each data center contains a perimeter network.

Your network contains an Exchange Server 2010 organization.

You plan to deploy Exchange Server 2010 Edge Transport servers in the perimeter networks.

You need to recommend a solution for the Edge Transport servers that meets the following requirements:

- Distributes inbound email messages across all Edge Transport servers
- Ensures that users receive inbound e-mail messages if an Edge Transport server fails
- Ensures that users receive inbound e-mail messages if a single data center network becomes unavailable
- Minimize costs

What should you recommend?

- A. In each perimeter network, deploy one Edge Transport server. Implement failover clustering.
- B. In each perimeter network, deploy two Edge Transport servers. Implement failover clustering.
- C. In each perimeter network, deploy one Edge Transport server. Configure a mail exchange (MX) record for each server.
- D. In each perimeter network, deploy two Edge Transport servers. Configure a mail exchange (MX) record for each server.

Answer: C

Question: 8

Your company has an Exchange 2010 organization that contains multiple Hub Transport servers. You have a line of business application that retry e-mail messages by using a Hub Transport server named Hub1. The application only supports sending e-mail to a single SMTP server. You need to ensure that the application can retry e-mail messages if Hub1 fails. What should you do?

- A. Implement log transactions
- B. Install and configure failover clustering on the Hub Transport servers.
- C. Implement Windows network load balancing on the Hub Transport servers.
- D. Create multiple MX records for the Hub Transport servers in the internal DNS zone.

Answer: C

Question: 9

Your company has a main office and a branch office. An Active Directory site exists for each office. The offices are connected by a WAN link. You plan to deploy Exchange Server 2010 in each site. You need to identify the number of Exchange servers required to meet the following requirements:

- Maintain user access to mailboxes if a single server fails
- Use the minimize account of Exchange servers in each site

How many servers should you deploy in each site?

- A. 1
- B. 2
- C. 3
- D. 4

Answer: B

Question: 10

You have an Exchange Server 2010 organization. The organization has a Hub Transport server that has anti-spam agents installed. You plan to delegate the administration of the organization to a group named Security Administrators. You need to ensure that members of Security Administrators can manage anti-spam setting in the organization. The solution must minimize the amount of permissions assigned to Security Administrators. Which management role group should you assign?

- A. Hygiene Management
- B. Organization Management
- C. Records Management
- D. Server Management

Answer: A

Explanation:

The Hygiene Management management role group is one of several built-in role groups that make up the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Role groups are assigned one or more

management roles that contain the permissions required to perform a given set of tasks. The members of a role group are granted access to the management roles assigned to the role group. For more information about role groups, see Understanding Management Role Groups. Users who are members of the Hygiene Management role group can configure the antivirus and anti-spam features of Exchange Server 2010. Third-party programs that integrate with Exchange 2010 can add service accounts to this role group to grant those programs access to the cmdlets required to retrieve and configure the Exchange configuration.

<http://technet.microsoft.com/en-us/library/dd776125.aspx>

Question: 11

Your company has three offices. An Active Directory site named Site1, Site2 and Site3 exists for each office. You have an Exchange Server 2010 organization. You deploy Exchange Server 2010 server 2010 servers in Site1. You plan to deploy Exchange Server 2010 servers in Site2 and Site3. You need to recommend a solution that allows the Exchange Server 2010 servers to connect with the Exchange Server 2003 servers. You must meet the following requirements:

- All e-mail messages that are sent to mailboxes on Exchange Server 2003 servers from mailboxes on Exchange Server 2010 servers delivered directly from a server in Site2.
- All e-mail messages that are sent to mailboxes on Exchange Server 2010 servers from mailboxes on Exchange Server 2003 servers delivered directly to a server in Site1.

What should you recommend?

- A. Create two SMTP connections and one Active Directory SMTP site link.
- B. Create a new routing group connector and modify the default routing group connector.
- C. Create an X400 connector to Site1 and modify the cost value for the default routing group connector.
- D. Move all Exchange Server 2003 servers and Exchange Server 2010 servers to a single routing group.

Answer: B

Explanation:

To coexist with Exchange server 2003 your Exchange 2010 servers must use the Exchange 2003 as a bridgehead. This will require a new routing group connector on the Exchange 2003 Servers

Question: 12

You have an Exchange Server 2003 organization. All e-mail messages sent to the organization from the Internet are delivered to an Exchange Server 2003 server. You plan to transition the delivery of e-mail from the Internet to an Exchange Server 2010 Hub Transport server. You need to create a transition plan for e-mail delivery from the Internet. What should you plan to modify?

- A. accepted domains
- B. address lists
- C. e-mail address policies
- D. Recover connectors

Answer: A

Question: 13

You have an Exchange Server 2010 organization. The organization contains a Mailbox server named Server1. Server1 hosts two mailbox databases and one public folder database. You plan to deploy a new Mailbox server named Server2. You need to recommend a high-availability solution for Server1 that meets the following requirements:

- Mailboxes and public folders must be available if a single Mailbox server fails

- Deploy the minimum number of servers

What should you recommend?

A. Install failover clustering on both servers, and then configure cluster continuous replication. Replicate all public folders to Server2.

B. Create and configure a database availability group (DAG).

Add Server1 and Server2 to the DAG. Create database copies.

Replicate all public folders to Server2.

C. Create and configure a database availability group (DAG).

Add Server1 and Server2 to the DAG. Deploy a new server named Server3.

Create database copies.

Configure Server3 as a dedicated public folder server.

D. Install failover Clustering on both servers, and then configure a single copy cluster (SCC).

Deploy a new server named Server3.

Configure Server3 as a dedicated public folder server.

Answer: B

Explanation:

This question really only talks about one server so I am not sure where server 2 enters the picture. In order to have to a high availability you will need a second server - which in that case B is the correct answer.

Question: 14

You have an Exchanger Server 2010 organization. You deploy an Edge Transport server. You need to implement a messages hygiene solution that meets the following requirements:

- Users must be able to receive e-mail from external recipients who have been added to their Sage Senders Lists
- The Edge Transport server must block all e-mail sent to invalid addresses inside the organization.

What should you do first?

A. Enable sender filtering

B. Create Send connectors

C. Configure real time block lists (RBLs)

D. Configure EdgeSync synchronization

Answer: D

Explanation:

In Microsoft Exchange Server 2010, the Edge Transport server role is deployed in your organization's perimeter network. Designed to minimize the attack surface, the Edge Transport server handles all Internet-facing mail flow, which provides SMTP relay and smart host services for the Exchange organization. Additional layers of message protection and security are provided by a series of agents that run on the Edge Transport server and act on messages as they're processed by the message transport components. These agents support the features that provide protection against viruses and spam and apply transport rules to control message flow. The computer that has the Edge Transport server role installed doesn't have access to Active Directory. All configuration and recipient information is stored in Active Directory Lightweight Directory Services (AD LDS). To perform recipient lookup tasks, the Edge Transport server requires data that resides in Active Directory. This data is synchronized to the Edge Transport server using EdgeSync. EdgeSync is a collection of processes that are run on a computer that has the Hub Transport server role installed to establish one-way replication of recipient and configuration information from Active

Directory to the AD LDS instance on an Edge Transport server. The Microsoft Exchange EdgeSync service copies only the information that's required for the Edge Transport server to perform anti-spam configuration tasks and the information about the connector configuration that's required to enable end-to-end mail flow. The Microsoft Exchange EdgeSync service performs scheduled updates so that the information in AD LDS remains current.

You can install more than one Edge Transport server in the perimeter network. Deploying more than one Edge Transport server provides redundancy and failover capabilities for your inbound message flow. You can load balance SMTP traffic to your organization between Edge Transport servers by defining more than one mail exchange (MX) resource record with the same priority in the Domain Name System (DNS) database for your mail domain. You can achieve consistency in configuration between multiple Edge Transport servers by using cloned configuration scripts.
<http://technet.microsoft.com/en-us/library/bb124701.aspx>

Question: 15

You have an Exchange Server 2003 organization. Users access public folders by using Microsoft Office Outlook 2003 and Outlook Web Access. You plan to transition the organization to Exchange Server 2010. You need to ensure that users can access public folders after their mailboxes have been moved to Exchange Server 2010. What should you do?

- A. Enable public folder referrals.
- B. Run the New Organization Relationship wizard.
- C. Create public folder replicas on an Exchange Server 2010 server.
- D. Run the Microsoft Exchange Inter-Organization Application tool from an Exchange Server 2003 server.

Answer: C

Explanation:

Public folders, introduced in the first version of Microsoft Exchange, are designed for shared access and provide an easy and effective way to collect, organize, and share information with other people in your work group or organization. Public folders are hierarchically organized, stored in dedicated databases, and can be replicated between servers running Exchange.

Public Folder Database Creation During Setup.

Computers running Outlook 2003 and earlier or Microsoft Entourage require a public folder database (previously called the public folder store) to connect to Exchange. Therefore, in a pure Exchange 2010 organization, as you install the Mailbox server role on the first server, Setup prompts you with the question Do you have any client computers running Outlook 2003 and earlier or Entourage in your organization? If the answer is yes, a public folder database is created. If the answer is no, a public folder database isn't created.

Question: 16

You have an Exchange organization that consists of the servers shown in the following table.

Server	Role	Exchange Server Version	Site
Server1	Mailbox Client Access	Exchange Server 2007 Service Pack 2 (SP2)	Site1
Server2	Mailbox Client Access	Exchange Server 2010	Site2
Server3	Hub Transport	Exchange Server 2007 Service Pack 2 (SP2)	Site1
Server4	Hub Transport	Exchange Server 2010	Site2

You plan to implement moderated transport for distribution groups in the organization. You need to recommend changes to the organization to support the planned implementation. What should you recommend?

- A. Upgrade Server 3 to Exchange Server 2010.
- B. Install Windows Server 2008 R2 global catalog servers.
- C. Replace all distribution groups with dynamic distribution groups.
- D. Use Server4 as the expansion server for all moderated distribution groups.

Answer: D

Question: 17

You have an Exchange Server 2010 organization. You need to recommend an e-mail retention solution to meet the following requirements:

- Ensure that users can manually control the expiration of messages in their inbox folders.
 - Ensure that administrators can archive messages that are older than a specified number of days automatically.
- What should you recommend?

- A. managed folders
- B. journal rules
- C. Personal Archives
- D. Retention policies

Answer: C

Question: 18

Your network contains two Exchange Server 2010 Edge Transport servers. The network also contains five Hub Transport servers in two Active Directory sites. All e-mail sent to the network is received by the Edge Transport servers. You plan to configure anti-spam filtering. You need to ensure that the anti-spam filtering configurations are applied to both Edge Transport servers. The solution must use a minimum amount of administrative effort. What should you do?

- A. Configure EdgeSync synchronization
- B. Implement Active Directory Federation Services (AD FS)
- C. Join both Edge Transport servers to an Active Directory domain and then create a forest trust for the internal forest
- D. Manually configure settings on one Edge Transport server and then export the settings to the other Edge Transport server

Answer: D

Question: 19

You have an Exchange Server 2010 organization. You plan to deploy a monitoring solution for Exchange Server 2010. You need to recommend a solution to track the usage of ActiveSync clients and to analyze usage trends. What should you include in the solution?

- A. Internet Information Server log files
- B. Exchange Server Mail Flow Troubleshooter
- C. Exchange Server Performance Troubleshooter
- D. Microsoft System Control Configuration Manager

Answer: A

Question: 20

You have an Exchange Server 2010 organization.

You plan to deploy a public folder access solution to meet the following requirements:

- Users in the legal department must be able send e-mail messages to public folders.
- Users in the legal department must not be able to read documents in the public folders by using Outlook Web App (OWA).

You need to recommend changes to public folder access that meet the company requirements.

What should you recommend?

- A. mail-enabled public folders and Editor Permissions
- B. mail-enabled public folders and Contributor permissions
- C. OWA segmentation and Reviewer permissions
- D. OWA segmentation and Send As permissions

Answer: B

Explanation:

Table 1 Public folder client access rights. At the very least Contributor permissions will allow a user to view and send email

Question: 21

Your network consists of a single Active Directory domain. The domain contains three domain controllers and one DNS server. You plan to deploy Exchange Server 2010. You need to recommend a DNS implementation that provides redundancy if a DNS server fails. What should you include in the recommendations?

- A. Active Directory integrated DNS server
- B. DNS forwarding
- C. integrated DNS and WINS
- D. multiple MX records

Answer: A

Explanation:

With 3 domain controller all running the DNS service this will provide good fault tolerance if a single server fails. Keep in mind that Exchange Server also requires Global Catalog Servers - so you should have more than one on the network.

Question: 22

Your company has three offices. Each office has a direct link to the Internet. The offices connect to the each other by using a WAN link. Your network consists of an Active Directory forest that contains two domains and one site. The functional level of the forest is windows server 2003. All domains controllers run Windows Server 2003 R2. Each office contains two domains controllers for each domain. All domain controllers are global catalog servers. In each office, you plan to deploy Mailbox, Client Access and Hub Transport Exchange Server 2010 servers. All e-mail messages sent to the Internet will be delivered from a local server in each office. You need to recommend changes to the Active

Directory environment to support the planned deployment of Exchange Server 2010. What should you recommend?

- A. Disable site link building for the forest.
- B. Modify the cost values for the default IP site link.
- C. Create a separate Active Directory subnet and site object for each office.
- D. Upgrade one domain controller in each office to windows Server 2008.

Answer: C

Question: 23

You have an Exchange Server 2010 organization and an Active Directory Rights Management Services (AD RMS) server. All users access their mailboxes by using Outlook Web App (OWA).

You need to plan a security solution for the organization to meet the following requirements:

- Secure messages by using administrator-defined templates
- Ensure that e-mail messages sent by users can be stored in an encrypted format

What should you include in the plan?

- A. a legal hold
- B. Domain Security
- C. Outlook Protection Rules
- D. Secure/Multipurpose Internet Mail Extensions (S/MIME)

Answer: C

Explanation:

Information workers exchange sensitive information such as financial reports and data, customer and employee information, and confidential product information and specifications, by e-mail everyday. In Microsoft Exchange Server 2010, Microsoft Outlook, and Microsoft Office Outlook Web App, users can apply Information Rights Management (IRM) protection to messages by applying an Active Directory Rights Management Services (AD RMS) rights policy template. This requires an AD RMS deployment in the organization. For more information about AD RMS, see Active Directory Rights Management Services.

However, when left to the discretion of users, messages may be sent in clear text without IRM protection. In organizations that use e-mail as a hosted service, there's a risk of information leakage as a message leaves the client and is routed and stored outside the boundaries of an organization. Although e-mail hosting companies may have well-defined procedures and checks to help mitigate the risk of information leakage, after a message leaves the boundary of an organization, the organization loses control of the information. Outlook protection rules can help protect against this type of information leakage.

In Exchange 2010, Outlook protection rules help your organization protect against the risk of information leakage by automatically applying IRM-protection to messages in Outlook 2010. Messages are IRM-protected before they leave the Outlook client. This protection is also applied to any attachments using supported file formats.

When you create Outlook protection rules on an Exchange 2010 server, the rules are automatically distributed to Outlook 2010 by using Exchange Web Services. For Outlook 2010 to apply the rule, the AD RMS rights policy template you specify must be available on users' computers.

Question: 24

You have an Exchange Server 2010 organization. You design a deployment of multiple Mailbox servers. Your company's Service Level Agreement (SLA) states that servers must support 1,000 concurrent connections to mailboxes while maintaining an ----- latency of less than 20 milliseconds. You need to verify that your design meets the

requirements of the SLA before you deploy servers in the production environment. Which tool should you use?

- A. Exchange Server Jetstress 2010
- B. Exchange Server User Monitor (ExMon)
- C. Exchange Server Load Generator (LoadGen) 2010
- D. Exchange Server Remote Connectivity Analyzer (ExRCA)

Answer: C

Explanation:

Use Microsoft Exchange Load Generator (LoadGen) as a simulation tool to measure the impact of MAPI, OWA, IMAP, POP and SMTP clients on Exchange servers. LoadGen allows you to test how a server running Exchange responds to e-mail loads. To simulate the delivery of these messaging requests, you run LoadGen tests on client computers. These tests send multiple messaging requests to the Exchange server, thereby causing a mail load. LoadGen is a useful tool for administrators who are sizing servers and validating a deployment plan. Specifically, LoadGen helps you determine if each of your servers can handle the load to which they are intended to carry. Another use for LoadGen is to help validate the overall solution.

<http://www.microsoft.com/download/en/details.aspx?id=14946>

Question: 25

Your company has an Active Directory forest. The network contains Exchange Server 2007 Service Pack 1 (SP1) and Exchange Server Service Pack 2 (SP2) servers. All domain controllers run windows Server 2003 Service Pack 1 (SP1). You plan to deploy Exchange Server 2010 on the network. You need to recommend changes to the servers so that you can deploy Exchange Server 2010 servers. What should you upgrade first?

- A. all domain controllers to Windows Server 2003 (x64) SP2
- B. all domain controllers to Windows Server 2008 (x86)
- C. all Exchange Server 2003 servers to Exchange Server 2007 SP2
- D. all Exchange Server 2007 SP1 servers to Exchange Server 2007 SP2

Answer: D

Question: 26

Your network contains 20 offices. Each office contains 1,000 users. The users access their e-mail messages by using Microsoft Exchange server. You have an Exchange Server 2010 organization. You need to recommend an Exchange Server solution that meets the following requirement:

- Ensures that users in each office download the list of recipients for their office only
 - Ensures that users in each office can send e-mail messages to any user in the organization
- What should you recommend?

- A. Create 20 new address lists and 20 offline address books (OABs).
- B. Create 20 new managed folder mailbox policies and 20 e-mail address policies.
- C. Create 20 new dynamic distribution groups and then create 20 new global address lists (GALs).
- D. Create 20 new mailbox databases and then move the mailboxes from each office to a separate mailbox database.

Answer: A

Question: 27

You have an Exchange Server 2010 organization that contains a database availability group (DAG). You need to recommend a Mailbox database security solution to meet the following requirements:

- Maximize read/write performance
- Prevent access to database files if a server is stolen

What should you recommend?

- A. Encrypted File System (EFS)
- B. DAG network encryption
- C. Rights Management Service (RMS)
- D. Windows BitLocker Drive Encryption

Answer: D

Question: 28

You have an Exchange Server 2010 organization. You have a global security group named Legal that contains all the members of your company's legal department. The company's security policy states that the Legal group must be able to search all mailboxes for e-mail messages that contain specific keywords. You need to recommend a solution for the organization that complies with the security policy. What should you include in the solution?

- A. a Discovery Management role group
- B. a legal hold
- C. administrator audit logging
- D. Mailbox journaling

Answer: A

Explanation:

In order to search mailboxes you need to be a member of the Discovery Management role group. The Discovery Management role group is one of several built-in role groups that make up the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Role groups are assigned one or more management roles that contain the permissions required to perform a given set of tasks. The members of a role group are granted access to the management roles assigned to the role group. For more information about role groups, see Understanding Management Role Groups. Administrators or users who are members of the Discovery Management role group can perform searches of mailboxes in the Exchange organization for data that meets specific criteria and can also configure legal holds on mailboxes.

<http://technet.microsoft.com/en-us/library/dd351080.aspx>

Question: 29

You have an Exchange Server 2010 organization.

Your company's compliance policy states the following:

- Delete e-mail messages sent to legal department users that are older than 180 days.
- Delete e-mail messages sent to all other users that are older than 60 days

You need to recommend a solution that meets the requirements of the compliance policy.

What should you recommend?

- A. Configure deleted item retention for all users.

- B. Configure Personal Archives for legal department users.
C. Create two Managed Folder mailbox policies.
Use one policy for the legal department users.
Use the other policy for all other users.
D. Create two new message classifications.
Use one messages classification for the e-mail sent to legal department users.
Use the other message classification for the e-mail sent to all other users.

Answer: C

Question: 30

You have an Exchange Server 2010 organization. The users access their mailboxes by using Outlook Web App (OWA). You need to plan a solution to reduce the number of e-mail messages that are accidentally sent to distribution groups that contain company executives. What should you include in the plan?

- A. custom MailTips
B. dynamic distribution groups
C. Outlook Protection Rules
D. sharing policies

Answer: A

Explanation:

MailTips are informative messages displayed to users while they're composing a message. Microsoft Exchange Server 2010 analyzes the message, including the list of recipients to which it's addressed, and if it detects a potential problem, it notifies the user with MailTips prior to sending the message. With the help of the information provided by MailTips, senders can adjust the message they're composing to avoid undesirable situations or non-delivery reports (NDRs). The following unproductive messaging scenarios are common in any messaging environment:

- NDRs resulting from messages that violate restrictions configured in an organization such as message size restrictions or maximum number of recipients per message.
- NDRs resulting from messages sent to recipients that don't exist, recipients that are restricted, or users whose mailboxes are full.
- Sending messages to users with Automatic Replies configured.
- All of these scenarios involve the user sending a message, expecting it to be delivered, and instead receiving a response stating that the message isn't delivered. Even in the best-case scenario, like the automatic reply, these events result in lost productivity. In the case of an NDR, this scenario could result in a costly call to the Help desk.

There are also several scenarios where sending a message won't result in an error, but can have undesirable, even embarrassing consequences:

- Messages sent to extremely large distribution groups.
- Messages sent to inappropriate distribution groups.
- Messages inadvertently sent to recipients outside your organization.
- Selecting Reply to All to a message that was received as a Bcc recipient.
- All of these problematic scenarios can be mitigated by informing users of the possible outcome of sending the message as they're composing the message. For example, if senders know that the size of the message they're trying to send exceeds the corporate policy, they won't attempt to send the message. Similarly, if senders are notified that the message they're sending will be delivered to people outside the organization, they're more likely to ensure that the content and the tone of the message are appropriate.
- By addressing the scenarios listed earlier, MailTips can help you to:

- Reduce the cost of processing and storing messages by preventing NDRs.
- Reduce the volume of Help desk calls caused by NDRs.
- Increase productivity by avoiding communications that won't succeed, for example, breaking the cycle of sending an e-mail message, receiving an automatic reply, and then redirecting the message.
- Inform your users as they compose e-mail messages about various policies configured in your organization that impose limits on the messages sent.
- Direct your users to the correct distribution groups.
- Reduce the risk of inadvertent disclosure of information to people outside your organization.

<http://technet.microsoft.com/en-us/library/dd297974.aspx>

Question: 31

You have an Exchange Server 2010 organization.

All users on the network connect to their mailboxes by using Microsoft Office Outlook.

Your company's compliance policy states that:

- A copy of e-mail messages sent to the human resources department from the Internet must be archived
- All archived e-mail messages must be stored on a third-party archival server

You need to recommend a solution that meets the requirements of the compliance policy.

What should you include in the solution?

- A. Journal rules
- B. Personal archives
- C. Retention Policies
- D. Transport Protection Rules

Answer: A

Explanation:

Journaling can help your organization respond to legal, regulatory, and organizational compliance requirements by recording inbound and outbound e-mail communications. When planning for messaging retention and compliance, it's important to understand journaling, how it fits in your organization's compliance policies, and how Microsoft Exchange Server 2010 helps you secure journaled messages.

<http://technet.microsoft.com/en-us/library/aa998649.aspx>

Question: 32

You have an Exchange Server 2010 organization. You enable journaling in the organization. You need to recommend a solution that prevents administrators from reading confidential e-mail messages sent between company executives. What should you recommend?

- A. Deploy Active Directory Rights Management Services (AD RMS) templates and create Outlook Protection Rules.
- B. Deploy Active Directory Rights Management Services (AD RMS) templates and create Transport Protection Rules.
- C. Deploy an X.509 certificate from an enterprise certification authority (CA) to each executive. Instruct the executive to connect to the Exchange servers by using SMTP over TLS.
- D. Deploy an X.509 certificate from a trusted third-party certification authority (CA) to each executive. Instruct the executive to encrypt e-mail messages by using Security/Multipurpose Internet Mail Extensions (S/MIME).

Answer: D

Question: 33

Your company has a main office and two branch offices. Your network consists of a single domain Active Directory forest. An Active Directory exists for each office. The main office contains five domain controllers that run windows Server 2004 (x64). Each branch office contains one read only domain control (RODC) that runs Windows Server 2008. All domain controllers are configured as global catalog servers. You plan to deploy one Exchange Server 2010 server in each site. You need to recommend changes to Active Directory to support the planned deployment. The solution must ensures that Exchange servers branch office site connect to their local domain controllers. What should you recommend?

- A. Implement a DNS zone for each office.
- B. Change all RODCs to Windows Server 2008 (x64) RODCs.
- C. Implement a writable domain controller in each branch office.
- D. Disable site link bridging for the forest and configure Exchange specific casts.

Answer: C

Explanation:

RODC domain controllers are not considered to be suitable for Exchange Servers. Microsoft documentation states you must have a writable domain controller to support exchange server

Question: 34

Your company has two main offices named Main1 and Main2. An Active Directory site exists for each office. Users connect locally to servers in both offices. The offices connect to each other by using a high speed WAN link. You plan to deploy Exchange Server 2010. You need to plan the deployment of Mailbox servers to meet the following requirements:

- Ensure that users can access their mailbox from a server in their site, if a single Mailbox server fails
- Ensure that users can access their mailboxes remotely if a site fails
- Minimize the number of servers

How many Mailbox servers should you include in the plan?

- A. 2
- B. 3
- C. 4
- D. 6

Answer: C

Question: 35

You have an Exchange Server 2010 organization that consists of 50 Exchange Server 2010 servers. Your company's security policy states that approved Exchange and Windows Server patches and security updates must be applied to all exchange servers with in one week of being released. You need to recommend a patch management solution that meets the following requirements:

- Allow administrators to manually approve patches and security updates
- Allow only the installation of approved patches and security updates
- Minimize the administrative effort to deploy patches
- Minimize the deployment casts

What should you include in the solution?

- A. Microsoft Update
- B. Microsoft System Center Configuration Manager
- C. Windows Server Update Services
- D. Windows Update

Answer: C

Question: 36

You have an Exchange Server 2010 organization. You need to plan a solution to prevent sensitive information from being forwarded on the Internet. What should you include in the plan?

- A. a custom Send connector
- B. custom MailTips
- C. Role Based Access Control (RBAC) role entries
- D. Transport Protection Rules

Answer: D

Question: 37

You have an Exchange Server 2010 organization. Your company's security policy states that only approved mobile devices can connect by using Exchange ActiveSync. You need to implement a solution that prevents specified mobile devices from connecting to the Exchange servers. What should you implement?

- A. a new client throttling policy
- B. a new Exchange ActiveSync device access role
- C. a new Exchange ActiveSync policy
- D. a new Microsoft Server ActiveSync virtual directory

Answer: C

Question: 38

Your network contains Exchange Server 2010 servers. All users access their mailboxes by using Outlook Web App (OWA). Your company's compliance policy states the following:

- All e-mail messages that contain customer contracts must be stored for three years
- Users must be able to classify e-mail messages that relate to customer contracts
- Users must be able to move e-mail messages to any folder

You need to recommend a solution that supports the requirements of the compliance policy. What should you recommend?

- A. Managed Folder mailbox policies
- B. an OWA mailbox policy
- C. Personal Archives and an Archive policy
- D. Retention Policy Tags and a Retention Policy

Answer: D

Explanation:

Retention tags are used to apply retention settings to folders and individual items such as e-mail messages and voice mail. These settings specify how long a message remains in a mailbox and the action to be taken when the message reaches the specified retention age. When a message reaches its retention age, it's moved to the personal archive or deleted. Unlike managed folders (the MRM feature introduced in Exchange Server 2007), retention tags allow users to tag their own mailbox folders and individual items for retention. Users no longer have to file items in managed folders provisioned by an administrator based on message retention requirements. You can use retention policies to group one or more retention tags and apply them to mailboxes. A mailbox can't have more than one retention policy. Retention tags can be linked to or unlinked from a retention policy at any time, and the changes automatically take effect for all mailboxes that have the policy applied.

A retention policy can have the following retention tags:

- One or more RPTs for supported default folders
- One DPT with the Move to Archive action
- One DPT with the Delete and Allow Recovery or Permanently Delete actions
- One DPT for voice mail messages in Exchange 2010 SP1
- Any number of personal tags

Although you can add any number of personal tags to a retention policy, having many personal tags with different retention settings can confuse users. We recommend linking no more than 10 personal tags to a retention policy. Retention policy can contain both archive tags (tags that move items to the personal archive mailbox) and deletion tags (tags that delete items). A mailbox item can also have both types of tags applied. Archive mailboxes don't have a separate retention policy. The same retention policy is applied to the primary and archive mailbox.

When planning to create retention policies, you must consider whether they'll include both archive and deletion tags. As mentioned earlier, a retention policy can have one DPT that uses the Move to Archive action and one DPT that uses either the Delete and Allow Recovery or Permanently Delete action. The DPT with the Move to Archive action must have a lower retention age than the DPT with a deletion action. For example, you can use a DPT with the Move to Archive action to move items to the archive mailbox in two years, and a DPT with a deletion action to remove items from the mailbox in seven years.

<http://technet.microsoft.com/en-us/library/dd297955.aspx>

Question: 39

Your network contains an internal network and a perimeter network. The internal network contains an Active Directory forest. The forest contains a single domain. You plan to deploy 10 Edge Transport servers on the perimeter network. You need to recommend a solution for the Edge Transport server deployment. The solution must meet the following requirements:

- Allow administrators to apply a single security policy to all Edge Transport servers
- Reduce the administrative overhead that is required to manage servers
- Minimize the attack surface of the internal network

What should you recommend?

- A. Implement Network Policy and Access Services (NPAS).
- B. Implement Active Directory Federation Services (AD FS).
- C. Create a new Active Directory domain in the internal forest, and then join all Edge Transport servers to the new domain.
- D. Create an Active Directory forest in the perimeter network, and then join all Edge Transport servers to the new domain.

Answer: A

Explanation:

Edge Servers must be in the DMZ - perimeter Network - I am not sure why they need 10 Edge Transport Servers - sounds like a slight overkill

Question: 40

You have an Exchange Server 2010 organization. Company policy states that a copy of user's mailbox must be kept for one year after the user leaves the company. All user accounts are in an organizational unit (OU) named OU1. A compliance administrator plans to export the mailboxes to personal folders. You need to recommend a solution that allows the compliance administrator to meet the requirements of the company policy. What should you include in the solution?

- A. a new management role assignment
- B. delegated perimeters to OU1
- C. managed folder mailbox policies
- D. new personal Archives

Answer: A

Explanation:

A management role assignment policy is a collection of one or more end-user management roles that enables end users to manage their own Microsoft Exchange Server 2010 mailbox and distribution group configuration. Role assignment policies, which are part of the Role Based Access Control (RBAC) permissions model in Exchange 2010, enable you to control what specific mailbox and distribution group configuration settings your end users can modify. Different groups of users can have role assignment policies specialized to them.

<http://technet.microsoft.com/en-us/library/dd638100.aspx>

Question: 41

You have an Exchange Server 2010 organization. The company has ten departments. All Active Directory user objects are located in a separate organizational unit (OU) for each department. Each user belongs to a separate Exchange distribution group for each department. You need to plan the assignment of administrative rights for organization. The plan must meet the following requirements:

- Managers of all departments must be prevented from changing the mail flow settings or e-mail address of a group
- Managers of all departments must be able to change the distribution group membership of their respective departments

What should you include in the plan?

- A. For each department distribution group, modify the Managed By settings.
- B. For each department distribution group, modify the message moderation settings.
- C. For each department manager, assign the MyDistributionGroupMembership management role.
- D. On each departmental OU, assign the department manager the Change permissions for group objects.

Answer: C

Explanation:

The MyDistributionGroupMembership management role enables individual users to view and modify their membership in distribution groups in an organization, provided that those distribution groups allow manipulation of group membership. This management role is one of several built-in roles in the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Management roles, which are assigned to one or more management role groups, management role assignment policies, users, or universal security groups (USG), act as a

logical grouping of cmdlets or scripts that are combined to provide access to view or modify the configuration of Exchange 2010 components, such as mailboxes, transport rules, and recipients. If a cmdlet or script and its parameters, together called a management role entry, are included on a role, that cmdlet or script and its parameters can be run by those assigned the role. For more information about management roles and management role entries, see Understanding Management Roles.

<http://technet.microsoft.com/en-us/library/dd876900.aspx>

Question: 42

You are the enterprise administrator for an Exchange Server 2010 organization. All users run Microsoft Office Outlook 2010. You are designing a sharing solution for your organization and a partner organization. The partner organization uses Exchange server 2010. You need to recommend a strategy for sharing information with the partner organization to meet the following requirements:

- Provide cross-organizational access to user contacts
- Provide cross-organizational access to free/busy information

What should you recommend?

- A. Creating cross forest trusts
- B. Implementing Federated Sharing
- C. Implementing Microsoft Modify LifeCycle Manager (ILM) 2007
- D. Running the Microsoft Exchange Inter-Organization Replication tool

Answer: B

Question: 43

You have an Exchange Server 2010 organization that has Active Directory Rights Management Services (AD RMS) installed. You need to recommend a messaging security solution that meets the following requirements:

- Ensures that disclaimers can be applied to all e-mail messages
- Ensures that all e-mail messages sent from the legal department cannot be printed

What should you include in the solution?

- A. Journal Report Decryption
- B. Retention policies
- C. Secure/Multipurpose Internet Mail Extensions (S/MIME)
- D. Transport Protection Rules

Answer: D

Question: 44

You have an Exchange Server 2010 organization.

You plan to deploy two new Mailbox servers. Both Mailbox servers will be members of a database availability group (DAG).

You need to recommend a hard-disk configuration for the new servers. Your recommendation must meet the following requirements:

- Minimize write performance
- Prevent a switchover if a single disk fails

Which disk configuration should you recommend?

- A. RAID 0 array
- B. RAID 1 array
- C. RAID 5 array
- D. RAID 10 array

Answer: D

Question: 45

Your company has a main office and 10 branch offices. Each office connects to the Internet by using a direct link. The main office connects to the branch offices by using a WAN link.

You plan to deploy Exchange Server 2010 servers in each office. You need to design Active Directory to meet the following Exchange Server 2010 requirements:

- Users must be able to access their mailboxes if a single domain controller fails
- Users must be able to send e-mail messages to the Internet if a WAN link fails

What should you include in the design?

- A. Create an Active Directory site for each office. Deploy two global Catalog servers in each site.
- B. Create an Active Directory site for each office. Deploy a single domain controller in each site, and then enable site link bridging.
- C. Create an Active Directory site for all of the offices. Deploy a global catalog server and a read only domain controller in each site.
- D. Create an Active Directory site for all of the offices. Deploy a global catalog server and two read only global catalog servers in each site.

Answer: A

Question: 46

You plan to deploy Exchange Server 2010 on your network.

You plan to deploy the servers configured as shown in the following table.

Hardware	Value
Processor	4-socket x64
RAM	32 GB
Hard disk	16 x 1-terabyte 7200 RPM SATA
Network interface	2 x 10-GB Ethernet

You need to recommend a solution to deploy Mailbox servers.

The solution must meet the following requirements:

- Maintain redundancy if a single disk fails
- Maintain redundancy if a single server fails
- Minimize hardware costs

What should you recommend?

- A. Deploy two Mailbox servers. Configure each server to have a RAID 5 array.
- B. Deploy a two-node Network Load Balancing cluster. Configure each server to have a RAID 5 array.
- C. Deploy a database availability group (DAG) that contains three members. Configure each member to use JDCO
- D. Deploy a three-node Network Load Balancing cluster. Configure each server to connect to a Fiber Channel (FC) Storage Area Network.

Answer: C

Explanation:

Pass4Sure had A as the correct answer - I do not feel this is correct and I believe C is the best answer

Question: 47

Your network contains two subnets named Subnet1 and Subnet2. Subnet1 contains all company servers. Subnet2 contains all client computers. Subnet1 and Subnet2 are separated by a firewall. Some client computers connect by using Outlook Any where and some client computers connect by using MAP1. You plan to deploy the Exchange Server 2010 servers shown in the following table.

Server Name	Role installed
Server1	Mailbox
Server2	Hub Transport
Server3	Client Access

You need to ensure that users can access their mailboxes and public folders by using Microsoft Office Outlook. What should you configure on the firewall?

- A. Open TCP ports, 80, 443, 135 and 1024 to 65535 from the client subnet to Server3. Open TCP port 25 to Server3.
- B. Open TCP ports 80, 135 and 1024 to 65535 from the client subnet to Server1. Open TCP port 25 to Server2.
- C. Open TCP ports 80 and 443 from the client subnet to Server3. Open TCP port 1024 to 65535 from the client subnet to Server1.
- D. Open TCP ports 441, 135, and 1024 to 65535 from the client subnet to Server1. Open TCP ports 135 and 1024 to 65535 from the subnet to server 3

Answer: C

Question: 48

Your company has a Active Directory forest. The forest contains two sites named Site1 and Site2. You plan to deploy Exchange Server 2010 servers in both sites. You need to plan a high availability subnet for the Mailbox servers that meets the following requirements:

- Users must be able to access their mailboxes if a single server fails
 - Users must be able to access their mailboxes remotely if a single site becomes unavailable
- What should you include in the plan?

- A. Deploy two Mailbox servers in each site. Install and configure continuous cluster replication (CCR).
- B. Deploy one Mailbox server in Site1 and one Mailbox server in Site2. Install and configure continuous cluster replication (CCR).
- C. Deploy one Mailbox server in Site1 and one Mailbox server in Site2. Install and configure continuous cluster replication (CCR).
- D. Deploy two mailbox servers in each site. Create two database availability groups (DAGs) named DAG1 and DAG2. Add the Mailbox server from Site1 to DAG1 and the Mailbox servers from Site2 to DAG2.

Answer: C

Explanation:

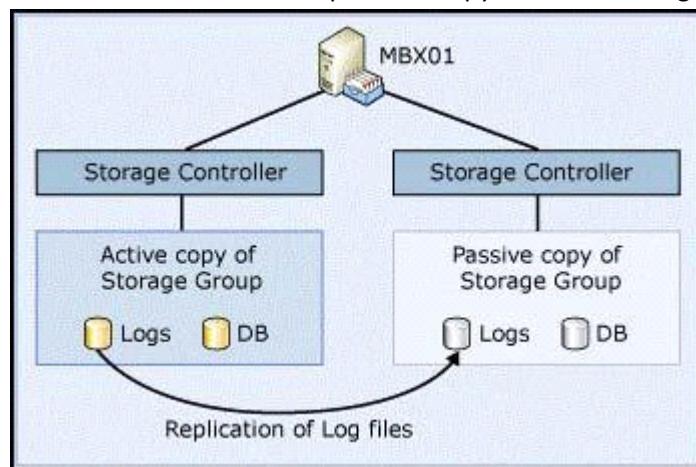
Pass4Sure had C as the correct answer and it looks like it is possible based on the following info however I did find this blurb CCR cluster nodes could be located in separate datacenters in order to provide site-level redundancy, but since

CCR was not developed with site resiliency in mind, there were too many complexities involved with a multi-site CCR cluster solution (for details on multi-site CCR cluster deployment take a look at a previous article series of mine). This made the Exchange Product group think about how they could provide a built-in feature geared towards offering site resilience functionality with Exchange 2007.

http://www.msexchange.org/articles_tutorials/exchange-server-2010/high-availability-recovery/uncoveringexchange-2010-database-availability-groups-dags-part1.html

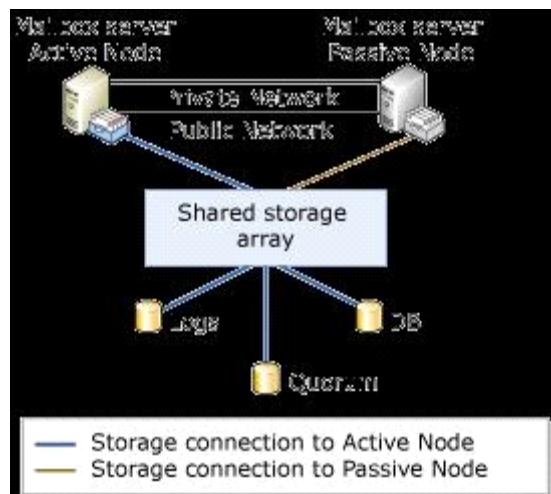
I really think that D is the better answer for this question

Exchange 2007 introduced LCR, CCR, SCC and SCR LCR (local continuous replication) this was mainly used for small business who wanted to replicate a copy of their Exchange database to another disk on the same server.



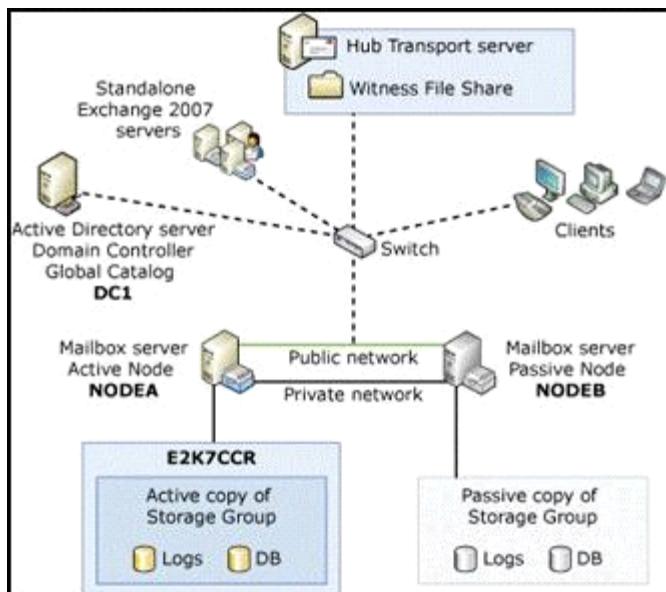
SCC (Single copy cluster) was what I would call a traditional Exchange cluster which used shared storage to host the Exchange database.

Basic architecture of an SCC

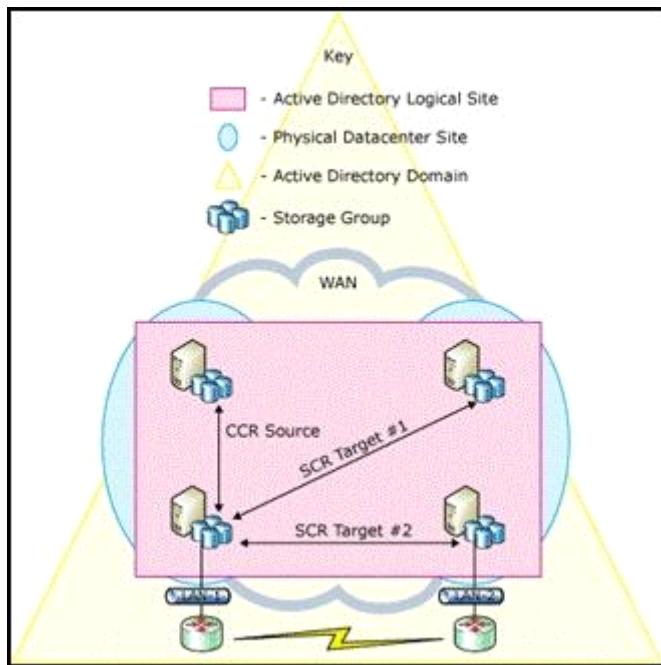


CCR (cluster continuous replication) was used to replicate Exchange database information between 2 Exchange server allowing for hardware and storage redundancy but was limited to 1 Active node and 1 Passive node.

Basic deployment of CCR



SCR (standby continuous replication) was introduced in Exchange 2007 SP1 to provide the ability to replicate Exchange databases to an disaster recovery location.



How did it use to work?

The concept of a DAG and how it functions I believe is easier learned by someone who hasn't worked with Exchange clusters previously. In Ex 200X an Exchange server was installed as either an Active or Passive cluster node at the time setup.exe was run. Depending on which version of Exchange you installed you had to create an Exchange virtual server (EVS) which was changed to cluster mailbox server (CMS) in Exchange 2007. When a user connected Outlook the mailbox server name was a clustered resource which moved between any number of nodes on the Exchange cluster. This allowed for no end user configuration changes all the resource moved between physical servers. An Exchange database was associated with the clustered resource and when you open EMC/ESM the only Exchange server name that was shown was the clustered node, let's call it CMS1. That means database one would always belong to CMS1 even when this moved between physical machines.

Here comes the DAG

So now it's time to forget everything that I just mentioned previously in this article about Exchange clustering.

What has been removed?

No more EVS/CMS

Database is no longer associated to a Server but is an Org Level resource
There is no longer a requirement to choose Cluster or Non Cluster at installation, an Exchange 2010 server can move in and out of a DAG as needed
The limitation of only hosting the mailbox role on a clustered Exchange server
Storage Groups have been removed from Exchange
Is anything the same?
1. Window Enterprise Edition is still required since a DAG still uses pieces of Windows Failover Clustering CCR cluster nodes could be located in separate datacenters in order to provide site-level redundancy, but since CCR was not developed with site resiliency in mind, there were too many complexities involved with a multi-site CCR cluster solution (for details on multi-site CCR cluster deployment take a look at a previous article series of mine). This made the Exchange Product group think about how they could provide a built-in feature geared towards offering site resilience functionality with Exchange 2007.

Question: 49

Your company has a main office and 10 branch offices. Each office has a direct link to the Internet. Each branch office connects to the main office. Your network consists of an Active Directory forest. Each office is configured as an Active Directory site. You plan to deploy an Exchange Server 2010 Hub Transport server in each site. You need to design a messages routing solution to meet the following requirements:

- Branch office connections to the Internet must be used to deliver e-mail
- Branch office servers must use the WAN link to the main office to deliver e-mail to other branch offices
- Branch office servers must be prevented from sending e-mail to the Internet by using the WAN link to the main office
- The solution must minimize administrative overhead

What should you include in the solution?

- A. One Send connector for each site
- B. One SMTP site link for each site
- C. Two Send connectors for each site
- D. 10 Send connectors for each site

Answer: A

Question: 50

You have an Exchange Server 2010 organization. Users have mobile devices that run Windows Mobile 6.1. You need to plan a solution to meet the following requirements:

- Ensure that users in the legal department can delete data from a mobile device if it is stolen
- Ensure that only administrators can perform remote wipes on all other mobile devices

What should you include in the plan?

- A. Create multiple Exchange ActiveSync policies.
- B. Upgrade all mobile devices to Windows Mobile 6.5.
- C. Create multiple Outlook Web App (OWA) mailbox policies.
- D. Implement Active Directory Rights Management Services (AD RMS).

Answer: A, C

Explanation:

Pass4Sure had both A and C as the correct answer however I feel only A is need

Understanding Outlook Web App Mailbox Policies

Applies to: Exchange Server 2010 SP2

Use Microsoft Office Outlook Web App mailbox policies to create organization-level policies to manage access to features in Outlook Web App. Outlook Web App mailbox policies allow you to create multiple policies at the organization level and apply them to individual mailboxes.

Looking for management tasks related to Outlook Web App mailbox policies? See Managing Outlook Web App Mailbox Policies.

In Exchange 2010, you can create multiple Outlook Web App mailbox policies and apply them to individual mailboxes. When an Outlook Web App mailbox policy is applied to a mailbox, it will override the settings of the virtual directory. In previous versions of Exchange, Outlook Web App features were managed by configuring the Outlook Web App virtual directories. Exceptions for individual mailboxes were accommodated by enabling or disabling features on individual mailboxes.

Configuring Outlook Web App Mailbox Policies

A default Outlook Web App mailbox policy is created automatically when the Client Access server role is installed. By default, all options are enabled on the default Outlook Web App mailbox policy. You can create as many Outlook Web App mailbox policies as necessary to meet the needs of your organization.

For example, you may want to create a policy that forces users to use WebReady Document Viewing to view attachments or a policy that limits users to the Light version of Outlook Web App.

You can use the Exchange Management Console or the Exchange Management Shell to create and configure Outlook Web App mailbox policies.

Applying Outlook Web App Mailbox Policies

Only one Outlook Web App mailbox policy can be applied to a mailbox.

If there's no Outlook Web App mailbox policy applied to a mailbox, the settings defined on the virtual directory will be applied.

An Outlook Web App mailbox policy can be applied to a mailbox as part of the new mailbox wizard, by using the EMC to modify an existing mailbox, or by using the Shell and the Set-CASMailbox cmdlet to apply a mailbox policy.

<http://technet.microsoft.com/en-us/library/dd335142.aspx>

Question: 51

Your company contains an internal network and a perimeter network. The internal network contains an Active Directory forest. The company has a single domain. You plan to deploy 10 Edge Transport servers on the perimeter network. You need to recommend a solution for the Edge Transport server deployment. The solution must meet the following requirements:

- Allow administrators to apply a single security policy to all Edge Transport servers
- Reduce the Administrative overhead that is required to manage servers
- Minimize the attack surface of the internal network

What should you recommend?

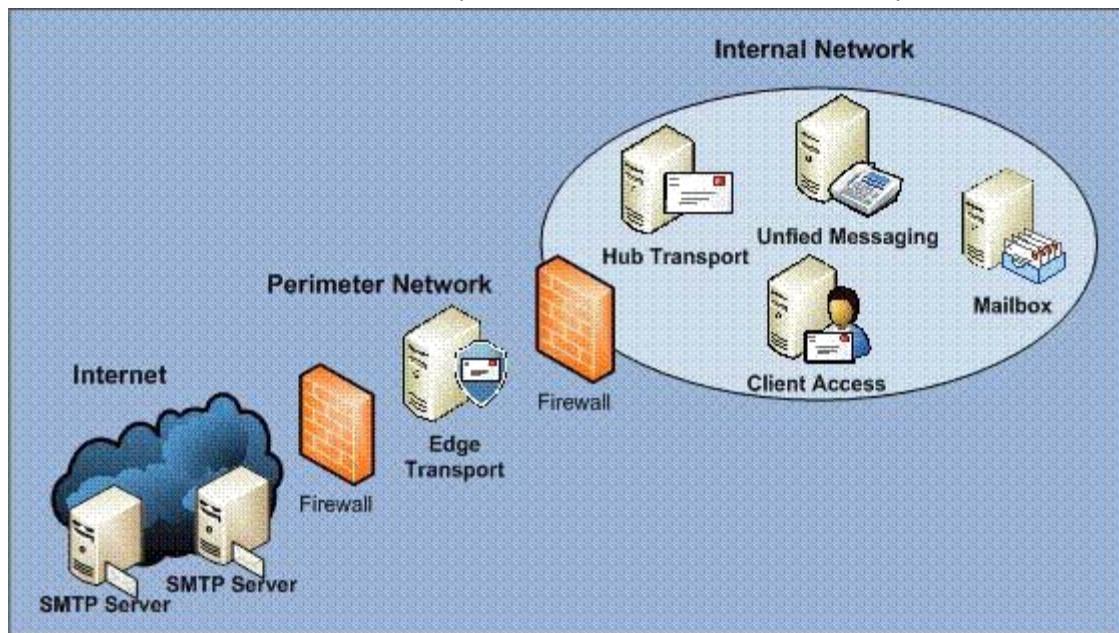
- A. Implement Network Policy and Access Services (NPAS).
- B. Implement Active Directory Federation Services (AD FS).
- C. Create a new Active Directory domain in the internal forest and then join all Edge Transport servers to the new domain.
- D. Create an Active Directory forest in the perimeter network and then join all Edge Transport servers to the new domain.

Answer: A

Explanation:

Pass4sure had A as the correct answer however I believe the correct answer is D. The Edge Transport Server role in Exchange Server 2007 is designed to be installed in your organization's perimeter network (aka DMZ or screened

subnet). The Edge Transport Server is the only Exchange 2007 server role that should not be part of your corporate Active Directory on your internal network; it should instead be installed on a stand-alone server in a workgroup or as a domain member in an Active Directory dedicated to servers located in the perimeter network as shown in Figure 1.



Although the Edge Transport Server role is isolated from Active Directory on the internal corporate production network, it is still able to communicate with the Active Directory by making use of a collection of processes known as EdgeSync that run on the Hub Transport Server and which, since it is part of the Active Directory, have access to the necessary Active Directory data. The Edge Transport server uses Active Directory Application Mode (ADAM) to store the required Active Directory data, which is data such as Accepted Domains, Recipients, Safe Senders, Send Connectors and a Hub Transport server list (used to generate dynamic connectors so that you do not need to create them manually).

It is important to understand that the EdgeSync replication is encrypted by default, and that the replication is a one-way process from Active Directory to Active Directory Application Mode (ADAM), this means that no data is replicated from ADAM to AD.

The first time EdgeSync replication occurs, the ADAM store is populated, and after that data from Active Directory is replicated at fixed intervals. You can specify the intervals or use the default settings, which when speaking configuration data is every hour and every 4th hour for recipient data.

http://www.msexchange.org/articles_tutorials/exchange-server-2007/planning-architecture/uncoveringexchange-2007-edge-transport-server-part1.html

Question: 52

You have an Exchange Server 2010 organization.

Your company's compliance policy states that the following occurs when a user leaves the company:

- The user account is disabled
- The user account and mailbox are deleted after six months
- All e-mail messages in the mailbox are retained for three years

You need to recommend a solution to retain the e-mail messages of users who leave the company. The solution must meet the following requirements:

- Ensure that a group named Group1 can manage the process
- Minimize disk space required to store the mailbox database

What should you recommend?

- A. Assign the Mailbox Search management role to Group1 and then create a retention policy.
- B. Assign the Mailbox Search management role to Group1 and then create a managed folder mailbox policy.

- C. Assign the Mailbox Import Export management role to Group1 and then configure Personal Archives for each mailbox.
- D. Assign the Mailbox Import Export management role to Group1 and then instruct Group1 to export mailboxes to personal folder (.pst) files.

Answer: D

Question: 53

Your network consists of a windows Server 2003 Active Directory forest that contains a windows Server 2003 enterprise certification authority (CA). You have an Exchange Server 2003 organization. Users access their mailboxes by using Windows Mobile 5.0 and Windows Mobile 6.1 devices. You plan to transition the organization to Exchange Server 2010. You need to plan a certificate solution for the Exchange Server 2010 deployment. The solution must minimize the amount of effort required to connect all mobile devices to the organization. What should you include in the plan?

- A. Create a self-signed certificate and install it on the Client Access server.
- B. Obtain a wildcard certificate from a trusted third-party CA and install it on the Client Access server.
- C. From an internal CA obtain a certificate that contains multiple names and install it on the Client Access server.
- D. From a trusted third-party CA obtain a certificate that contains multiple names and install it on the Client Access server.

Answer: D

Explanation:

Security Services for Windows Mobile 5.0 and Windows Mobile 6. 6/2/2010 Windows Mobile implements the following security services as part of the core operating system. Windows Mobile implements these security services so that applications can make use of them; for example, the built-in Outlook Mobile client can use SSL (and, by extension, various cryptographic algorithms) for POP and IMAP accounts.

Question: 54

You have an Exchange 2010 organization. Your company's security policy states that all connections to Outlook Web App (OWA) must use smart card authentication. You need to recommend a solution to meet the security policy requirements. Which two possible ways to achieve this goal should you recommend? (Each correct answer presents a complete solution. Choose two.)

- A. Require certificate-based authentication for all Internet-facing Client Access servers.
- B. Require Windows Integrated Authentication for all Internet-facing Client Access servers.
- C. Deploy an Edge Transport server and then disable Windows Integrated Authentication.
- D. Deploy a server that runs Microsoft Internet Security and Acceleration (ISA) Server and enable Kerberos constrained delegation.

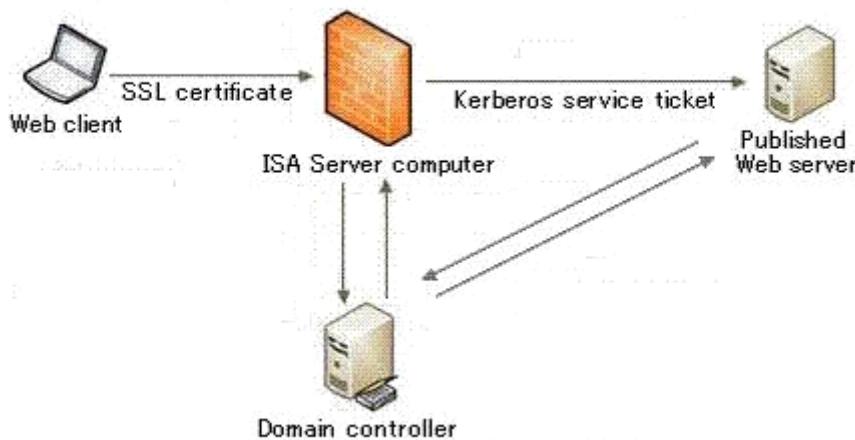
Answer: A, D

Explanation:

Microsoft® Internet Security and Acceleration (ISA) Server 2006 can publish Web servers and authenticate users to verify their identity before allowing them to access a published Web server. If a published Web server also needs to authenticate a user that sends a request to it and if the ISA Server computer cannot delegate authentication to the published Web server by passing user credentials to the published Web server or impersonating the user, the

published Web server will request the user to provide credentials for a second time. ISA Server can pass user credentials directly to a Web published server only when these credentials are received using Basic authentication or HTTP forms-based authentication. In particular, credentials supplied in a Secure Sockets Layer (SSL) certificate cannot be passed to a published server.

ISA Server 2006 introduces support for Kerberos constrained delegation to enable published Web servers to authenticate users by Kerberos after their identity has been verified by ISA Server using a non-Kerberos authentication method. When used in this way, Kerberos constrained delegation eliminates the need for requiring users to provide credentials twice. For example, because it is unrealistic to perform Kerberos authentication over the Internet, SSL certificates might be used for authenticating users at the ISA Server computer. After ISA Server verifies the user's identity, ISA Server cannot pass the SSL client certificate provided by the user to a published server, but it can impersonate the user and obtain a Kerberos service ticket for authenticating the user (client) to a published Web server.



An ISA Server computer serving as a firewall that sits between the Internet and your organization's intranet must authenticate clients that send requests over the Internet to servers in your organization to prevent attacks from anonymous and unauthorized users. Every organization determines which authentication method can ensure that external clients are identified with sufficient confidence and that unauthorized clients cannot gain access to a published internal server. Many large organizations (including Microsoft) are moving toward the use of smart cards, which are actually just secured storage devices for an SSL client certificate, as a means to identify their users instead of relying on passwords. Smart cards enable two-factor authentication based on something that the user has (the smart card) and something that the user knows (the personal identification number (PIN) for the smart card), providing a more secure level of authentication than passwords. Internal servers often need to authenticate users who send requests to them both from computers on the Internet and from computers on the intranet within the organization. For example, a mail server must verify the identity of users, including internal users, before allowing them access to the appropriate personal mailboxes. The authentication performed by an edge firewall clearly does not fully meet the needs of these servers. If ISA Server can forward a user's credentials to an internal server, there is no need to prompt the user for a second time to obtain appropriate credentials. However, when SSL client certificates are used, ISA Server cannot delegate a user's credentials to an internal mail server, such as a Microsoft Exchange server, because ISA Server never receives a password that can be passed on to that server. There is also no way to forward an SSL client certificate to another server. This is an intended security feature of the SSL protocol. Kerberos constrained delegation provides a way for ISA Server to impersonate a user sending a Web request and authenticate to specific services running on specific, published Web servers, including Exchange Outlook Web Access servers, when ISA Server knows only the user name after it verifies the identity of the user.

Question: 55

You have an Active Directory domain named contoso.local. You plan to deploy an Exchange Server 2010 organization that will contain the following server:

- Two Edge Transport servers named Edge1.contoso.com and Edge2.contoso.com
- Two Hub Transport servers named hub1.contoso.local and hub2.contoso.local

You need to design a solution that ensures that e-mail messages from the Internet can be delivered to internal recipients if a single Edge Transport server fails. What should you include in the design?

- A. two Remote Domains
- B. two SRV resource records
- C. two EdgeSync Subscriptions
- D. two mail exchange (MX) records

Answer: D

Question: 56

You have Exchange Server 2003 organization. The organization contains a front end server named FE1 and a back end server accessible from the Internet by using mail.contoso.com. You plan to transition the organization to Exchange Server 2010. You will deploy a Mailbox server named MIX1 and a Client Access server named CAS1. Users will access Outlook Web Access and Outlook Web App (OWA) by using the URL. <https://mail.contoso.com>. You need to recommend a DNS configuration for the external name of mail.contoso.com. Which server should be associated with the name mail.contoso.com?

- A. BE1
- B. CAS1
- C. FE1
- D. MIX1

Answer: B

Question: 57

You have an Exchange Server 2010 organization. Your network is separated from the Internet by a firewall. You need to identify the ports that must be opened on the firewall to allow clients from the Internet to use the following connections:

- Outlook Anywhere
- Outlook Web App (OWA)
- Exchange ActiveSync
- IMAP4 over Secure Sockets Layer (SSL)

Which TCP ports should you identify?

- A. 25, 443 and 993
- B. 26, 443 and 995
- C. 25, 80, 143 and 3269
- D. 80, 143, 443 and 389

Answer: A

Question: 58

You have an Exchange Server 2010 Hub Transport server named Hub1. You install an application on a third-party

server named Server1. You discover that the application cannot authenticate to remote servers. You need to ensure that the application can relay e-mail messages by using Hub1. What should you do?

- A.
Create a new Send connector
Add the TCP/IP address of Server1 to the Send connector
Modify the permissions for the Send connector
- B.
Create a new Receive connector
Add the TCP/IP address of Server1 to the Receive connector
Modify the permissions for the Receive connector
- C.
Add the TCP/IP address of Server1 to the default Receive connector
Create a message classification
Create a transport rule
Add the TCP/IP address of Server1 to the Client Receive connector
- D. Create a remote domain
- E. Create a transport rule

Answer: B

Question: 59

You have an Exchange Server 2010 organization that contains two Client Access servers. You deploy a Microsoft Internet Security and Acceleration (ISA) Server. You need to recommend a high availability solution for the Client Access servers. The solution must meet the following requirements:

- Ensure that Outlook Web App (OWA) connections are available if a single Client Access server fails
 - Ensure that client access services are available if a single service fails on a Client Access server
- What should you recommend?

- A. Deploy a hardware load balancer.
- B. Deploy Windows Network Load Balancing.
- C. Publish each Client Access server in a separate publishing rule.
- D. Publish both Client Access servers in a single publishing rule as a Web server farm.

Answer: D

Explanation:

Before we begin we must first use the same procedure used for migrating the SSL certificate from Exchange Server 2003 to Exchange Server 2007 to also migrate the certificate to the ISA Server 2006 firewall. Once an SSL certificate has been configured on the ISA server we can continue with the publishing rules for Outlook Web Access.

Open the **ISA Server Management** console and navigate to <ISA server name>/Firewall Policy.



Click on **Publish Exchange Web Client Access** in the Tasks pane on the right side of the ISA Server Management Console.

Firewall Policy Tasks

- Publish **Exchange** Web Client Access
- Publish **Mail** Servers
- Publish **SharePoint** Sites
- Publish **Web** Sites
- Publish **Non-Web Server** Protocols
- Create **Access** Rule

Enter a meaningful name for the new publishing rule such as "Exchange Remote Access". Click **Next** to continue.

Exchange Publishing rule name:

To continue, click **Next**.

Select the Exchange version **Exchange Server 2007** and tick the **Outlook Web Access** box. Click **Next** to continue.

Exchange version:

Web client mail services:

Outlook Web Access

Outlook Anywhere (RPC/HTTP(s))

Publish additional folders on the Exchange Server for Outlook 2007 clients

Choose **Publish a single Web site or load balancer**. Click **Next** to continue.

Publish a single Web site or load balancer

Use this option to publish a single Web site, or to publish a load balancer in front of several servers.

[Help about publishing a single Web site or load balancer](#)

Publish a server farm of load balanced Web servers

Use this option to have ISA Server load balance requests between a server farm (mirrored servers).

[Help about publishing server farms](#)

Choose **Use SSL to connect to the published Web server or server farm** as this is the most secure option. Click **Next** to continue.

Use SSL to connect to the published Web server or server farm

ISA Server will connect to the published Web server or server Farm using HTTPS (recommended).



Use non-secured connections to connect the published Web server or server farm



Question: 60

You have an Exchange Server 2010 organization. Your company acquires two companies named Contoso, Ltd and N---- Traders. You need to ensure that users from Contoso have only contoso.com e-mail addresses and users from Northwind Traders have only traders.com e-mail addresses. What should you create and configure?

- A. two accepted domains and two e-mail address policies
- B. two remote domains and two accepted domains
- C. two transport rules and two address remote entries
- D. two Receive connectors and two address lists

Answer: A

Question: 61

You have an Exchange Server 2010 organization. You plan to deploy a database availability group (DAG). You need to recommend disk configurations for the servers in the organization. The solution must minimize costs. What should you recommend?

- A. 7200 RPM SATA hard disks in a Direct Attach Storage (DAS)
- B. 7200 RPM SATA hard disks in a Network Attached Storage (NAS)
- C. 15000 RPM SAS hard disks in a Network Attached Storage (NAS)
- D. 15000 RPM SAS hard disks in a Fiber Channel (FC) Storage Area Network (SAN)

Answer: A

Explanation:

DAG has been designed to run well on low cost hard drive storage. Generally, there are no special storage requirements that are specific to DAGs or mailbox database copies. DAGs don't require or use cluster managed shared storage.

<http://technet.microsoft.com/en-us/library/dd638104.aspx>

Question: 62

You have an Active Directory forest. You plan to deploy an Exchange Server 2010 organization that contains the following servers:

- Two Edge Transport servers
- Two Hub Transport servers

You need to recommend changes to the organization to ensure that e-mail messages can be sent to the Internet if a single transport server fails. What should you recommend?

- A. Configure shadow redundancy for the Hub Transport servers.
- B. Implement failover clustering on both Hub Transport servers.
- C. Configure both Edge Transport servers as source servers for a Send connector.
- D. Create one mail exchange (MX) record and one SRV record for each Edge Transport server in the internal DNS zone.

Answer: C

Explanation:

Send connectors create a logical connection to remote e-mail systems and are responsible for outbound transmission of e-mail messages. If you use the EdgeSync process, it will configure the Send connectors required for mail flow to the Internet and to the Edge Transport servers in your Microsoft Exchange Server 2010 organization. If your organization requires a Send connector with specific configuration options, or if you don't use the EdgeSync process, you must manually configure Send connectors.

Question: 63

You have an Exchange Server 2007 organization. All users connect to mailboxes by using Microsoft Office Outlook 2003. You plan to transition the organization to Exchange Server 2010. You need to recommend a solution for mailbox access that meets the following requirements:

- Minimize support costs
- Minimize software costs
- Provide access to Public folders

What should you recommend?

- A. Implement POP3 and IMAP4 access
- B. Implement Personal Archive and forms-based authentication
- C. Implement Autodiscover and upgrade all client computers to Outlook 2010
- D. Implement Outlook Anywhere and modify the Outlook RPC encryption settings

Answer: D

Question: 64

Your network contains two data centers named Datacenter1 and Datacenter2. An Active Directory site exists for each data center. The data centers connect to the Internet by using a direct link. The data centers connect to each other by using a high speed WAN link. You plan to deploy Exchange Server 2010 Mailbox servers in both data centers. You need to plan message routing to meet the following requirements:

- Ensure outbound delivery of e-mail messages if a single server fails
- Automatically load balance the Hub Transport server in each site
- Deploy the minimum number of servers

What should you include in the plan?

- A. In each data center, deploy one Hub Transport server.
Create and configure one Send connector.
- B. In each data center, deploy two Hub Transport servers.
Create and configure one Send connector.
- C. In each data center, deploy one Edge Transport server.
Create and configure two Send connectors.
- D. In each data center, deploy two Edge Transport servers.
Create and configure two Send connectors.

Answer: B

Question: 65

You have an Exchange organization that contains Exchange 2000 Server Service Pack 3 (SP3), Exchange Server 2003 Service Pack 2 (SP2) and Exchange Server 2007 Service Pack 1 (SP1) servers. You need to transition the organization to Exchange Server 2010. What should you do first?

- A. Remove all Exchange Server 2007 SP1 servers from the organization.
- B. Remove all Exchange 2000 Server and all Exchange Server 2003 servers from the organization.
- C. Remove all Exchange 2000 Server servers from the organization and then upgrade all Exchange Server 2007 servers to SP2.
- D. Remove all Exchange Server 2003 servers from the organization and then upgrade all Exchange Server 2007 servers

to SP2.

Answer: C

Question: 66

You have an Exchange Server 2010 organization. You plan to deploy a public folder access solution that meets the following requirements:

- Users in the legal department must be able read e-mail sent to public folders
- Users in the legal department must not be able to post documents to public folders by using Outlook Web App (OWA)

You need to recommend modification to the organization to meet the requirements of the public folder access solution. What should you recommend?

- A. Modify the mailbox permissions.
- B. Modify the OWA segmentation settings.
- C. Modify the public folder client permissions.
- D. Modify the public folder administrative permissions.

Answer: C

Question: 67

Your company has an Exchange Server 2010 organization. The company's compliance policy states that all e-mail messages older than three months must be deleted automatically. You need to recommend a solution to prevent the deletion of e-mail for users on extended leave. The solution must ensure that users can view of their e-mail when they return to work. What should you recommend?

- A. a legal hold
- B. a retention hold
- C. an Outlook Protection Rule
- D. an Transport Protection Rule

Answer: B

Explanation:

Placing a mailbox on retention hold suspends the processing of a retention policy or managed folder mailbox policy for that mailbox. Retention hold is designed for scenarios such as a user being on vacation or away temporarily. During retention hold, users can log on to their mailbox and change or delete items. When you perform a mailbox search, deleted items that are past the deleted item retention period aren't returned in search results. To make sure items changed or deleted by users are preserved in legal hold scenarios, you must place a mailbox on legal hold. For more information, see Place a Mailbox on Litigation Hold. You can also include retention comments for mailboxes you place on retention hold. The comments are displayed in supported versions of Microsoft Outlook.

<http://technet.microsoft.com/en-us/library/dd335168.aspx>

Question: 68

Your network contains an internal network and a perimeter network. The perimeter network contains an Exchange Server 2010 Edge Transport server. You need to recommend a remote management solution for the Edge Transport

server that meets the following requirements:

- All management traffic must be encrypted
 - The solution must allow remote administration from the internet network
 - The solution must support the use of the Exchange Management Console (EMC)
- What should you recommend?

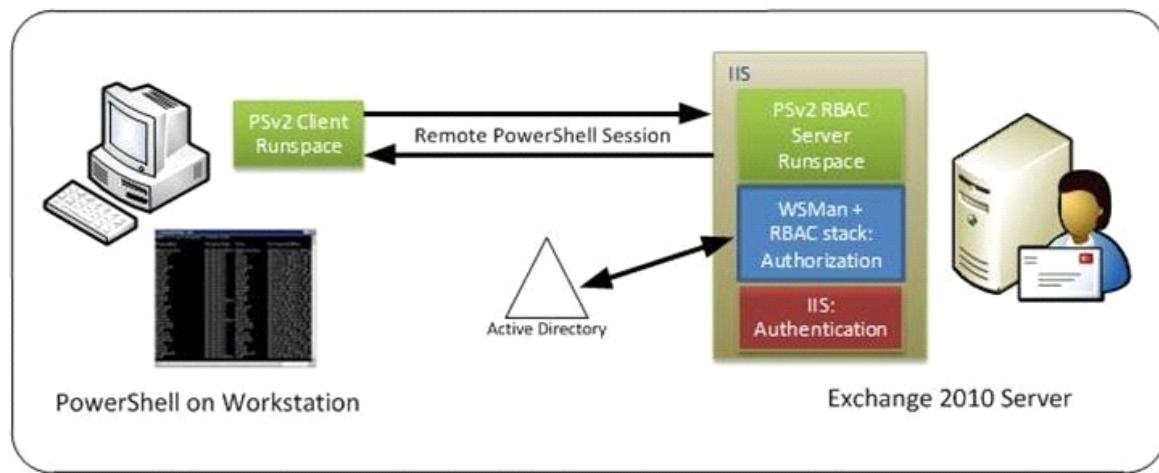
- A. Lightweight Directory Access Protocol (LDAP) over Secure Socket Layer (SSL).
- B. Remote Desktop Protocol (RDP) over Secure Socket Layer (SSL).
- C. Windows Management Instrumentation Command-line (WMIC)
- D. Windows Remote Management (WinRM) over SSL

Answer: D

Explanation:

To start off, you first need to be aware that in Exchange 2010, all management is done via Remote PowerShell, even when opening the Management Tools on an Exchange server. Where this differs from Exchange 2007 is that there is now a much larger dependency on IIS, as Remote PowerShell requests are sent via the HTTP protocol and use IIS as the mechanism for connections. IIS works with the WinRM (Windows Remote Management) service, and the WSMAN (Web Services for Management) protocol to initiate the connection.

When you click on the Exchange Management Shell shortcut, a Remote PowerShell session is opened. Instead of simply loading the Exchange snap-in (as we did with Exchange 2007), PowerShell connects using IIS to the closest Exchange 2010 server via WinRM. WinRM then performs authentication checks, creates the remote session and presents to you the cmdlets that you have access to via RBAC (Role Based Access Control).



Since all Remote PowerShell connections go through IIS, we have identified some of the most common errors that may be exhibited when attempting to open the Exchange Management tools along with the most common causes of those errors and how to address these issues. We have attempted to list these in order of frequency.

Question: 69

Your network contains two Active Directory site. The sites connect to each other by using a WAN link. You plan to deploy two Exchange Server 2010 Mailbox servers and two Client Access servers in each site. Each site will contain a Client Access array. You need to recommend a solution to deploy Hub Transport servers. The solution must meet the following requirements:

- Continue to deliver e-mail messages to users in other sites if a single Hub Transport server fails
- Support the planned Client Access array deployment
- Minimize the number of Exchange servers

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

- A. Add the Hub Transport server role to each Mailbox server.

- B. Add the Hub Transport server role to each Client Access server.
- C. Deploy two Hub Transport servers on two new servers in each site.
- D. Deploy one Hub Transport server on a new server and then install the SMTP service on each Client Access server.

Answer: A, B

Question: 70

You have an Exchange Server 2010 organization. An Edge Transport server sends and receives all e-mail messages from the internet. You notice that some servers on the Internet identify e-mail messages from your organization as spam. You need to minimize the possibility that e-mail messages send from your organization are identified as spam. What should you do?

- A. Implement Microsoft Forehead Security for Exchange Server.
- B. Create SenderID TXT records for the Edge Transport servers.
- C. Configure the Edge Transport servers to use a real-time block list (RBL).
- D. Install a server certificate from a trusted third-party certification authority (CA).

Answer: B

Explanation:

You heard right, Sender Id is coming! What is Sender Id, you ask? Don't feel bad, most Exchange admins are asking the same question. Essentially (and very simplified) Sender Id is part of an initiative (I'm not sure that is the exact correct word), to reduce spam. Sender Id is part of the Sender Policy Framework (SPF). So how does it work? First, you create a DNS TXT record for your domain (or domains) that identifies the mail servers from which e-mail will be sent for your domain. SMTP servers that support Sender Id will then check that TXT record when they receive a message from one of your users. Here is the FUD (fear, uncertainty, and doubt) part. If the message is coming from a domain that does not have a Sender Id TXT record or the record does not match the sending IP address, the receiving system has a couple of options:

- Do nothing.
- Reject the message entirely. (!!!!)
- Accept the message and then delete it prior to delivering it to the user.
- Give the message to the anti-spam inspection system with the assumption that the antispam system (such as Microsoft's IMF starting in Exchange 2003 SP2) will give the message a higher spam probability if the sender's domain does not have valid Sender Id records

<http://mostlyexchange.blogspot.ca/2005/07/sender-id-is-coming-get-your-txt.html>

Question: 71

You have an Exchange Server 2010 organization that contains two Hub Transport servers.

You need to design a recovery plan for the Hub Transport servers that meets the following requirements:

- Restores all Windows settings
- Restores all Exchange configurations
- Minimizes administrative effort

What should you include in the plan?

- A. Retention of Exchange server computer accounts in Active Directory.

Backup and recovery of Windows system state

A recovery installation of Exchange Server 2010

- B. Retention of Exchange server computer accounts in Active Directory.

- Backup and recovery of transport queues.
A custom installation of Exchange Server 2010
C. Recovery of Windows system state.
Backup and recovery of transport queues.
A typical installation of Exchange Server 2010
D. Backup and recovery of Windows system state.
A repair installation of Windows Server 2008.
A typical installation of Exchange Server 2010

Answer: A

Question: 72

Your company has 10 offices. The offices connect to the Internet by using a WAN link. The offices connect to each other by using a VPN connection. An Active Directory site exists for each office. You plan to deploy Exchange Server 2010. Each site will contain two Exchange Server 2010 servers. You need to recommend the placement of domain controllers and global catalog servers to meet the following requirements:

- Minimize the number of domain controllers
 - Must be able to deliver e-mail messages between users of the same office, if a domain controller and a WAN link fail simultaneously
- What should you recommend?

- A. In each site, install two global catalog servers.
B. In each site, install two domain controllers. Enable Universal Group Membership caching for each site.
C. In each site, install two domain controllers. Create a publishing point for an offline address list on one Exchange server in each site.
D. In each site, install one domain controller that is configured as a global catalog server. Enable Universal Group Membership caching for each site.

Answer: A

Question: 73

You have a Microsoft Internet Security and Accelerator (ISA) 2006 server that provides all Internet access for your company. You have two Mailbox servers configured in a database availability group (DAG), two Client Access servers, and two Hub Transport servers. You need to recommend changes to the environment to ensure that users can access Outlook Web App (OWA) from the Internet if any single server fails. What should you recommend?

- A. Configure a Client Access server array.
B. Deploy a second ISA server and create an ISA server array.
C. Implement Windows Network Load Balancing for the Client Access servers.
D. Deploy two Edge Transport servers that are configured to use EdgeSync synchronization.

Answer: B

Question: 74

Your network contains an internal network and a perimeter network. The internal network contains a single Active Directory site. The perimeter network contains two Exchange Server 2010 Edge Transport servers. You plan to deploy

an Exchange Server 2010 organization on the internal network. You need to plan the deployment of Hub Transport server roles to meet the following requirements:

- If a single Hub Transport server fails, e-mail messages from the Internet must be delivered to the Mailbox servers.
- If a single Hub Transport server fails, users must be able to send e-mail messages to other users that have mailboxes on the same Mailbox server.

What should you include in the plan?

- A. Deploy one Edge Transport server on the internal network, and then configure EdgeSync synchronization.
- B. Deploy one Hub Transport server on the internal network, and then configure EdgeSync synchronization.
- C. Deploy one Hub Transport server on the internal network and one Hub Transport server on the perimeter network.
- D. Deploy two Hub Transport servers on the internal network.

Answer: D

Question: 75

You have an Exchange Server 2010 organization. You need to recommend a client access solution that meets the following requirements:

- Reduces the time required for users to reconnect to user mailboxes if a single Client Access server fails
- Prevents users from being prompted for authentication if a single Client Access server fails

What should you recommend?

- A. Client Access server array and hardware load balancer
- B. database availability group (DAG) and hardware load-balancer
- C. failover clustering and database availability group (DAG)
- D. Windows Network Load Balancing and failover clustering

Answer: A

Explanation:

Understanding Load Balancing in Exchange 2010

Load balancing is a way to manage which of your servers receive traffic. Load balancing provides failover redundancy to ensure your users continue to receive Exchange service in case of computer failure. It also enables your deployment to handle more traffic than one server can process while offering a single host name for your clients.

In addition to load balancing, Microsoft Exchange Server 2010 provides several solutions for switchover and failover redundancy. These solutions include the following:

High availability and site resilience

You can deploy two Active Directory sites in separate geographic locations, keep the mailbox data synchronized between the two, and have one of the sites take on the entire load if the other fails. Exchange 2010 uses database availability groups (DAGs) to keep multiple copies of your mailboxes on different servers synchronized.

Online mailbox moves

In an online mailbox move, end users can access their e-mail accounts during the move. Users are only locked out of their accounts for a brief time at the end of the process, when the final synchronization occurs. Online mailbox moves are supported between Exchange 2010 databases and between Exchange Server 2007 Service Pack 3 (SP3) or a later version of Exchange 2007 and Exchange 2010 databases. You can perform online mailbox moves across forests or in the same forest.

Shadow redundancy Shadow redundancy protects the availability and recoverability of messages while they're in transit. With shadow redundancy, the deletion of a message from the transport databases is delayed until the transport server verifies that all the next hops for that message have completed. If any of the next hops fail before reporting successful delivery, the message is resubmitted for delivery to the hop that didn't complete. Load balancing

serves two primary purposes. It reduces the impact of a single Client Access server failure within one of your Active Directory sites. In addition, load balancing ensures that the load on your Client Access server and Hub Transport computers is evenly distributed. Architectural Changes in Exchange 2010

Load Balancing Several changes in Exchange 2010 make load balancing important for your organization. The Exchange RPC Client Access service and the Exchange Address Book service on the Client Access server role improve the user's experience during Mailbox failovers by moving the connection endpoints for mailbox access from Outlook and other MAPI clients to the Client Access server role instead of to the Mailbox server role. In earlier versions of Exchange, Outlook connected directly to the Mailbox server hosting the user's mailbox, and directory connections were either proxied through the Mailbox server role or referred directly to a particular Active Directory global catalog server. Now that these connections are handled by the Client Access server role, both external and internal Outlook connections must be load balanced across the array of Client Access servers in a deployment to achieve fault tolerance.

A load-balanced array of Client Access servers is recommended for each Active Directory site and for each version of Exchange. It isn't possible to share one load-balanced array of Client Access servers for multiple Active Directory sites or to mix different versions of Exchange or service pack versions of Exchange within the same array. When you install Exchange 2010 within your existing organization and configure a legacy namespace for coexistence with previous versions of Exchange, your clients will automatically connect to the Exchange 2010 Client Access server or server array. The Exchange 2010 Client Access server or Client

Access server array will then proxy or redirect client requests for mailboxes on older Exchange versions to either Exchange 2003 front-end servers or Exchange 2007 Client Access servers that match the mailbox version

Question: 76

You have an Exchange Server 2010 organization. The network contains an Exchange Server 2010 Mailbox server named Server1. All mailboxes are stored on Server1. You perform a Typical installation of Exchange Server 2010 on a new server named Server2. You plan to implement redundancy for mailbox access. You need to recommend a solution that ensures that client computers can reconnect to their mailbox within five minutes if Server1 fails. What should you recommend?

- A. Configure cluster continuous replication (CCR).
Implement a file share witness.
- B. Configure a Network Load Balancing cluster that includes Server1 and Server2.
Implement Active Directory-integrated DNS zones.
- C. Configure a database availability group (DAG) that includes Server1 and Server2.
Set the time to live (TTL) for the DNS record.
- D. Configure a database availability group (DAG) that includes Server1 and Server2.
Use the same certificate for both servers.

Answer: C

Question: 77

You have a main office and five branch offices. The offices connect to each other by using a WAN link. An Active Directory site exists for each office. Each site has a separate IP site link to all other sites. The main office site is configured as a hub site. You have an Exchange Server 2010 organization. You discover that messages sent between offices are not routed through the Hub Transport servers in the main office. You need to ensure that all messages sent between offices are routed through the Hub Transport servers in the main office. What should you do?

- A. Change all IP site links to SMTP site links.
- B. Modify the Exchange-specific cost for each site link.
- C. From the Hub Transport servers in each site, create a journal rule.

D. From the Hub Transport servers in each site, create a transport rule.

Answer: B

Explanation:

You can set an Exchange cost on an Active Directory IP site link in Microsoft Exchange Server 2010. By default, Exchange uses the cost assigned to an IP site link for Active Directory replication purposes to compute a routing topology.

Looking for other management tasks related to managing message routing? Check out Managing MessageRouting.

<http://technet.microsoft.com/en-us/library/bb266946.aspx>

Question: 78

You have an Exchange Server 2003 organization. All servers have 32-bit hardware. You plan to transition to Exchange Server 2010 and deploy new Mailbox servers. You need to evaluate the current servers to provide recommendations for the deployment of the new Mailbox servers. What should you include in the evaluation?

A. Number of concurrent connections to Outlook Web App

Number of mailbox databases

Memory utilization

B. Number of concurrent connections to Outlook Web App

RPC latency

Disk I/O latency

C. Number of concurrent MAPI connections

Size of mailbox databases

Number of mailboxes

D. Number of mailboxes

Disk I/O latency

RPC latency

Answer: C

Question: 79

You have an Exchange Server 2010 organization. Users access the internal network by using a server named ISA1 that runs Microsoft Internet Security and Acceleration (ISA) Server. You need to configure mailbox access from the Internet to meet the following requirements:

- Users must be able to download an offline address book (OAB)
- Users must be able to access their mailboxes by using Outlook Anywhere
- Users must be able to access their mailboxes by using Outlook Web App (OWA)
- The solution must minimize administrative overhead

What should you create from ISA1?

A. an access rule for TCP ports 135, 389, and 993

B. an access rule for TCP ports 389, 636, and 1024

C. publishing rules for the OWA, EWS, RPC, Autodiscover, and OAB virtual directories

D. publishing rules for the OWA, Microsoft-Server-ActiveSync, Public, and OAB virtual directories

Answer: C

Question: 80

Your network consists of an Active Directory forest named contoso.com. Contoso.com has an Exchange Server 2010 organization. A subsidiary company has a separate Active Directory forest named fabrikam.com. Fabrikam.com has an Exchange Server 2007 organization. You plan to consolidate both organizations. Your company's consolidation strategy includes the following requirements:

- Support costs must be minimized
- Mailbox access must be easily shared between users
- All e-mail messages must be hosted on Exchange Server 2010 mailbox servers

You need to recommend a solution to meet the requirements of the consolidation strategy. What should you recommend?

- A. Move all recipients from fabrikam.com to contoso.com.
- B. Transition all servers in fabrikam.com to Exchange Server 2010.
- C. In contoso.com, create a resource mailbox for each recipient in fabrikam.com.
- D. Move all computer accounts for the Exchange servers in fabrikam.com to contoso.com. On each server, run Setup.com /M:RecoverServer.

Answer: A

Question: 81

Your network consists of a single Active Directory forest. You have an Exchange Server 2003 organization. You need to create a plan to transition the organization to Exchange Server 2010. The plan must meet the following requirements:

- Ensure that e-mail messages can be sent between all users in the organization
- Ensure that administrators can modify address lists from Exchange Server 2010 servers
- Ensure that users who are moved to Exchange Server 2010 can access all public folders in the organization

What should you include in the plan?

- A. Two Send connectors a sharing policy address lists that use OPATH
- B. Two Send connectors public folder replication new address lists
- C. A two-way routing group connector a sharing policy new address lists
- D. A two-way routing group connector public folder replication address lists that use OPATH

Answer: D

Question: 82

You have an Exchange Server 2010 organization. Your company acquires another company that has an Exchange Server 2010 organization. You need to recommend a solution for the Exchange Server 2010 organization to meet the following requirements:

- All users must be able to view the global address lists (GALs) for both organizations
- All users must be able to view free/busy information for users in both organizations

What should you include in the solution?

- A. Implement Active Directory Federation Services (AD FS).
Run the Microsoft Exchange Inter-Organization Replication tool
- B. Implement Microsoft Identity Lifecycle Manager (ILM) 2007.
Create a two-way cross-forest trust between both organizations
- C. Create a federation trust between both organizations.

Implement Microsoft Identity Lifecycle Manager (ILM) 2007.

Run the New Organization Relationship wizard

D. Create a two-way cross-forest trust between both organizations.

Implement Active Directory Federation Services (AD FS).

Run the Microsoft Exchange Inter-Organization Replication tool

Answer: C

Explanation:

Identity Lifecycle Manager (ILM) 2007 enables IT organizations to reduce the cost of managing the identity and access lifecycle by providing a single view of a user's identity across the heterogeneous enterprise and through the automation of common tasks. ILM 2007 builds on the metadirectory and user provisioning capabilities in Microsoft Identity Integration Server 2003 (MIIS 2003) and adds new capabilities for managing strong credentials such as smartcards with Certificate Lifecycle Manager 2007 (CLM 2007). ILM 2007 provides an integrated approach that pulls together metadirectory, certificate and password management, and user provisioning across Windows® and other enterprise systems. ILM 2007 has two central components, one that includes metadirectory and user provisioning capabilities and another for certificate and smart card management.

Question: 83

You have an Exchange Server 2003 organization. You plan to transition the organization to Exchange Server 2010. You need to recommend a plan that allows the Exchange Server 2003 servers to coexist with Exchange Server 2010 servers. The plan must meet the following requirements:

- Support journaling of e-mail messages that are sent to distribution lists from a mailbox on an Exchange Server 2003 server
- Support journaling of e-mail messages that are sent to distribution lists from a mailbox on an Exchange Server 2010 server

What should you recommend?

A. Implement Personal Archives.

B. Implement Universal Group Membership Caching.

C. Use only Exchange Server 2003 servers for the expansion of distribution groups.

D. Use only Exchange Server 2010 Hub Transport servers for the expansion of distribution groups.

Answer: D

Question: 84

Your network contains a single Active Directory domain. You have an Exchange Server 2010 organization that contains a Hub Transport server named Hub1. Hub1 receives all e-mail messages that are sent to your organization from the Internet. A new company security policy states that domain-joined servers must not be accessible directly from the Internet. You need to create a message hygiene solution to meet the following requirements:

- Comply with the new security policy
- Minimize the amount of spam that is delivered to the internal Exchange servers in the organization

What should you do first?

A. Deploy an Edge Transport server, and then configure EdgeSync synchronization.

B. Deploy a new Hub Transport server, and then install the anti-spam transport agents.

C. Deploy a new Hub Transport server, and then deploy Active Directory Federation Services (AD FS).

D. Deploy an Edge Transport server, and then disable Active Directory Lightweight Directory Services (AD LDS).

Answer: A

Question: 85

Your network contains three Active Directory sites named Site1, Site2, and Site3. Users can only access Site1 from the Internet. In each site, you plan to deploy a Mailbox server and a Hub Transport server. You need to plan the deployment of Exchange servers to meet the following requirements:

- Ensure that Exchange ActiveSync and Outlook Anywhere clients can connect to their Mailboxes from the Internet
- Minimize hardware costs

What should you include in your plan?

- A. In Site1, deploy one Client Access server.
- B. In each site, deploy one Client Access server.
- C. In Site1, deploy one Client Access server and one Edge Transport server.
- D. In each site, deploy one Client Access server and one Edge Transport server.

Answer: B

Question: 86

You have an Exchange Server 2010 organization named contoso.com. Your company plans to provide business continuity services for a company named Fabrikam. Fabrikam has an Exchange Server 2007 organization and uses the fabrikam.com SMTP domain. You need to configure your organization to queue and relay all e-mail messages sent to fabrikam.com from the Internet. What should you do?

- A. Create a new remote domain, and then modify the mail exchange (MX) record for the fabrikam.com public DNS domain.
- B. Create a new remote domain, and then modify the mail exchange (MX) records for the contoso.com public DNS domain.
- C. Create a new External Relay Accepted Domain, and then modify the mail exchange (MX) records for the contoso.com public DNS domain.
- D. Create a new External Relay Accepted Domain, and then modify the mail exchange (MX) records for the fabrikam.com public DNS domain.

Answer: D

Question: 87

You have an Exchange Server 2010 organization. You need to recommend a mailbox storage management solution for your organization to meet the following requirements:

- Apply quota limits for users by department
- Automatically apply quota limits for new users

What should you recommend?

- A. A storage group for each department.
- B. A mailbox database for each department.
- C. An organizational unit for each department.
- D. A managed folder mailbox policy for each department.

Answer: B

Question: 88

Your company has a Windows Server 2003 Active Directory forest that contains a single domain. The functional level of the forest is set to Windows 2000 native. You have an Exchange organization that contains Exchange Server 2003 Service Pack 2 (SP2) and Exchange Server 2007 Service Pack 2 (SP2) servers. You plan to transition the organization to Exchange Server 2010. You need to prepare Active Directory for the installation of the first Exchange Server 2010 server. What should you do?

- A. Set the functional level of the forest to Windows Server 2003.
- B. Prepare the legacy Exchange permissions from the Exchange Server 2010 installation source files.
- C. Add the Exchange Server 2010 schema extensions by using the Exchange Server 2010 installation source files.
- D. Upgrade all domain controllers to Windows Server 2008, and then set the functional level of the domain to Windows Server 2008.

Answer: A

Question: 89

You have an Exchange Server 2010 organization. All users connect to their mailboxes by using Microsoft Office Outlook 2007 Service Pack 2 (SP2) and Windows 7. Your company's security administrators deploy Outlook Protection Rules. You need to recommend a client connection solution for the organization to ensure that Outlook Protection Rules can be used. What should you recommend?

- A. Upgrade all client computers to Outlook 2010.
- B. Instruct all users to connect to Outlook Web App (OWA).
- C. Instruct all users to install the Rights Management Service (RMS) client.
- D. Instruct all users to install the Secure/Multipurpose Internet Mail Extensions (S/MIME) control.

Answer: A

Explanation:

Outlook Protection Rules

Although users can apply IRM protection to messages manually before they send them, they may occasionally neglect to do so for messages that should be protected. Outlook protection rules in Exchange Server 2010 can help in protecting your organization from information leakage by applying IRM protection to messages automatically when they are sent from Outlook 2010. When IRM protection is applied to a message, any attachments in supported file formats have IRM protection applied to them as well. Because Outlook protection rules are applied within Outlook, the client must be running Outlook 2010 because this is the only version of Outlook that can use Outlook protection rules.

[http://mscerts.programming4.us/application_server/exchange%20%20server%202010%20%20designing%20and%20implementing%20ad%20rms%20integration%20\(part%202\)%20-%20ad%20rms%20and%20exchange%20server%202010.aspx](http://mscerts.programming4.us/application_server/exchange%20%20server%202010%20%20designing%20and%20implementing%20ad%20rms%20integration%20(part%202)%20-%20ad%20rms%20and%20exchange%20server%202010.aspx)

Question: 90

You have an Exchange Server 2010 organization. You plan to provide users with the ability to schedule meetings. You

need to recommend a scheduling solution that meets the following requirements:

- Ensures that users can schedule conference rooms for meetings
 - Ensures that conference room owners can change the settings of meetings scheduled by users
- What should you include in the solution?

- A. Managed Folder Assistant
- B. public folders
- C. resource mailboxes
- D. room list distribution groups

Answer: C

Question: 91

You have an Exchange Server 2010 organization. You plan to delegate administration of the organization. You have a group named Technicians that contains all the level-two technicians in the organization. You need to ensure that the Technicians group can manage the properties of all the mailbox databases. The solution must minimize the number of permissions assigned to the Technicians group. Which management role should you assign to the Technicians group?

- A. Help Desk
- B. Organization Management
- C. Recipient Management
- D. Server Management

Answer: D

Explanation:

Administrator who are the members of server management role group have administrative access to Exchange 2010 server configuration. They don't have access to administer Exchange 2010 recipient configuration.

Question: 92

You have an Exchange Server 2010 organization. Your company's security policy states that users must not be able to encrypt e-mail messages by using Outlook Web App (OWA). You need to recommend a client access solution that meets the requirements of the security policy. What should you include in the solution?

- A. managed folder mailbox policies
- B. multiple OWA virtual directories
- C. OWA segmentation
- D. WebReady Document Viewing

Answer: C

Explanation:

Segmentation lets you enable and disable many features in Outlook Web App. You can manage segmentation using the EMC or the Shell. By default, segmentation changes take effect after 60 minutes of inactivity for users who are signed in to Outlook Web App, or when a user signs in to Outlook Web App. To force the changes to take effect immediately, restart Internet Information Services (IIS) by running the command iisreset/noforce on the Client Access server.

S/MIME	<i>SMimeEnabled</i>	If it's enabled, this option lets users download the S/MIME control for Outlook Web Ap http://technet.microsoft.com/en-us/library/bb123962.aspx
--------	---------------------	---

Question: 93

You have an Exchange Server 2010 organization that contains five Hub Transport servers, five Mailbox servers and one Edge Transport server. You need to provide a solution to ensure that users can prevent legitimate inbound e-mail messages from being classified as spam. What should you do?

- A. Enable sender filtering
- B. Enable Sender ID filtering
- C. Configure a custom MailTip
- D. Configure safelist aggregation

Answer: D

Explanation:

Safelist Aggregation

In Microsoft Exchange Server 2007, the term safelist aggregation refers to a set of anti-spam functionality that is shared across Microsoft Office Outlook and Microsoft Exchange. This functionality collects data from the antispam Safe Recipients Lists or Safe Senders Lists and contact data that Outlook users configure, and makes this data available to the anti-spam agents on the computer that has the Edge Transport server role installed. Safelist aggregation can help reduce the instances of false-positives in anti-spam filtering that is performed by the Edge Transport server. When you configure safelist aggregation, the Content Filter agent passes safe email messages to the organization's mailbox without additional processing. E-mail messages that Outlook users receive from contacts that those users have added to their Outlook Safe Recipients List or Safe Senders List or have trusted are identified by the Content Filter agent as safe. An Outlook contact is a person, inside or outside the user's organization, about whom the user can save several types of information, such as e-mail and street addresses, telephone and fax numbers, and Web page URLs.

Safelist aggregation can help reduce the instances of false-positives in anti-spam filtering that is performed by the Edge Transport server. A false-positive is a positive test or filter result that is in a subject or body of data that does not possess the attribute for which the filter or test is being conducted. In the context of spam filtering, a false-positive occurs when a spam filter incorrectly identifies a message from a legitimate sender as spam.

For organizations that filter hundreds of thousands of messages from the Internet every day, even a small percentage of false-positives means that users might not receive many messages that were identified incorrectly as spam and therefore were quarantined or deleted.

Safelist aggregation can be the most effective way to reduce false-positives. Outlook 2003 and the next release of Outlook, which is included in Office 2007, let users create Safe Senders Lists. Safe Senders Lists specify a list of domain names and e-mail addresses from which the Outlook user wants to receive messages. By default, e-mail addresses in Outlook Contacts and in the Exchange Server global address list are included in this list. By default, Outlook adds all external contacts to which the user sends mail to the Safe Senders List.

Information Stored in the Outlook User's Safelist Collection

A safelist collection is the combined data from the user's Safe Senders List, Safe Recipients List, Blocked Senders List, and external contacts. This data is stored in Outlook and in the Exchange mailbox. The following types of information are stored in an Outlook user's safelist collection:

Safe senders and safe recipients - The P2 From: field of the e-mail message indicates a sender. The To: field of the e-mail message indicates a recipient. Safe senders and safe recipients are represented by full Simple Mail Transfer Protocol (SMTP) addresses, such as masato@contoso.com. Outlook users can add senders and recipients to their safe lists.

Safe domain - The domain is the part of an SMTP address that follows the @ symbol. For example, contoso.com is the

domain in the masato@contoso.com address. Outlook users can add sending domains to their safe lists.

External contacts - Two types of external contacts can be included in the safelist aggregation. The first type of external contact includes contacts to whom Outlook users have sent mail. This class of contact is added to the Safe Senders List only if an Outlook user selects the corresponding option in the Junk E-mail settings in Outlook 2003 or Exchange Server 2007.

The second type of external contact includes the users' Outlook contacts. Users can add or import these contacts into Outlook. This class of contact is added to the Safe Senders List only if an Outlook user selects the corresponding option in the Junk E-mail Filter settings in Outlook 2003 or Outlook 2007.

How Exchange Uses the Safelist Collection

The safelist collection is stored on the user's mailbox server. A user can have up to 1,024 unique entries in a safelist collection.

In earlier versions of Exchange Server, the user's mailbox server accessed the safelist collection during spam filtering to allow e-mail from senders on the Safe Senders List to pass through.

In Exchange Server 2007, the safelist collection is stored on the user's mailbox, but you can push it to the Active Directory directory service, where the safelist collection is stored on each user object. When the safelist collection is stored on the user object in Active Directory, the safelist collection is aggregated with the antispam functionality of Exchange Server 2007 and is optimized for minimized storage and replication so that the Edge Transport server can process the safelist aggregation. The Content Filter agent on the Edge Transport server can access the safelist collection for each recipient. EdgeSync replicates the safelist collection to the Active Directory Application Mode (ADAM) instance on the Edge Transport server.

Note Safelist collection entries are one-way hashed (SHA-256) before they are stored in Active Directory. This minimizes storage and replication size, and it renders the safelist collections unreadable by malicious users.

Hashing of Safelist Collection Entries

The safelist collection entries are hashed (SHA-256) one way before they are stored as array sets across two user object attributes, msExchangeSafeSenderHash and msExchangeSafeRecipientHash, as a binary large object. When data is hashed, an output of fixed length is produced; the output is also likely to be unique. For hashing of safelist collection entries, a 4-byte hash is produced. When a message is received from the Internet, Exchange Server hashes the sender address and compares it to the hashes that are stored on behalf of the Outlook user to whom the message was sent. If an inbound hash matches, the message bypasses content filtering.

One-way hashing of safelist collection entries performs the following important functions:

It minimizes storage and replication space. Most of the time, hashing reduces the size of the data that is hashed. Therefore, saving and transmitting a hashed version of a safelist collection entry conserves storage space and replication time. For example, a user who has 200 entries in his or her safelist collection would create about 800 bytes of hashed data that is stored and replicated in Active Directory.

It renders user safelist collections unusable by malicious users. Because one-way hash values are impossible to reverse-engineer into the original SMTP address or domain, the safelist collections do not yield usable e-mail addresses for malicious users who might compromise an Edge Transport server.

Enabling Safelist Aggregation

You can enable safelist aggregation by running the Exchange Management Shell Update-SafeList command on a user's mailbox. The Update-SafeList command reads the safelist collection from the user's mailbox, hashes each entry, sorts the entries for easy search, and then converts the hash to a binary attribute. Finally, the Update-SafeList command compares the binary attribute that was created to any value that is stored on the attribute. If the two values are identical, the Update-SafeList command does not update the user attribute value with the safelist aggregation data. If the two attribute values are different, the Update-SafeList command updates the safelist aggregation value. This logic, where the binary values are compared before updates, is intended to significantly minimize resource use on Active Directory replication. Periodic use of Update-Safelist ensures that the most up-to-date safelist aggregation is in Active Directory.

To make the safelist aggregation data in Active Directory available to Edge Transport servers in the perimeter network, you must install and configure the EdgeSync tool so that the safelist aggregation data is replicated to the Active Directory Application Mode (ADAM) instance on the Edge server.

Question: 94

You have an Exchange Server 2010 organization. You plan to delegate Exchange administrative rights to some users in the organization. You need to recommend a solution that tracks all changes made to the Exchange organization. What should you include in the solution?

- A. administrator audit logging
- B. circular logging
- C. diagnostic logging
- D. Windows Security Auditing

Answer: A

Explanation:

You can use administrator audit logging in Microsoft Exchange Server 2010 to log when a user or administrator makes a change in your organization. By keeping a log of the changes, you can trace changes to the person who made the change, augment your change logs with detailed records of the change as it was implemented, comply with regulatory requirements and requests for discovery, and more.

By default, audit logging is enabled in new installations of Microsoft Exchange Server 2010 Service Pack 1 (SP1).

Question: 95

You have an Exchange Server 2010 organization that contains Windows Mobile 5.0 devices. Your company plans to replace all mobile devices with Windows Mobile 6.5 devices. You need to identify which users accessed their mailboxes by using Windows Mobile 5.0 devices in the past month. What should you do?

- A. Create a Data Collector Set.
- B. Install and run the Exchange Server User Monitor (ExMon).
- C. Export and review the Internet Information Services (IIS) logs.
- D. Enable User Agent logging, and then review the agent logs.

Answer: C

Question: 96

You have an Exchange Server 2010 organization. You need to recommend a solution that prevents the permanent deletion of e-mail messages from the mailboxes of employee who have been dismissed from the company. What should you recommend?

- A. Implement managed folders.
- B. Implement a legal hold for each mailbox.
- C. Implement a Retention Policy for each mailbox.
- D. Implement an Outlook Protection Rule for each mailbox.

Answer: B

Question: 97

You have an Exchange Server 2010 organization. The organization contains a global security group named Group1. You plan to deploy a monitoring solution for the Exchange servers in your organization. You need to recommend a solution that allows members of Group1 to monitor the performance of Exchange Server 2010 servers. Your solution must prevent members of Group1 from modifying the configurations of the Exchange Server 2010 organization. What should you include in the solution?

- A. Delegation of Control Wizard
- B. Federation Trusts
- C. Reliability Monitor
- D. Role Based Access Control (RBAC)

Answer: D

Explanation:

Role Based Access Control (RBAC) is the new permissions model in Microsoft Exchange Server 2010. With RBAC, you don't need to modify and manage access control lists (ACLs), which was done in Exchange Server 2007. ACLs created several challenges in Exchange 2007, such as modifying ACLs without causing unintended consequences, maintaining ACL modifications through upgrades, and troubleshooting problems that occurred due to using ACLs in a nonstandard way. RBAC enables you to control, at both broad and granular levels, what administrators and end-users can do. RBAC also enables you to more closely align the roles you assign users and administrators to the actual roles they hold within your organization. In Exchange 2007, the server permissions model applied only to the administrators who managed the Exchange 2007 infrastructure. In Exchange 2010, RBAC now controls both the administrative tasks that can be performed and the extent to which users can now administer their own mailbox and distribution groups.

RBAC has two primary ways of assigning permissions to users in your organization, depending on whether the user is an administrator or specialist user, or an end-user: management role groups and management role assignment policies. Each method associates users with the permissions they need to perform their jobs. A third, more advanced method, direct user role assignment, can also be used

For further reading see:

<http://technet.microsoft.com/en-us/library/dd298183.aspx>

Question: 98

Your company has a main office and 10 branch offices. You have an Exchange Server 2010 organization. All Exchange servers are installed on virtual machines. You need to create a monitoring plan for the Exchange servers that meets the following requirements:

- Identify Exchange server errors
- Provide alerts when Exchange services are stopped
- Produce statistical analysis and reporting

Which tool should you include in the plan?

- A. Microsoft System Center Service Manager
- B. Microsoft System Center Operations Manager
- C. Microsoft System Center Configuration Manager
- D. Microsoft System Center Virtual Machine Manager

Answer: B

Explanation:

System Center Operations Manager 2007 R2, Microsoft's end-to-end service-management product, is your best

choice for Windows environments. It works seamlessly with Microsoft infrastructure servers, such as Windows Server, and application servers, such as Microsoft Exchange, helping you to increase efficiency while enabling greater control of the IT environment.

<http://www.microsoft.com/en-us/server-cloud/system-center/operations-manager.aspx>

Question: 99

Your network consists of an Active Directory domain that contains the domain controllers shown in the following table.

Site	Server	Role	Operating System	Platform
Site1	Server1	Global catalog	Windows Server 2008 Service Pack 2 (SP2)	x64
Site2	Server2	Domain controller	Windows Server 2008	x86
	Server3	Read-only domain controller	Windows Server 2008	x64

You plan to deploy an Exchange Server 2010 server in each site. You need to recommend changes to the domain controllers to support the installation of Exchange Server 2010. What should you do?

- A. Enable Server2 as a global catalog server.
- B. Enable Server3 as a global catalog server.
- C. Upgrade Server2 to Windows Server 2008 SP2 (x64).
- D. Upgrade Server3 to Windows Server 2008 SP2 (x64).

Answer: A

Explanation:

Exchange Server needs to have Global Catalog Servers in each site that has Exchange Servers deployed

Question: 100

Your company has a main office and 50 branch offices. Each office is configured as an Active Directory site. Each branch office site contains a domain controller. The main office site contains all the global catalog servers in the forest. Each branch office contains a WAN link that connects to the main office. You need to plan the deployment of new Mailbox servers to meet the following requirements:

- Ensure that users in the branch offices can access their mailboxes if their local domain controller fails
- Deploy the minimum number of Exchange servers

What should you include in the plan?

- A. One Mailbox server in each office and global catalog servers in each branch office
- B. One Mailbox server in each office and Universal Group Membership Caching in each branch office
- C. One Mailbox server in each branch office only
- D. Multiple Mailbox servers in the main office only

Answer: D

Explanation:

This is an interesting question however if you break it down it starts to make sense Main Office has the Global Catalog Servers - not the Branch Offices Branch Offices connect to the main office via a Wan Link While each branch office

does have a domain controller they are not Global Catalog Servers. Further there are 50 branch offices so it makes no sense to deploy a mailbox server in each branch office or to have 50 Global Catalog Servers. The best answer is D as this would meet the requirement of deploying the least amount of Exchange Servers.

Question: 101

Your Exchange Server 2010 organization contains two Hub Transport servers in a single site.

The organization receives all e-mail sent to a SMTP domain named contoso.com. Your company purchases another company that uses a SMTP domain named fabrikam.com. You plan to manage message hygiene for both SMTP domains. You need to recommend changes to the organization to support the planned deployment. The solution must prevent e-mail sent to fabrikam.com from being delivered to your internal organization. What should you recommend?

- A. Deploy a new Hub Transport server, and then create remote domains.
- B. Deploy a new Hub Transport server, and then configure transport rules.
- C. Deploy an Edge Transport server, and then create accepted domains.
- D. Deploy an Edge Transport server, and then configure a federation trust.

Answer: C

Explanation:

The correct answer is C - while a hub transport can provide message hygiene for this question deploying Edge Transport Servers is the proper solution

Question: 102

You have an Exchange Server 2010 organization. You need to recommend a storage solution that meets the following requirements:

- Provides users with an alternate location for storing e-mail messages
- Provides users with access to the alternate location by using Outlook Web App (OWA)

What should you recommend?

- A. journal rules
- B. managed folders
- C. personal archives
- D. personal folders (.pst)

Answer: C

Question: 103

You have an Exchange Server 2010 organization. Your company's legal department sends compliance e-mail messages by adding recipients to the blind carbon copy (Bcc) field. The company's compliance policy includes the following requirements:

- All e-mail messages sent to external recipients must be archived in a central repository
- Compliance officers must be able to identify all the recipients of archived e-mail messages

You need recommend a solution to meet the compliance policy requirements. What should you recommend?

- A. journal rules
- B. message tracking

- C. Personal Archives
- D. transport rules

Answer: A

Explanation:

Journaling is the ability to record all communications, including e-mail communications, in an organization for use in the organization's e-mail retention or archival strategy. To meet an increasing number of regulatory and compliance requirements, many organizations must maintain records of communications that occur when employees perform daily business tasks.

Archiving refers to backing up the data, removing it from its native environment, and storing it elsewhere, therefore reducing the strain of data storage. You may use Exchange journaling as a tool in your e-mail retention or archival strategy.

Although journaling may not be required by a specific regulation, compliance may be achieved through journaling under certain regulations. For example, corporate officers in some financial sectors may be held liable for the claims made by their employees to their customers. To verify that the claims are accurate, a corporate officer may set up a system where managers review some part of employee-to-client communications regularly. Every quarter, the managers verify compliance and approve their employees' conduct. After all managers report approval to the corporate officer, the corporate officer reports compliance, on behalf of the company, to the regulating body. In this example, e-mail messages might be one type of the employee-to-client communications that managers must review; therefore, journaling can be used to collect all e-mail messages sent by client-facing employees. Other client communication mechanisms may include faxes and telephone conversations, which may also be subject to regulation. The ability to journal all classes of data in an enterprise is a valuable functionality of the IT architecture.

Question: 104

You have an Exchange Server 2010 organization for a company named Contoso, Ltd. Contoso has the following security policy:

- Messages that contain the word budget cannot be sent to external recipients
 - Messages that contain the name Northwind Traders must be sent to the legal department automatically
- You need to recommend a solution to meet the security policy. What should you recommend?

- A. Create two transport rules.
- B. Create two message classifications.
- C. Create one transport rule and configure a legal hold.
- D. Create one message classification and configure a legal hold.

Answer: A

Question: 105

You have an Exchange Server 2010 organization. You have a group named Help Desk that contains all the help desk users in the organization. You need to ensure that the Help Desk group can manage all the mailboxes and mail-enabled contacts in the organization. The solution must minimize the number of permissions assigned to the Help Desk group. Which management role should you assign to the Help Desk group?

- A. Mail Recipients
- B. Mail Recipient Creation
- C. Organization Client Access
- D. Recipient Policies

Answer: A

Explanation:

The Mail Recipients management role enables administrators to manage existing mailboxes, mail users, and mail contacts in an organization. This role can't create these recipients. Use the Mail Recipient Creation role to create them.

This role type doesn't enable you to manage mail-enabled public folders or distribution groups. Use the following roles to manage these objects:

Mail Enabled Public Folders Role

Distribution Groups Role

<http://technet.microsoft.com/en-us/library/dd876911.aspx>

Question: 106

You have an Exchange Server 2010 organization. You need to plan a message hygiene solution that meets the following requirements:

- Spoofing must be minimized
- Open SMTP relays must be added to IP block lists automatically

What should you include in the plan?

- A. Sender ID filtering and recipient filtering
- B. Sender ID filtering and sender reputation
- C. sender filtering and recipient filtering
- D. sender reputation and recipient filtering

Answer: B

Explanation:

Sender ID is intended to combat the impersonation of a sender and a domain, a practice that's frequently called spoofing. A spoofed mail is an e-mail message that has a sending address that was modified to appear as if it originates from a sender other than the actual sender of the message.

Spoofed mails typically contain a From: address that purports to be from a certain organization. In the past, it was relatively easy to spoof the From: address, in both the SMTP session, such as the MAIL FROM: header, and in the RFC 822 message data, such as From: "Masato Kawai" masato@contoso.com, because the headers weren't validated.

Sender reputation evaluates several sender characteristics to calculate an SRL. Among the characteristics that sender reputation evaluates are the results of a test for open proxy servers. Frequently, spammers route messages through open proxy servers on the Internet. By routing spam through open proxy servers, spammers can send messages that appear to originate from a different server than their own.

When sender reputation calculates an SRL, sender reputation tries to connect to the sender's originating IP address by using a variety of common proxy protocols, such as SOCKS4, SOCKS5, HTTP, Telnet, Cisco, and Wingate. Sender reputation formats a protocol-specific request in an attempt to connect back to the Edge Transport server from the open proxy server by using an SMTP request. If an SMTP request is received from the proxy server, sender reputation verifies that the proxy server is an open proxy server and adjusts the SRL rating according to this result. By default, detection of open proxy servers is enabled on sender reputation.

<http://technet.microsoft.com/en-us/library/bb124512.aspx>

Question: 107

Your network contains an Exchange Server 2010 server. You need to plan a mailbox sharing solution for the

organization to meets the following requirements:

- Ensure that assistants can read and modify the e-mail messages of their managers
- Ensure that assistants can impersonate their managers when they send e-mail messages

What should you include in the plan?

- A. Full Access and Send As permissions
- B. Full Access and send on behalf of permissions
- C. Role Based Access Control (RBAC) assignments and Send As permissions
- D. Role Based Access Control (RBAC) assignments and send on behalf of permissions

Answer: A

Question: 108

You have an Exchange Server 2010 organization named contoso.com. The organization contains two Client Access servers named CAS1 and CAS2 that are in a Client Access server array. All internal and external users connect to their mailboxes by using mail.contoso.com. You need to install a certificate on the Client Access servers to meet the following requirements:

- Support 500 client computers that are not joined to the Active Directory domain
- Support clients that use Microsoft Office Outlook in Cached Exchange Mode, Autodiscover, and Exchange ActiveSync
- Minimize client and user support costs

What should you do?

- A. From a trusted third-party certification authority (CA), generate a certificate request that contains the mail.contoso.com and Autodiscover names.
- B. From a trusted third-party certification authority (CA), generate a certificate request that contains the CAS1.contoso.com and CAS2.contoso.com names.
- C. From an internal Active Directory-integrated certification authority (CA), generate a certificate request that contains the mail.contoso.com and Autodiscover names.
- D. From an internal Active Directory-integrated certification authority (CA), generate a certificate request that contains the CAS1.contoso.com and CAS2.contoso.com names.

Answer: A

Question: 109

You have an Exchange Server 2010 organization. Your company has a relationship with another company. The partner company has an Exchange Server 2010 organization. You need to recommend a security solution to meet the following requirements:

- Ensure that all e-mail delivery between your servers and the partner company's servers is encrypted
- Ensure that all communication between your servers and the partner company's servers is authenticated

What should you include in the solution?

- A. Active Directory Rights Management Services (AD RMS)
- B. Domain Security
- C. Forms-based Authentication
- D. Secure/Multipurpose Internet Mail Extensions (S/MIME)

Answer: B

Explanation:

Domain Security refers to the set of functionality in Microsoft Exchange Server 2010 and Microsoft Office Outlook 2007 that provides a relatively low-cost alternative to S/MIME or other message-level security solutions. The purpose of the Domain Security feature set is to provide administrators a way to manage secured message paths over the Internet with business partners. After these secured message paths are configured, messages that have successfully traveled over the secured path from an authenticated sender are displayed to users as Domain Secured in the Outlook and Microsoft Office Outlook Web App interface. Domain Security uses mutual Transport Layer Security (TLS) authentication to provide session-based authentication and encryption. Mutual TLS authentication differs from TLS as it's usually implemented. Typically, when TLS is implemented, the client verifies that the connection securely connects to the intended server by validating the server's certificate. This is received as part of TLS negotiation. In this scenario, the client authenticates the server before the client transmits data. However, the server doesn't authenticate the session with the client. With mutual TLS authentication, each server verifies the connection with the other server by validating a certificate that's provided by that other server. In this scenario, where messages are received from external domains over verified connections in an Exchange 2010 environment, Outlook 2007 displays a Domain Secured icon.

<http://technet.microsoft.com/en-us/library/bb124392.aspx>

Question: 110

Your company has an Active Directory forest named contoso.com. You plan to deploy an Exchange Server 2010 organization that will contain two servers. Each server will have the Client Access server role, the Hub Transport server role, and the Mailbox server role installed. You plan to add both servers to a database availability group (DAG). You need to recommend a high-availability solution for the Client Access server role. Your solution must ensure that users are not prompted to authenticate if a Client Access server becomes unavailable. What should you recommend?

- A. Create and configure a Client Access server array, and then install a hardware load balancer.
- B. Create and configure a Client Access server array, and then install Windows Network Load Balancing on both servers.
- C. Deploy Microsoft Internet Security and Acceleration (ISA) Server 2006, and then implement DNS round robin.
- D. Deploy Microsoft Internet Security and Acceleration (ISA) Server 2006, and then install Windows Network Load Balancing.

Answer: A

Explanation:

A is the correct answer for this question.

While it is possible to install the Windows Network Load Balancing for a client access array that solution will not work for this question.

Windows Network Load Balancing

Windows Network Load Balancing (WNLB) is the most common software load balancer used for Exchange servers. There are several limitations associated with deploying WNLB with Microsoft Exchange.

WNLB can't be used on Exchange servers where mailbox DAGs are also being used because WNLB is incompatible with Windows failover clustering. If you're using an Exchange 2010 DAG and you want to use WNLB, you need to have the Client Access server role and the Mailbox server role running on separate servers.

Due to performance issues, we don't recommend putting more than eight Client Access servers in an array that's load balanced by WNLB.

WNLB doesn't detect service outages. WNLB only detects server outages by IP address. This means if a particular Web service, such as Outlook Web App, fails, but the server is still functioning, WNLB won't detect the failure and will still route requests to that Client Access server. Manual intervention is required to remove the Client Access server experiencing the outage from the load balancing pool.

WNLB configuration can result in port flooding, which can overwhelm networks.

Because WNLB only performs client affinity using the source IP address, it's not an effective solution when the source IP pool is small. This can occur when the source IP pool is from a remote network subnet or when your organization is using network address translation.

<http://technet.microsoft.com/en-us/library/ff625247.aspx>

Question: 111

You have an Exchange Server 2010 organization. The network contains two Mailbox servers that are configured in a database availability group (DAG). You plan to implement a disaster recovery solution. You need to recommend a solution that ensures that the active mailbox database copy is unaffected by the backup process. You want to achieve this goal while minimizing costs. What should you recommend?

- A. Windows Server Backup
- B. Network Attached Storage (NAS) snapshots
- C. Microsoft System Center Configuration Manager
- D. Microsoft System Center Data Protection Manager

Answer: D

Explanation:

Data Protection Manager 2010 (DPM 2010) is part of the System Center family of management products from Microsoft. It delivers unified data protection for Windows servers such as SQL Server, Exchange, SharePoint, Virtualization and file servers -- as well as Windows desktops and laptops.

Question: 112

You deploy multiple Mailbox servers. Each Mailbox server contains a copy of a mailbox database named DB1. You need to recommend a solution that allows administrators to remove corrupt messages that have been replicated before the corrupt messages are applied to each copy of DB1. What should you recommend?

- A. Modify log truncation.
- B. Enable circular logging.
- C. Implement lagged copies.
- D. Configure shadow redundancy.

Answer: C

Explanation:

Using Replay Lag and Truncation Lag Options

Mailbox database copies support the use of a replay lag time and a truncation lag time, both of which are configured in minutes. Setting a replay lag time enables you to take a database copy back to a specific point in time. Setting a truncation lag time enables you to use the logs on a passive database copy to recover from the loss of log files on the active database copy. Because both of these features result in the temporary build-up of log files, using either of them will affect your storage design.

<http://technet.microsoft.com/en-us/library/dd335158.aspx>

Question: 113

You have an Exchange Server 2010 organization. The organization contains two servers named Server1 and Server2. Server1 and Server2 have the Mailbox server role and the Hub Transport server role installed. Server 1 and Server2

are members of a database availability group (DAG). You need to plan the deployment of Client Access servers to meet the following requirements:

- Users must be able to access their mailboxes if a single server fails
- Users must not attempt to connect to a failed server

What should you include in your plan?

A. On Server1 and Server2, install the Client Access server role.

Implement failover clustering.

B. On Server1 and Server2, install the Client Access server role.

Configure network interface card (NIC) teaming on each server.

C. Deploy two new Client Access servers.

Implement load balancing by using DNS round robin.

Create a Client Access server array.

D. Deploy two new Client Access servers.

Implement load balancing by using a Windows Network Load Balancing cluster.

Create a Client Access server array.

Answer: D

Explanation:

Correct Answer is D.

As the Client Access role has been deployed on separate servers you can use the Windows Network and Load Balancing feature. WNLB, you need to have the Client Access server role and the Mailbox server role running on separate servers.

<http://technet.microsoft.com/en-us/library/ff625247.aspx>

Question: 114

You have an Exchange Server 2003 organization. All users connect to their mailboxes by using Microsoft Office Outlook. You start to transition the organization to new Exchange Server 2010 servers. The new servers are on a secured subnet that is separated by a firewall. You will move half of the mailboxes to the new servers. Client Access servers and Mailbox servers are on the secured subnet. Client computers on the network can access the Client Access servers. You need to recommend a solution that allows users to connect to Public Folders by using Outlook or Outlook Web App (OWA).

- A. Public Folder referrals and forms-based authentication
- B. Public Folder referrals and HTTP connections to the Mailbox servers
- C. Public Folder replicas and MAPI connections to the Mailbox servers
- D. Public Folder replicas and WebReady Document Viewing

Answer: C

Question: 115

Your network consists of an Active Directory forest that contains two sites named Site1 and Site2. From the Internet, users can only access servers in Site1. You have an Exchange Server 2007 organization. Each site contains servers that run the Client Access server role, the Mailbox server role, and the Hub Transport server role. You plan to transition the organization to Exchange Server 2010. You need to recommend the server role that you must transition first to Exchange Server 2010. Your solution must provide the least amount of downtime for users in the organization. Which servers should you transition first?

- A. the Client Access servers in Site1
- B. the Client Access servers in Site2
- C. the Hub Transport servers in Site1
- D. the Hub Transport servers in Site2

Answer: A

Question: 116

Your network contains two Active Directory sites named Site1 and Site2. Only Site1 can be accessed from the Internet. You have an Exchange Server 2010 organization. You deploy a Client Access server in Site1 and enable Windows Integrated Authentication for Outlook Web App (OWA). In Site2, you deploy a Mailbox server and a Client Access server. You need to configure the Exchange organization to meet the following requirements:

- Allow users to access their mailboxes from the Internet by using OWA
- Prevent authentication prompts from displaying when users connect to OWA by using domain- joined computers that are connected to the internal network

What should you do?

- A. Modify the Exchange virtual directory on the Client Access server in Site1.
- B. Modify the Exchange virtual directory on the Client Access server in Site2.
- C. Modify the OWA virtual directory on the Client Access server in Site1.
- D. Modify the OWA virtual directory on the Client Access server in Site2.

Answer: D

Explanation:

As only site 1 has internet you need to modify the owa virtual directory on Site 2.

Question: 117

Your network contains a single Active Directory forest. The forest contains two domain trees named contoso.com and fabrikam.com. You have an Exchange Server 2010 organization. The e-mail addresses for the organization are configured as shown in the following table. You need to ensure that all outbound e-mail messages from fabrikam.com appear to originate from contoso.com. Users in contoso.com must be able to send e-mail messages to users in fabrikam.com by using the address format alias@fabrikam.com. What should you do first?

- A. Deploy an Edge Transport server.
- B. Deploy a Microsoft Internet Security and Acceleration (ISA) server.
- C. Modify the accepted domain entry for contoso.com.
- D. Modify the accepted domain entry for fabrikam.com.

Answer: A

Explanation:

A is the correct answer as you will need to do an address rewrite to make email appear that it has originated from contoso.com. This can only be done with the Edge Transport Server

Question: 118

A corporate environment will include Exchange Server 2010. You need to recommend a solution that allows point-in-time recovery of the mailbox databases. What should you recommend?

- A. Disable circular logging.
- B. Configure the transport dumpster.
- C. Use lagged database copies.
- D. Use highly available database copies.

Answer: C

Explanation:

Point-in-time database snapshot

If a past point-in-time copy of mailbox data is requirement for your organization, Exchange provides the ability to create a lagged copy in DAG environment. This can be useful in the rare event that there's a logical corruption that replicates across the databases in the DAG, resulting in a need to return to a previous point in time. It may also be useful if an administrator accidentally deletes mailboxes or user data. Recovery from a lagged copy ton be faster than restoring from a backup because lagged copies don't require a time-consuming copy process from the backup server to the Exchange server. This can significantly lower total cost of ownership by reducing end-user downtime.

Question: 119

A corporate environment includes Exchange Server 2010. A full backup of the Exchange Server mailbox databases is performed nightly. The databases and transaction logs in the environment are described in the following table.

Name	Database volume size	Transaction log volume size
DB01	100GB	20GB
DB02	150GB	30GB

You need to recommend the minimum size for a recovery volume that will accommodate recovering the most recent data in the event of a logical database corruption of a single mailbox database. What should you recommend?

- A. 180 GB
- B. 150 GB
- C. 250 GB
- D. 120 GB

Answer: A

Question: 120

A corporate environment includes Exchange Server 2010. The Exchange Server environment includes one Mailbox server, one Client Access server, and one Hub Transport server. One Edge Transport server resides in the perimeter network. You are designing a disaster recovery solution for the Edge Transport server. The solution must provide the ability to perform the following tasks:

- Restore the Edge Transport server configuration.
- Restore log files and transport queue databases.
- Backup and restore only the minimum amount of data.

You need to recommend a solution that meets the requirements.

What should you recommend?

- A. Export the Edge Transport server configuration by using the ExportEdgeConfig.ps1 script. Perform a system state backup of the Edge Transport server and back up the exported server configuration.
- B. Export the Edge Transport server configuration by using the ExportEdgeConfig.ps1 script. Perform a system state backup of a domain controller and back up the exported server configuration.
- C. Perform a system state backup of the Edge Transport server and an export of the Edge Subscription file server by using Windows Server Backup.
- D. Perform a full backup of the Edge Transport server by using Windows Server Backup.

Answer: D

Explanation:

What Needs to be Backed Up on Edge Transport Servers



To plan for backup and recovery of the Edge Transport server you first need to understand where the server stores its configuration and data.

Active Directory Lightweight Directory Service – each Edge Transport server runs its own instance of AD LDS, which is used to store a subset of information about recipients in the Exchange organization, as well as information about the connectors that are established between the Edge Transport server and the Hub Transport servers for mail flow. The AD LDS database and log files are stored on the file system of the server.

Edge Configuration – the Edge Transport server configuration can be exported to an XML file for cloning between servers and for recovery purposes. The Edge configuration file is stored on the file system of the server. This does not include the Edge Subscription information that connects the Edge Transport server to Hub Transport servers.

System State – the system state contains information such as service startup and dependency settings in the registry, which is important if any settings have been modified from the defaults. The System State is also important if extra third party applications or agents have been installed on the Edge Transport server, local security policies have been applied, administrative accounts or groups created or modified, and a range of other items that may be important in a recovery.

Other Files – other files such as transport queue databases and log files are also stored on the file system.

Backing up Everything

A full system backup of the server encompasses all of the required information for a recovery, however this takes longer to backup and consumes the most backup storage.

This makes it impractical if frequent backups are required throughout the day, for example in a high volume email environment the transport queue databases might be backed up every 5 minutes to reduce the risk of losing in-transit emails if the server crashed.

A full backup can also take longer to recover in some cases, however this is less of a concern if multiple Edge Transport servers are deployed.

Question: 121

A corporate environment includes Exchange Server 2010. The environment is configured as shown in the following table.

Server name	Location	Exchange Server 2010 role	Notes
HQ-HTCAS1	Main office	Hub Transport, Client Access	Client Access server array FQDN is exchange.contoso.com
HQ-HTCAS2	Main office	Hub Transport, Client Access	Client Access server array FQDN is exchange.contoso.com
HQ-MBX1	Main office	Mailbox	Member of the database availability group (DAG)
HQ-MBX2	Main office	Mailbox	Member of the DAG
DR-HTCAS1	Disaster recovery site	Hub Transport, Client Access	Not part of an array
DR-MBX1	Disaster recovery site	Mailbox	Member of the DAG

The company is planning to test a complete site failover.

You have the following requirements:

- Ensure that users can connect to their mailboxes in the disaster recovery site by using Microsoft Outlook 2010.
- Minimize downtime during the site failover.
- Minimize client connectivity issues after the site failover.

You need to recommend a solution that meets the requirements. What should you recommend?

- Prior to the site failover, raise the time to live (TTL) value of exchange.contoso.com to the maximum value. After the site failover, update exchange.contoso.com to point to DR-MBX1.
- Prior to the site failover, lower the time to live (TTL) value of exchange.contoso.com to the minimum value. After the site failover, update exchange.contoso.com to point to DR-HTCAS1.
- Add a DNS record pointing exchange.contoso.com to the DR-HTCAS1 server.
- Add a DNS record pointing exchange.contoso.com to the DR-MBX1 server.

Answer: B

Question: 122

A corporate environment includes Exchange Server 2010 deployed at the company headquarters and at a branch office. Each location includes one Mailbox server, one Client Access server, and one Hub Transport server. Each location has two Edge Transport servers in the perimeter network. The current MX record preferences and Edge Transport servers are shown in the following table.

Location	Server name	MX record preference
Headquarters	ET-HQ01	10
Headquarters	ET-HQ02	20
Branch office	ET-BR03	30
Branch office	ET-BR04	40

You have the following requirements:

- Balance external email between the headquarters and branch office locations.
 - Balance email delivered to each location between the location's Edge Transport servers.
- You need to recommend a solution that meets the requirements.
What should you recommend?

- A. Update the MX record preference for ET-BR03 to 10, and remove the MX records for ET-HQ02 and ET-BR04.
- B. Update the MX record preference for ET-HQ02 to 10, for ET-BR03 to 10, and for ET-BR04 to 10.
- C. Update the MX record preference for ET-HQ02 to 10, for ET-BR03 to 20, and for ET-BR04 to 20.
- D. Update the MX record preference for ET-HQ02 to 10, and remove the MX records for ET-BR03 and ET-BR04.

Answer: B

Question: 123

A corporate environment includes Exchange Server 2010 SP1 deployed in a primary datacenter and in a secondary datacenter. The datacenters are in separate Active Directory Domain Services (AD DS) sites. Each datacenter includes AD DS domain controllers, Global Catalog servers, DNS servers, and two Mailbox servers. The primary datacenter contains one file share witness. All Mailbox servers are members of one database availability group (DAG). Each datacenter has independent Internet access. A dedicated high-speed network connection exists between the datacenters.

You are designing a failover plan. You have the following requirements:

- Provide a highly available solution in the event that the primary datacenter fails.
- Provide mailbox access for employees through the secondary datacenter.
- Ensure that each Mailbox database is active in only one location at a time.
- Ensure that failback to the primary datacenter completes gracefully.

You need to design a solution that meets the requirements.

What should you recommend?

- A. Configure the AutoDatabaseMountDial property to Lossless on all Mailbox servers before an outage occurs. During an outage, ensure that all Exchange services in the primary datacenter are running, validate the health of the secondary datacenter Exchange servers, and restart the secondary datacenter Mailbox servers.
- B. Configure the AutoDatabaseMountDial property to BestAvailability on all Mailbox servers before an outage occurs. During an outage, stop and disable any running Exchange services in the primary datacenter, validate the health of the secondary datacenter Exchange servers, and restart the secondary datacenter Mailbox servers.
- C. Enable datacenter activation coordination (DAC) mode before an outage occurs. During an outage, stop and disable any running Exchange services in the primary datacenter, validate the health of the secondary datacenter Exchange servers, and activate the secondary datacenter Mailbox servers.
- D. Disable datacenter activation coordination (DAC) mode before an outage occurs. During an outage, ensure that all Exchange services in the primary datacenter are running, validate the health of the secondary datacenter Exchange servers, and activate the secondary datacenter Mailbox servers.

Answer: C

Explanation:

Understanding Datacenter Activation Coordination Mode

Applies to: Exchange Server 2010 SP1

Topic Last Modified: 2011-05-26

Datacenter Activation Coordination (DAC) mode is a property setting for a database availability group (DAG). DAC mode is disabled by default and should be enabled for all DAGs with two or more members that use continuous replication. DAC mode shouldn't be enabled for DAGs in third-party replication mode unless specified by the third-

party vendor.

If a catastrophic failure occurs that affects the DAG (for example, a complete failure of one of the datacenters), DAC mode is used to control the startup database mount behavior of a DAG. When DAC mode isn't enabled, and a failure occurs that affects multiple servers in the DAG, when a majority of the DAG members are restored after the failure, the DAG will restart and attempt to mount databases. In a multi-datacenter configuration, this behavior could cause split brain syndrome, a condition that occurs when all networks fail, and DAG members can't receive heartbeat signals from each other. Split brain syndrome can also occur when network connectivity is severed between the datacenters. Split brain syndrome is prevented by always requiring a majority of the DAG members (and in the case of DAGs with an even number of members, the DAG's witness server) to be available and interacting for the DAG to be operational. When a majority of the members are communicating, the DAG is said to have quorum.

For example, consider a scenario where the first datacenter contains two DAG members and the witness server, and the second datacenter contains two other DAG members. If the first datacenter loses power and you activate the DAG in the second datacenter (for example, by activating the alternate witness server in the second datacenter), if the first datacenter is restored without network connectivity to the second datacenter, the active databases within the DAG may enter a split brain condition.

How DAC Mode Works DAC mode is designed to prevent split brain from occurring by including a protocol called Datacenter Activation Coordination Protocol (DACP). After a catastrophic failure, when the DAG recovers, it won't automatically mount databases even though the DAG has a quorum. Instead DACP is used to determine the current state of the DAG and whether Active Manager should attempt to mount the databases.

You might think of DAC mode as an application level of quorum for mounting databases. To understand the purpose of DACP and how it works, it's important to understand the primary scenario it's intended to deal with. Consider the two-datacenter scenario. Suppose there is a complete power failure in the primary datacenter. In this event, all of the servers and the WAN are down, so the organization makes the decision to activate the standby datacenter. In almost all such recovery scenarios, when power is restored to the primary datacenter, WAN connectivity is typically not immediately restored.

This means that the DAG members in the primary datacenter will power up, but they won't be able to communicate with the DAG members in the activated standby datacenter. The primary datacenter should always contain the majority of the DAG quorum voters, which means that when power is restored, even in the absence of WAN connectivity to the DAG members in the standby datacenter, the DAG members in the primary datacenter have a majority and therefore have quorum.

This is a problem because with quorum, these servers may be able to mount their databases, which in turn would cause divergence from the actual active databases that are now mounted in the activated standby datacenter. DACP was created to address this issue. Active Manager stores a bit in memory (either a 0 or a 1) that tells the DAG whether it's allowed to mount local databases that are assigned as active on the server. When a DAG is running in DAC mode (which would be any DAG with three or more members), each time Active Manager starts up the bit is set to 0, meaning it isn't allowed to mount databases. Because it's in DAC mode, the server must try to communicate with all other members of the DAG that it knows to get another DAG member to give it an answer as to whether it can mount local databases that are assigned as active to it. The answer comes in the form of the bit setting for other Active Managers in the DAG. If another server responds that its bit is set to 1, it means servers are allowed to mount databases, so the server starting up sets its bit to 1 and mounts its databases.

But when you recover from a primary datacenter power outage where the servers are recovered but WAN connectivity has not been restored, all of the DAG members in the primary datacenter will have a DACP bit value of 0; and therefore none of the servers starting back up in the recovered primary datacenter will mount databases, because none of them can communicate with a DAG member that has a DACP bit value of 1.

DAC Mode for DAGs with Two Members DAGs with two members have inherent limitations that prevent the DACP bit alone from fully protecting against application-level split brain syndrome. For DAGs with only two members, DAC mode also uses the boot time of the DAG's alternate witness server to determine whether it can mount databases on startup. The boot time of the alternate witness server is compared to the time when the DACP bit was set to 1.

If the time the DACP bit was set is earlier than the boot time of the alternate witness server, the system assumes that the DAG member and witness server were rebooted at the same time (perhaps because of power loss in the primary datacenter), and the DAG member isn't permitted to mount databases.

If the time that the DACP bit was set is more recent than the boot time of the alternate witness server, the system assumes that the DAG member was rebooted for some other reason (perhaps a scheduled outage in which maintenance was performed or perhaps a system crash or power loss isolated to the DAG member), and the DAG member is permitted to mount databases.

Dd979790.important(en-us,EXCHG.141).gif!Important:

Because the alternate witness server's boot time is used to determine whether a DAG member can mount its active databases on startup, you should never restart the alternate witness server and the sole DAG member at the same time. Doing so may leave the DAG member in a state where it cannot mount databases on startup. If this happens, you must run the `Restore-DatabaseAvailabilityGroup` cmdlet on the DAG. This resets the DACP bit and permits the DAG member to mount databases.

Other Benefits of DAC Mode In addition to preventing split brain syndrome at the application level, DAC mode also enables the use of the built-in site resilience cmdlets used to perform datacenter switchovers. These include the following: `Stop-DatabaseAvailabilityGroup` `Restore-DatabaseAvailabilityGroup` `Start-DatabaseAvailabilityGroup` Performing a datacenter switchover for DAGs that are not in DAC mode involves using a combination of Exchange tools and cluster management tools.

For more information about datacenter switchovers, see [Datacenter Switchovers](#).

Enabling DAC Mode DAC mode can be enabled only by using the Exchange Management Shell. Specifically, you can use the `Set-DatabaseAvailabilityGroup` cmdlet to enable and disable DAC mode, as illustrated in the following example.

```
Set-DatabaseAvailabilityGroup -Identity DAG2 -DatacenterActivationMode DagOnly
```

In the preceding example, a DAG named DAG2 is enabled for DAC mode.

For more information about enabling DAC mode, see [Configure Database Availability Group Properties](#) and [Set-DatabaseAvailabilityGroup](#).

Question: 124

A corporate environment includes Exchange Server 2010. Two teams of support technicians manage mailboxes for the organization. You have the following requirements:

- The Tier 1 support team must manage mailboxes for all users other than those in the Executive Organizational Unit (OU).
- The Tier 2 support team must manage mailboxes for all users in the Executive OU.

You need to recommend a solution that meets the requirements. What should you recommend?

- A. Create an exclusive scope for the Tier 2 support team.
- B. Create an explicit scope for the Tier 1 support team.
- C. Create an exclusive scope for the Tier 1 support team.
- D. Create a configuration scope for the Tier 2 support team.

Answer: A

Explanation:

Understanding Exclusive Scopes

Applies to: Exchange Server 2010 SP1

Topic Last Modified: 2010-06-25

Exclusive scopes are a special type of explicit management scope that can be associated with management role assignments. Exclusive scopes are designed to enable situations where you have a group of highly valuable objects, such as a CEO mailbox, and you want to tightly control who has access to manage those objects.

A role assignment that has an exclusive scope is called an **exclusive role assignment**.

When you create an exclusive scope, only those who are assigned that exclusive scope, or an equivalent exclusive scope, can modify the objects that match the scope. Role assignees who aren't assigned that exclusive scope, or an equivalent, can't modify the objects that match the scope, even if their own roles have scopes that would otherwise include the objects. Exclusive scopes override any other regular scope that isn't exclusive. This behavior is similar to how a deny access control entry (ACE) on an Active Directory access control list (ACL) functions.

An **equivalent exclusive scope** refers to another exclusive scope that matches some of the same objects as another exclusive scope. The scopes don't have to match the same complete set of objects. Both scopes may be able to modify some, or all, of the objects that match them.

[More Res](#)

Related I

[Understar](#)

[View Role](#)

[Active Dir](#)

Related I

[Visit the E](#)

Related I

[Ask a que](#)

[Visit the fi](#)

[Exchange](#)

Question: 125

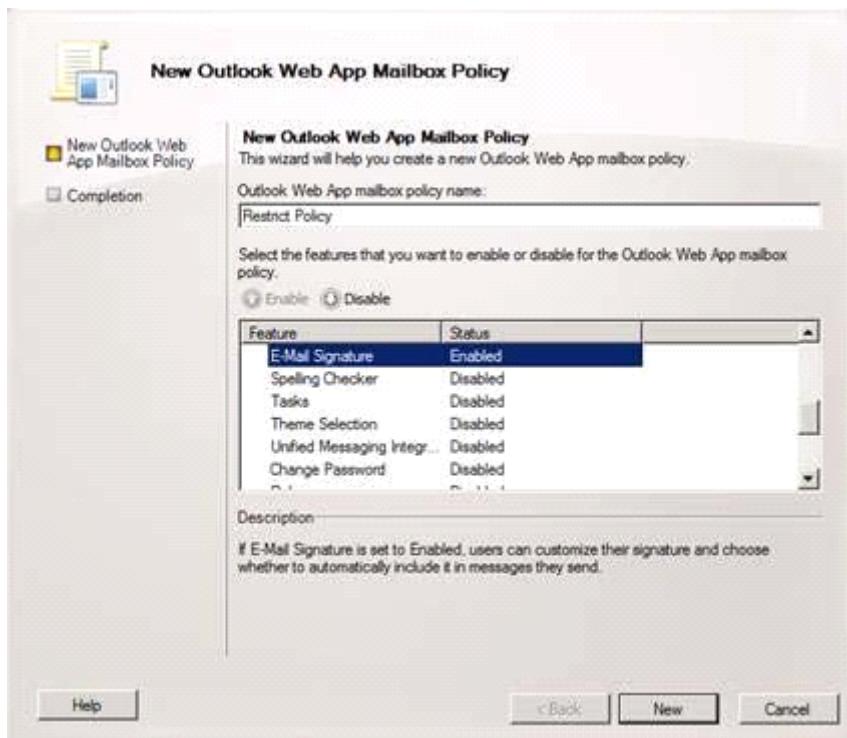
A corporate environment includes Exchange Server 2010 and Active Directory Domain Services (AD DS). You need to recommend a solution for preventing a specific group of users from changing their AD DS passwords in Outlook Web App (OWA). The solution must not affect other users. What should you recommend?

- A. Create a new Outlook Web App mailbox policy
- B. Configure the authentication settings on the OWA virtual directory
- C. Configure OWA virtual directory segmentation
- D. Create a new managed folder mailbox policy

Answer: A

Explanation:

Use Microsoft Office Outlook Web App mailbox policies to create organization-level policies to manage access to features in Outlook Web App. Outlook Web App mailbox policies allow you to create multiple policies at the organization level and apply them to individual mailboxes.



Question: 126

A corporate environment includes Exchange Server 2010 and Active Directory Domain Services (AD DS). Client computers and the Exchange servers are joined to a single AD DS domain. When users connect to Outlook Web App (OWA) from their client computers, they are prompted for their credentials. You need to recommend a solution that allows users to connect to OWA from their client computers without being prompted for credentials. What should you recommend?

- A. Basic authentication
- B. Digest authentication for Windows domain servers
- C. forms-based authentication
- D. integrated Windows authentication

Answer: D

Explanation:

Exchange Server 2010 Outlook Web App Authentication Types

There are four authentication methods available for Exchange Server 2010 OWA. They are:

Integrated Authentication – this allows domain users who are logged on to domain computers to automatically logon to Outlook Web App. This is useful for internal Outlook Web App access as it simplifies the logon process for domain users (they don't need to logon once to the computer and then a second time for OWA). However Integrated Authentication is not suitable for remote access by people using non-domain member computers, or people who are connecting via proxy servers.

Question: 127

A corporate environment includes a main office and a branch office. The company plans to deploy Exchange Server

2010. The Mailbox servers will be part of a single database availability group (DAG) that spans both locations. There is only intermittent connectivity between the two locations. You need to recommend a public folder database solution that enables users from either location to consistently access public folders. Which two actions should you recommend? (Each correct answer presents part of the solution. Choose two.)

- A. Create a single public folder database in the branch office and add it as a replica for the public folders.
- B. Configure public folder referrals between the main office and the branch office.
- C. Create a single public folder database in the main office and add it as a replica for the public folders.
- D. Configure cross-site RPC Client Access on the DAG.

Answer: A, C

Question: 128

A corporate environment includes an on-premise deployment of Exchange Server 2010 SP1 and an Active Directory Domain Services (AD DS) domain. The company plans to move some users to a cloud-based Exchange Server 2010 SP1 environment. The migration process must meet the following requirements:

- Integrate the on-premise environment with the cloud-based environment.
- Migrate all existing mailbox items.
- Authenticate all users by using their AD DS credentials.
- Share calendar availability information among all users.

You need to recommend a tool for gathering information and verifying that the requirements can be met. Which tool should you recommend?

- A. Exchange Deployment Assistant
- B. Exchange Best Practices Analyzer
- C. Exchange Pre-Deployment Analyzer
- D. Exchange Remote Connectivity Analyzer

Answer: A

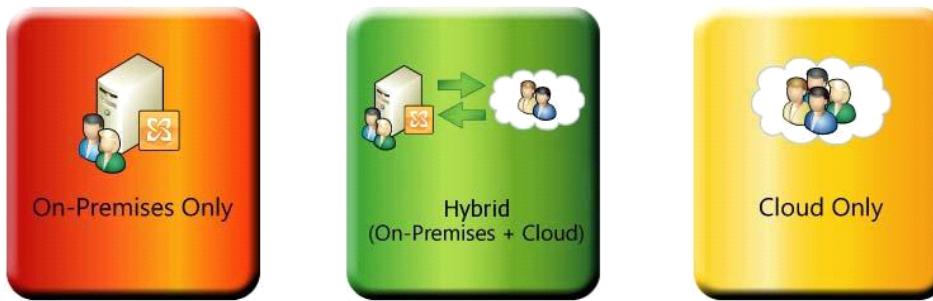
Explanation:

 Microsoft®
Exchange Server
Deployment Assistant

Exchange Help | Forums | Feedback | About

Welcome to the Exchange Server Deployment Assistant! This tool asks you a few questions about your current environment and then generates customized instructions you can use to upgrade to Exchange 2010 on-premises or in the cloud.

Select an option below to get started....



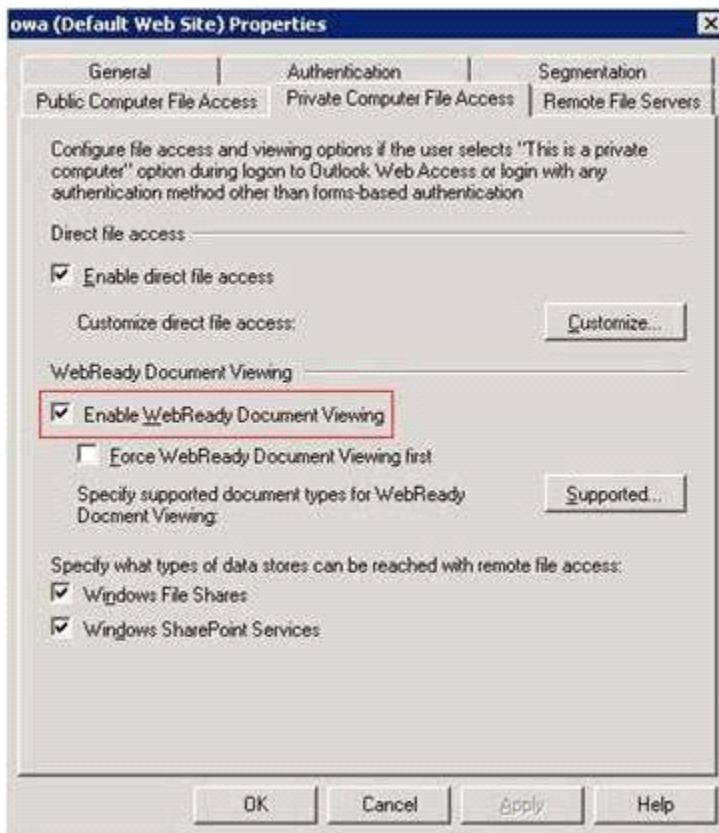
Question: 129

A corporate environment includes Exchange Server 2010. All employees connect to their mailboxes by using a web browser. You need to recommend a solution that will force only a specific group of employees to use WebReady Document Viewing when connecting to their mailboxes. What should you recommend?

- A. Configure an Outlook Web App mailbox policy.
- B. Configure the Outlook Web App virtual directory on all Client Access servers.
- C. Create and configure a Group Policy Object (GPO) and link it to the Organizational Unit (OU) where the computer accounts for the employees reside.
- D. Create and configure a Group Policy Object (GPO) and link it to the Organizational Unit (OU) where the user accounts for the employees reside.

Answer: B

Explanation:



Question: 130

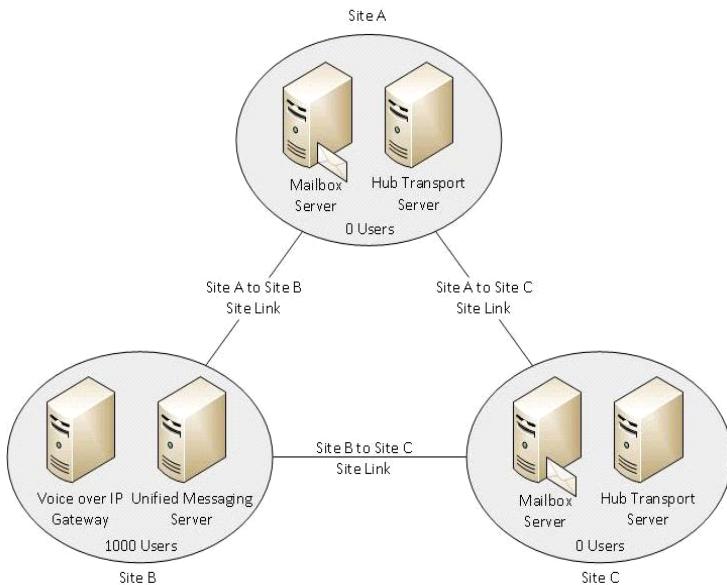
A corporate environment includes an on-premise deployment of Exchange Server 2010 SP1. Client computers run Microsoft Outlook 2010. Contractors use a cloud-based Exchange Server 2010 SP1 service and have email accounts on the contractors.contoso.com domain. Employees cannot view calendar availability information for contractors from their client computers. You need to recommend the first step in sharing calendar availability information between employees and contractors. What should you recommend?

- A. Create a sharing policy.
- B. Create an organization relationship.
- C. Create a federation trust.
- D. Create a forest trust.

Answer: C

Question: 131

A corporate environment will include Exchange Server 2010 in a single Active Directory Domain Services (AD DS) domain. The AD DS site topology and Exchange Server topology are configured as shown in the exhibit. (Click the Exhibit button.)



You need to recommend an approach for the placement of the Client Access servers. Which two actions should you recommend? (Each correct answer presents part of the solution. Choose two.)

- A. Deploy only one Client Access server in Site B.
- B. Deploy one Client Access server in Site A.
- C. Deploy two Client Access servers in Site B.
- D. Deploy one Client Access server in Site C.

Answer: B, D

Question: 132

A corporate environment will include Exchange Server 2010 in a single Active Directory Domain Services (AD DS) domain. The primary DNS suffix of the domain controllers is not the same as the DNS domain name. You are designing the Exchange Server 2010 deployment plan. You need to recommend a solution that allows Exchange Server 2010 servers to access the domain controllers. What should you recommend?

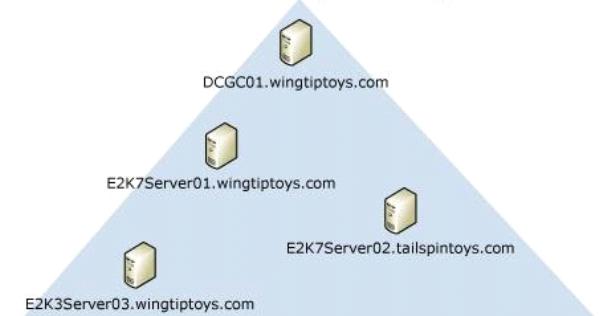
- A. Modify the DNS-Host-Name AD DS attribute on the domain object container.
- B. Modify the NETBIOS-Name AD DS attribute on the Exchange Server computer objects.
- C. Modify the msDS-AllowedDNSSuffixes AD DS attribute on the domain object container.
- D. Modify the msDS-AdditionalDnsHostName AD DS attribute on the domain object container.

Answer: C

Explanation:

■ Scenario 1

In this scenario, the primary DNS suffix of the domain controller is not the same as the DNS domain name. The domain controller is disjointed in this scenario. The domain, including Exchange servers and Microsoft Outlook client computers, can have a primary DNS suffix that either matches the primary DNS suffix or the DNS domain name.

Domain controller and member computers are disjointed

DNS domain name: tailspintoy.com
 Primary DNS suffix for DCGC01: wingtiptoy.com (disjoint)

Primary DNS suffix for E2K7Server01 and E2K3Server03: wingtiptoy.com (disjoint)
 Primary DNS suffix for E2K7Server02: tailspintoy.com
 msDS-AllowedDNSSuffixes: wingtiptoy.com

To allow Exchange 2007 servers to access domain controllers that are disjointed, you must modify the **msDS-AllowedDNSSuffixes** Active Directory attribute. You must add both of the DNS suffixes to the attribute. For detailed steps about how to modify the attribute, see [The computer's primary DNS suffix does not where it resides](#).

**Question: 133**

You have an Active Directory forest that contains one site. You plan to deploy an Exchange organization. All servers in the organization will have Exchange Server 2010 Service Pack 1 (SP1) installed. The relevant Mailbox servers are configured as shown in the following table.

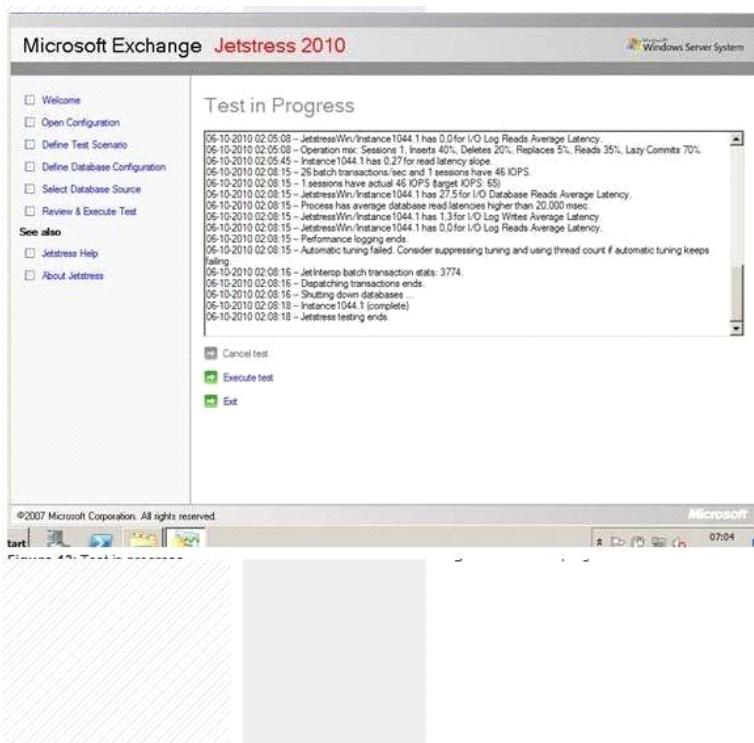
Server name	Database name	Database availability group (DAG) name
MBX1	MDB01	DAG1
MBX1	MDB02	DAG1
MBX2	MDB03	DAG1
MBX2	MDB04	DAG1
MBX3	MDB05	DAG2
MBX3	MDB06	DAG2
MBX4	MDB07	DAG2
MBX4	MDB08	DAG2

Each Mailbox server will host 2,000 mailboxes. Corporate policy states that the servers must have a maximum write latency of 100 ms and an average write latency of 10 ms. The hardware vendor for the planned deployment provides test hardware. You need to recommend a solution to ensure that the planned deployment meets the requirements of the corporate policy. Which of the following solutions is the best recommendation? (More than one answer choice may achieve the goal. Select the BEST answer.)

- Identify the workload at which the hardware can deliver acceptable latency by using the Jetstress tool.
- Gather a baseline of the disk I/O usage by using the Windows Performance Monitor.
- Calculate the number of IOPS required for the planned deployment by using the Exchange 2010 Mailbox Server Role Requirements Calculator.
- Test the performance of the hardware under a simulated user workload by using the Loadgen tool.

Answer: A

Explanation:

**Analyzing Results**

After the test is completed, the performance data is analyzed and saved to Performance_(DateTime).html file. All the performance counter named Performance_(DateTime).blg that you can use for some monitoring.

Consider the following guidelines when examining the data collected:

Performance counter instance	Guidelines for performance
I/O Database Reads Average Latency (msec)	The average value should be less than 20 milliseconds (msec). The maximum values should be less than 50 msec.
I/O Log Writes Average Latency (msec)	Log disk writes are sequential. Average write latencies should be less than 10 msec, with a maximum of less than 50 msec.
%Processor Time	Average should be less than 10%. The maximum should be less than 20%.
Available Mbytes (32-bit Windows Server only)	Minimum should be no less than 50 megabytes (MB).
Free System Page Table Entries (32-bit Windows Server only)	Minimum should be no less than 1000000.
Transition Pages Repurposed/sec (Windows Server 2003, Windows Server 2008, Windows Server 2008 R2)	Average should be less than 1000.

Question: 134

A company has an on-premise Exchange Server 2007 SP2 environment. Client computers run Microsoft Outlook 2010. The company plans to migrate to a cloud-based Microsoft Exchange Server 2010 SP1 service. You need to recommend a solution for ensuring that Outlook locates the cloud-based servers when users check calendar availability information. What should you recommend?

- A. Add a CNAME record.
- B. Add an MX record.
- C. Synchronize the AD DS directory from the on-premise environment.
- D. Synchronize the AD DS directory from the cloud-based environment.

Answer: A**Explanation:**

What you need to do is add a CNAME record with the host value of Autodiscover. So the full record would be autodiscover.domain.com. Once you have that CNAME you need to point it to autodiscover.outlook.com. The way you know this works is to do an NSLOOKUP:

nslookup autodiscover.domain.com

You should see something like this:

Server: dns.corp.domain.com

Address: 192.168.1.10

Non-authoritative answer:

Name: autodiscover.outlook.com

Address: 65.55.94.54

Question: 135

You have an Exchange organization. All servers in the organization have Exchange Server 2010 Service Pack 1 (SP1)

installed. The Exchange organization contains two Hub Transport servers, two Client Access servers, and two Mailbox servers. All Exchange servers are located on the internal network. Your company plans to use Microsoft Exchange Hosted Services for message hygiene. You need to recommend changes to the Exchange organization to meet the following requirements:

- Ensure that the company can send e-mail messages if a single server fails.
- Ensure that the company can receive e-mail messages if a single server fails.
- Prevent Internet hosts from initiating connections directly to servers on the internal network.

Which of the following changes is the best recommendation? (More than one answer choice may achieve the goal. Select the BEST answer.)

A. Move the two Hub Transport servers to the perimeter network. Update the public Mail Exchanger (MX) records to point to the Exchange Hosted Services servers. Configure Exchange Hosted Services to forward e-mail to the new servers. Configure the internal firewall to allow communication from the Hub Transport servers to the internal network. Create an additional Send connector.

B. Deploy two new Edge Transport servers on the perimeter network. Update the public Mail Exchanger (MX) records to point to the Exchange Hosted Services servers. Configure Exchange Hosted Services to forward e-mail to the new servers. Configure the internal firewall to allow communication from the Edge Transport servers to the internal network. Enable EdgeSync synchronization.

C. Deploy two new Hub Transport servers on the perimeter network.

Update the public Mail Exchanger (MX) records to point to the new Hub Transport servers.

Configure the internal firewall to allow communication from the Hub Transport servers to the internal network.

Create an additional Send connector.

D. Deploy two new Edge Transport servers on the perimeter network.

Update the public Mail Exchanger (MX) records to point to the new Edge Transport servers.

Configure the internal firewall to allow communication from the Edge Transport servers to the internal network.

Enable EdgeSync synchronization.

Answer: B

Question: 136

A corporate environment includes Exchange Server 2003 SP2 and an Active Directory Domain Services (AD DS) domain. The company intends to transition to Exchange Server 2010. The Exchange 2003 Recipient Update Service (RUS) must function properly after you update the AD DS schema for Exchange Server 2010. You need to recommend a solution for preparing the environment before updating the schema. What should you recommend?

- A. Add each Exchange Server 2010 Mailbox server to the Exchange Enterprise Servers group in AD DS.
- B. Run the setup /PrepareLegacyExchangePermissions command.
- C. Run the setup /PrepareDomain command.
- D. Add each Exchange Server 2010 server to the Exchange Domain Servers group in AD DS.

Answer: B

Explanation:

Prepare Legacy Exchange 2003 Permissions

Applies to: Exchange Server 2010 SP1

Topic Last Modified: 2011-04-23

When upgrading from Exchange Server 2003 to Exchange Server 2010, you must first grant specific Exchange permissions in each domain in which you have run Exchange 2003 DomainPrep. To do this, you run the `setup /PrepareLegacyExchangePermissions` command. Granting these permissions is part of preparing Active Directory and your domains for installing Exchange Server 2010. For detailed instructions, see [Prepare Active Directory and Domains](#).

This topic explains why you must run the `setup /PrepareLegacyExchangePermissions` command, when you run it, and what permissions are set by the command in your Exchange Server 2010 organization.

Why Run Setup /PrepareLegacyExchangePermissions

Essentially, you must run the `setup /PrepareLegacyExchangePermissions` command so that the Exchange 2003 Recipient Update Service functions correctly after you update the Active Directory schema for Exchange Server 2010. This section explains the main issue and how running the command resolves this issue.

Question: 137

You are transitioning an Exchange Server environment from Exchange Server 2007 SP2 to Exchange Server 2010. You deploy all Exchange Server 2010 Client Access servers and Hub Transport servers, and move Internet mail flow from Exchange Server 2007 SP2 to Exchange Server 2010. All mailboxes are on Exchange Server 2007 SP2. Each message sent to a specific distribution group must be approved by an executive assistant. You need to recommend a solution that meets the requirement. What should you recommend?

- A. Configure the message delivery restrictions for the distribution group.
- B. Create an Exchange Server 2010 Hub Transport rule, and set an Exchange Server 2007 SP2 Hub Transport server as the expansion server for the distribution group.
- C. Designate the executive assistant as the manager of the distribution group.
- D. Create an Exchange Server 2010 Hub Transport rule, and set an Exchange Server 2010 Hub Transport server as the expansion server for the distribution group.

Answer: D

Explanation:

Understanding Moderated Transport

Applies to: Exchange Server 2010 SP1

Topic Last Modified: 2010-08-05

Using the moderated transport feature in Microsoft Exchange Server 2010, you can require all e-mail messages sent to specific recipients be approved by moderators. You can configure any type of recipient as a moderated recipient, and Exchange 2010 Hub Transport servers will ensure that all messages sent to those recipients go through an approval process.

In any type of organization, you may need to restrict access to specific recipients. The most common scenario is the need to control messages sent to large distribution groups. Depending on your organization's requirements, you may also need to control the messages sent to executive mailboxes or partner contacts. You can use moderated recipients to accomplish these tasks.

More R
Relate
Underst
Can't R
Configu

Relate
Visit the

Relate
Ask a q
Visit the

Exchan

Note:

Previous versions of Exchange don't support moderated recipients. If a message sent to a moderated distribution group is expanded on a Hub Transport server 2007, it will be delivered to all members of that distribution group, bypassing the moderation process. If you have Exchange 2007 Hub Transport servers in your organization, and you want to use moderated distribution groups, you must designate an Exchange 2010 Hub Transport server as the expansion server for the distribution groups. Doing this ensures that all messages sent to the distribution group are moderated.

Question: 138

A corporate environment includes an on-premise deployment of Exchange Server 2010 SP1 and client computers that run Microsoft Outlook 2010. An Active Directory Domain Services (AD DS) domain named contoso.com contains user accounts for all employees. The company plans to move the mailboxes of the Sales team members to a cloud-based Exchange Server 2010 SP1 service provider. Sales team members will have primary email addresses of contoso.com and secondary email addresses of cloud.contoso.com. You need to recommend a solution for ensuring that the Autodiscover service continues to configure Outlook for all users. What should you recommend?

- A. Run the Export-AutoDiscoverConfig cmdlet.
- B. Mail-enable the on-premise AD DS user accounts of the Sales team members with email addresses of cloud.contoso.com.
- C. Create a new Autodiscover virtual directory.
- D. Configure the ExternalUrl property of the Autodiscover virtual directory to autodiscover.cloud.contoso.com.

Answer: B

Question: 139

A corporate environment includes Exchange Server 2010. Support technicians do not have access to email message status information. Support technicians must currently escalate user requests for email message status to Exchange Server administrators. You need to recommend a solution that allows support technicians to display email message status in the Exchange Control Panel (ECP). What should you recommend?

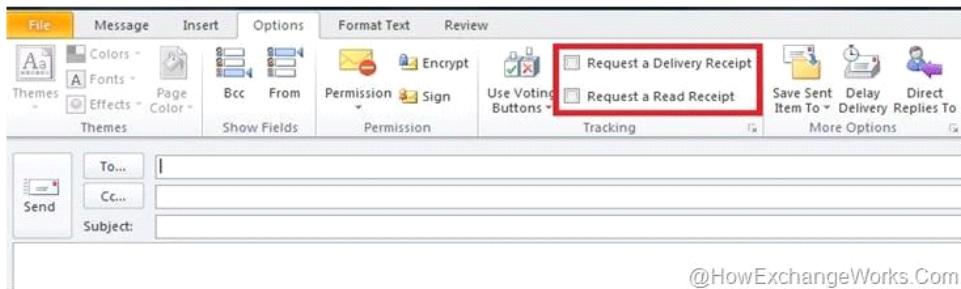
- A. Grant the support technicians Read access to the SMTP protocol log files.
- B. Assign the support technicians to the Message Tracking role.
- C. Grant the support technicians Read access to the SMTP connectivity log files.
- D. Assign the support technicians to the Records Management role.

Answer: B

Explanation:

Turn On Email "Read Status" Tracking For Your Organization In Exchange 2010...

All of us are familiar with turning on "read receipt" and "delivery receipt" while composing an important message to make sure that the message has been delivered & read by the recipients.



Though this option was useful to some extent in knowing whether the email was read, recipients could always deny sending "read receipt" to the sender.

With Exchange 2010, you can turn on this feature globally, which means that all emails flowing in your organization can be checked for its "read status". The good thing is that the sender can do it him/herself. Let me explain the feature in action.

By default, the feature is disabled. This is the case in both Exchange 2010 & SP1. To check the current configuration, run `Get-OrganizationConfig | fl read*`

To turn on the feature, run `Set-OrganizationConfig -ReadTrackingEnabled $true`

```
[PS] C:\Windows\system32>Get-OrganizationConfig | fl read*
ReadTrackingEnabled : False

[PS] C:\Windows\system32>Set-OrganizationConfig -ReadTrackingEnabled $true
[PS] C:\Windows\system32>
```

Microsoft® Outlook Web App



.....

Mail

Calendar

Delivery Report

Testing Read

From: Rajith Enchiparambil
To: Raj test
Sent: 21/09/2010 15:3

E-Mail This Report

Delivery Report for

Submitted
21/09/2010 15:33
The message was subn

Delivered
21/09/2010 15:33
The message was succ

Question: 140

A corporate environment includes Exchange Server 2010 SP1 and an Active Directory Domain Services (AD DS) domain. Client computers run Microsoft Outlook 2010. You need to recommend an approach for identifying when a mailbox is accessed by someone other than the mailbox owner. What should you recommend?

- A. Run a report from the Exchange Control Panel (ECP).
- B. Run the Get-LogonStatistics cmdlet.
- C. Search the message tracking logs.
- D. Run the Search-AdminAuditLog cmdlet.

Answer: A

Explanation:

Run a Non-Owner Mailbox Access Report

The Non-Owner Mailbox Access Report in the Exchange Control Panel lists the mailboxes that have been accessed by someone other than the person who owns the mailbox. When a mailbox is accessed by a non-owner, Microsoft Exchange logs information about this action in a mailbox audit log that is stored as an e-mail message in a hidden folder in the mailbox being audited. Entries from this log are displayed as search results and include a list of mailboxes accessed by a non-owner, who accessed the mailbox and when, the actions performed by the non-owner, and whether the action was successful.

This topic explains the following:

- Why would you need to know about non-owner mailbox access?
- Before you can run a mailbox auditing report
- What are the types of non-owners?
- What gets logged in the mailbox audit log?
- Run a non-owner mailbox access report

Question: 141

A corporate environment includes Exchange Server 2010 SP1. Client computers run Microsoft Outlook 2010 using Standard Client Access Licenses (CALs). You need to recommend a solution that allows long-term message archival and minimizes hardware costs. Which two actions should you recommend? (Each correct answer presents part of the solution. Choose two.)

- A. Apply a retention policy tag to each mailbox.
- B. Utilize personal archives that are stored in a cloud-based Exchange Server 2010 SP1 environment.
- C. Acquire an Enterprise CAL for each user.
- D. Create a retention policy tag and set the age limit for retention.

Answer: B, C

Question: 142

A corporate environment includes Exchange Server 2010. Client computers run Microsoft Outlook 2010. In the current environment, when users need to recover Outlook items that have been permanently deleted from the Deleted Items folder, administrators must recover the items from a backup of the Exchange Server environment. You have the following requirements:

- Do not require administrators to recover items from the Exchange Server backups.
- Enable online recovery by administrators of permanently deleted items.
- Automatically purge items after a specific period of time.

You need to recommend a solution that meets the requirements.

- A. Implement litigation hold.
- B. Configure single item recovery.
- C. Create a retention policy.
- D. Create a recovery database.

Answer: B

Question: 143

A corporate environment includes Exchange Server 2010 and an Active Directory Domain Services (AD DS) domain. Multiple auditing teams search mailboxes from the Exchange Control Panel (ECP) for specific types of content. You need to recommend a solution that restricts access to the results of a specific search to a specific auditing team. What should you recommend?

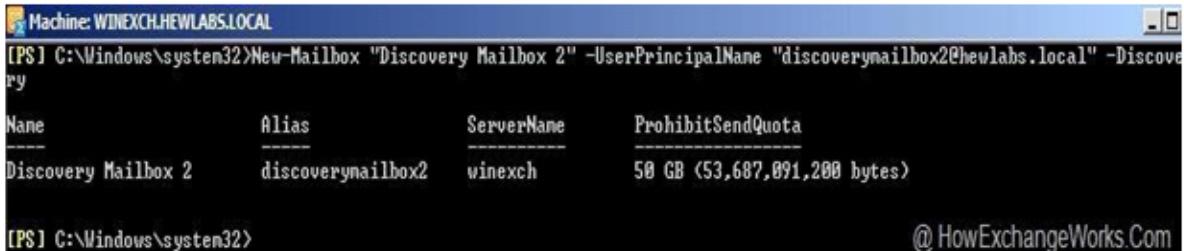
- A. Create an AD DS security group for each auditing team. Assign the security groups to the Legal Hold role.
- B. Create an arbitration mailbox for each auditing team and grant each team Read permissions to its designated mailbox.
- C. Create an AD DS security group for each auditing team. Assign the security groups to the Message Tracking role.
- D. Create a discovery mailbox for each auditing team and grant each team Read permissions to its designated mailbox.

Answer: D

Explanation:

The exchange setup creates a default discovery mailbox, which will be enough for small organizations. For large companies, they may need multiple discovery mailboxes as the searches are performed frequently and the results are kept for a longer period of time. Creating a new discovery mailbox is simple enough. Run the command below in Shell (you can't use EMC).

New-Mailbox "Discovery Mailbox 2" -UserPrincipalName discoverymailbox2@domain.local -Discovery
The key is that the switch "-discovery" needs to be added. Apart from that, the command is the same as creating a new user mailbox. Once the mailbox has been created, you need to assign full access to the "Discovery Management" group. It is easy enough to do it from the console. Right click the mailbox, select "Manage Full Access Permission" and add the group.



```
[PS] C:\Windows\system32>New-Mailbox "Discovery Mailbox 2" -UserPrincipalName "discoverymailbox2@hewlabs.local" -Discovery  
Name Alias ServerName ProhibitSendQuota  
Discovery Mailbox 2 discoverymailbox2 winexch 50 GB (53,687,091,200 bytes)
```

[PS] C:\Windows\system32> @ HowExchangeWorks.Com



Question: 144

A corporate environment includes Exchange Server 2010. Client computers run Microsoft Outlook 2010. You have the

following requirements:

- Log actions taken by delegates or administrators on a users mailbox.
 - Log when email messages are moved to the Deleted Items folder by users other than the mailbox owner.
- You need to recommend a solution that meets the requirements. What should you recommend?

- A. Use the Set-AdminAuditLogConfig cmdlet.
- B. Use the New-MailboxAuditLogSearch cmdlet.
- C. Use the Set-Mailbox cmdlet.
- D. Use the Set-MailboxAuditBypassAssociation cmdlet.

Answer: C

Explanation:

Use the Set-Mailbox cmdlet to modify the settings of an existing mailbox. You can use this cmdlet for one mailbox at a time. To perform bulk management, you can pipeline the output of various Get- cmdlets (for example, the Get-Mailbox or Get-User cmdlets) and configure several mailboxes in a single-line command.

You can also use the Set-Mailbox cmdlet in scripts.

<http://technet.microsoft.com/en-us/library/bb123981.aspx>

Question: 145

A company that is running Exchange Server 2010 merges with a company that is running Exchange Server 2007. After the merger, all external email will be delivered by the Exchange Server 2010 Hub Transport server. The company intends to keep both Exchange Server environments active for the next year. You are designing an infrastructure deployment plan. You have the following requirements:

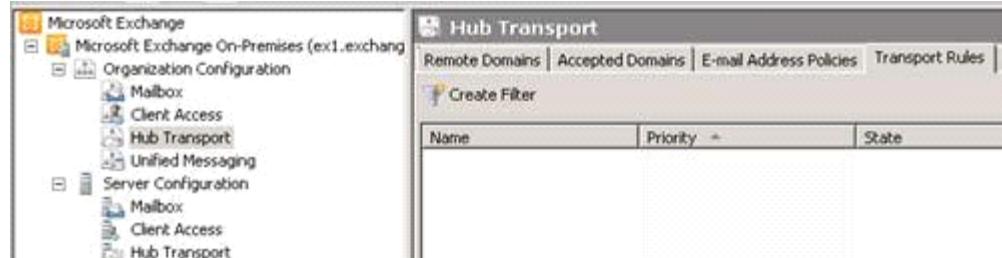
- Ensure that users with Exchange Server 2010 mailboxes can send external email messages to any domain.
 - Ensure that users with Exchange Server 2007 mailboxes can send external email messages to only specific domains.
- You need to recommend a solution that meets the requirements. What should you recommend?

- A. Configure transport rules on the Exchange Server 2010 Hub Transport server.
- B. Configure remote domains on the Exchange Server 2010 Hub Transport server.
- C. Configure accepted domains on the Exchange Server 2007 Hub Transport server.
- D. Configure transport rules on the Exchange Server 2007 Hub Transport server.

Answer: A

Explanation:

Block Users Sending to Specific Domains with Exchange Server 2010. In some scenarios an organization will want to prevent email users from sending messages to certain external domain names. This can be achieved with Exchange Server 2010 using a Transport Rule. Open the Exchange Management Console and navigate to Organization Config/Hub Transport.



Start a New Transport Rule. Give the rule an appropriate name and description.

Introduction

This wizard helps you create a new transport rule. Transport Rules check each message for predefined conditions. If the condition is true for a message, the rule actions are applied to it.

Name:

Block emails sent to specific domain names

Comment:

Block outbound emails sent to specific external domain names.]

Enable Rule

Choose conditions of “From users that are inside the organization” and “When a recipients address contains specific words”. Click on “specific words” and add the domain name you want to block, for example “@fabrikam” (without quotes). You can enter several domain names in this list.

Conditions

Step 1: Select condition(s):

- between members of distribution list and distribution list
- when the manager of any sender is people
- when the sender is the manager of a recipient
- if the sender and recipient's AD Attribute are Evaluation
- when a recipient's address contains specific words
- when a recipient's address matches text patterns
- when a recipient's properties contain specific words
- when a recipient's properties match text patterns
- when any of the recipients in the To field is people
- when any of the recipients in the "To" field is a member of distribution list

Step 2: Edit the rule description by clicking an underlined value:

Apply rule to messages

from users that are 'Inside the organization'

and when a recipient's address contains specific words

**Specify words**

Words:

<input type="button" value="Add"/>	<input type="button" value="Edit"/>	<input type="button" value="X"/>
------------------------------------	-------------------------------------	----------------------------------

@fabrikam
@nwtraders.com

Click Next and choose actions of “Send rejection message to sender...“.

Actions

Step 1: Select actions:

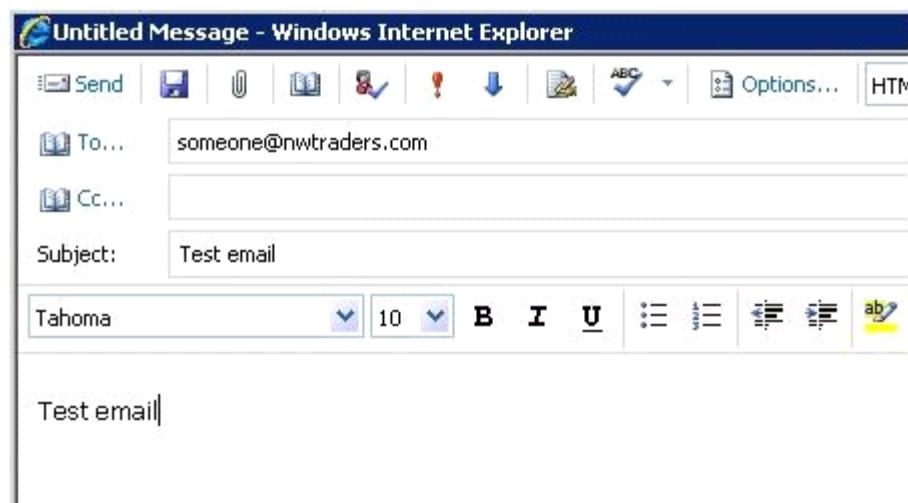
- remove header
- add a recipient in the To field addresses
- copy the message to addresses
- Blind carbon copy (Bcc) the message to addresses
- add the sender's manager as a specific recipient type
- forward the message to addresses for moderation
- forward the message to the sender's manager for moderation
- redirect the message to addresses
- send rejection message to sender with enhanced status code
- Delete the message without notifying anyone

Step 2: Edit the rule description by clicking an underlined value:

Apply rule to messages
from users that are '[Inside the organization](#)'
and when a recipient's address contains '[@fabrikam](#)' or '[@nwtraders.com](#)'
send '[Emails to this domain are not permitted](#)' to sender with '[5.7.1](#)'

Enter a rejection message and an enhanced status code so that the sender or the IT admins can easily tell why the email was rejected.

Complete the Transport Rule wizard and test the new rule by trying to send an email to that domain name.



You should now receive a bounce message from the Exchange server with the text that you configured.

Microsoft Outlook

To: someone@nwtraders.com

- This type of message isn't fully supported in Conversation mode. Click here to open the full version, which may show you more details.

Delivery has failed to these recipients or groups:

someone@nwtraders.com (someone@nwtraders.com)
Your message wasn't delivered due to a permission or security issue. It may have been rejected by a moderator, accept e-mail from certain senders, or another restriction may be preventing delivery.

Diagnostic information for administrators:

Generating server: ex1.exchangeserverpro.local

someone@nwtraders.com
#550 5.7.1 Emails to this domain are not permitted ##

Original message headers:

Question: 146

A corporate environment includes Exchange Server 2010 SP1 and client computers that run Microsoft Outlook 2010. You create a Hierarchical Address Book (HAB). Organizational groups must be added to the HAB and organized alphabetically. You need to recommend a solution for adding and alphabetizing the organizational groups. Which two actions should you recommend? (Each correct answer presents part of the solution. Choose two.)

- A. Modify the PhoneticDisplayName parameter of the security groups.
- B. Create security groups for the organizational groups and designate them as members of the HAB.
- C. Create distribution groups for the organizational groups and designate them as members of the HAB.
- D. Modify the DisplayName parameter of the distribution groups.

Answer: C, D

Explanation:

Understanding Hierarchical Address Books

Applies to: Exchange Server 2010 SP2

Topic Last Modified: 2010-09-30

The hierarchical address book (HAB) is a feature in Microsoft Exchange Server 2010 and the Microsoft Outlook 2010 address book that enables end users to browse for recipients in their Exchange organization using an organizational hierarchy. In most Exchange 2010 deployments, users are limited to the default global address list (GAL) and its associated recipient properties. Additionally, the structure of the GAL often doesn't accurately reflect the management or seniority relationships among recipients in your organization. Being able to customize an HAB that maps to your organization's unique business structure provides your users with an efficient method for locating internal recipients.

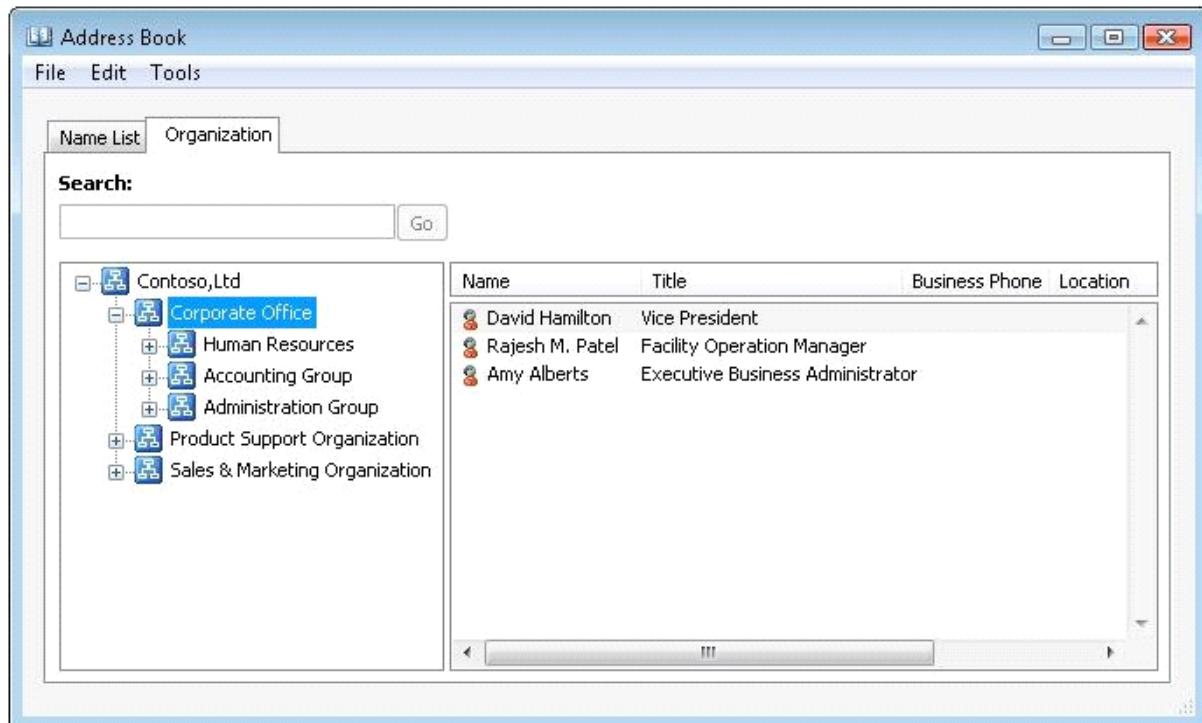
Using Hierarchical Address Books In an HAB, your root organization (for example, Contoso, Ltd) is used as the top-level tier. Under this top-level tier, you can add several child tiers to create a customized HAB that's segmented by division, department, or any other organizational tier you want to specify. The following figure illustrates an HAB for Contoso, Ltd with the following structure:

The top-level tier represents the root organization Contoso, Ltd.

The second-level child tiers represent the business divisions within Contoso, Ltd: Corporate Office, Product Support Organization, and Sales & Marketing Organization.

The third-level child tiers represent departments within the Corporate Office division: Human Resources, Accounting Group, and Administration Group.

Example HAB for Contoso, Ltd



You can provide an additional level of hierarchical structure by using the SeniorityIndex parameter. When creating an HAB, use the SeniorityIndex parameter to rank individual recipients or organizational groups by seniority within these organizational tiers. This ranking specifies the order in which the recipients or groups are displayed in the HAB. For example, in the preceding example, the SeniorityIndex parameter for the recipients in the Corporate Office division is set to the following:

- 100 for David Hamilton
- 50 for Rajesh M. Patel
- 25 for Amy Alberts

Note:

If the SeniorityIndex parameter isn't set or is equal for two or more users, the HAB sorting order uses the PhoneticDisplayName parameter value to list the users in ascending alphabetical order. If the PhoneticDisplayName parameter value isn't set, the HAB sorting order defaults to the DisplayName parameter value and lists the users in ascending alphabetical order.

Configuring Hierarchical Address Books

Detailed instructions for creating HABs are included in the topic [Configure Hierarchical Address Books](#). The general steps are as follows:

Create a distribution group that will be used for the root organization (top-level tier). If desired, you can use an existing organizational unit in your Exchange forest for the distribution group.

Create distribution groups for the child tiers and designate them as members of the HAB. Modify the SeniorityIndex parameter of these groups so they're listed in the proper hierarchical order within the root organization.

Add organization members. Modify the SeniorityIndex parameter of the members so they're listed in the proper hierarchical order within the child tiers.

For accessibility purposes, you can use the PhoneticDisplayName parameter, which specifies a phonetic pronunciation of the DisplayName parameter. To learn more about the PhoneticDisplayName parameter and speech recognition, see [Understanding Automatic Speech Recognition Directory Lookups](#).

Question: 147

A corporate environment includes deployments of Exchange Server 2010 in North America and Europe. All client computers connect to an Active Directory Domain Services (AD DS) domain named contoso.com. The topology of the Exchange organization is shown in the following table.

Users access Outlook Web App (OWA) by browsing to <https://owa.contoso.com/owa>. The configuration of the OWA virtual directory URLs on each Client Access server is shown in the following table.

Users with mailboxes hosted on server MB02 cannot remotely connect to their mailboxes by using OWA . You need to recommend a solution that allows the users to remotely connect to their mailboxes. What should you recommend?

AD DS site	Server name	Role(s)	Internet facing
North-America	MB01	Mailbox	Yes
North-America	CAHT01	Client Access, Hub Transport	Yes
Europe	MB02	Mailbox	No
Europe	CAHT02	Client Access, Hub Transport	No

Server name	InternalUrl property		ExternalUrl property
CAHT01	https://caht01.contoso.com/owa		https://owa.contoso.com/owa
CAHT02	https://caht02.contoso.com/owa		https://owa.contoso.com/owa

- A. Set the ExternalUrl property on the CAHT01 OWA virtual directory to <https://caht02.contoso.com/owa>.
- B. Set the InternalUrl property on the CAHT01 OWA virtual directory to <https://owa.contoso.com/owa>.
- C. Set the ExternalUrl property on the CAHT02 OWA virtual directory to \$null.
- D. Set the InternalUrl property on the CAHT02 OWA virtual directory to \$null.

Answer: C

Question: 148

Your network contains a perimeter network and an internal network. You are designing an Exchange organization for a company named Contoso, Ltd. All servers in the organization will have Exchange Server 2010 Service Pack 1 (SP1) installed. Contoso plans to use a third-party message hygiene solution on the Internet to relay all inbound SMTP e-mail to the Exchange servers. You need to recommend an inbound SMTP e-mail deployment solution for the Exchange organization. The solution must ensure that all Exchange servers can be managed by using Group Policies. Which of the following solutions is the best recommendation? (More than one answer choice may achieve the goal. Select the BEST answer.)

- A. Deploy Edge Transport servers on the perimeter network
Deploy Hub Transport servers on the internal network
Join the Edge Transport servers to a separate Active Directory forest on the perimeter network
Join the Hub Transport servers to the internal Active Directory forest
- B. Deploy Edge Transport servers and Hub Transport servers on the internal network
Join the Edge Transport servers to a separate Active Directory forest on the perimeter network
Join the Hub Transport servers to the internal Active Directory forest
- C. Deploy a reverse proxy server on the perimeter network
Deploy Edge Transport servers and Hub Transport servers on the internal network
Join the Hub Transport servers and the Edge Transport servers to the internal Active Directory forest.
- D. Deploy a reverse proxy server, Edge Transport servers, and Hub Transport servers on the perimeter network
Join the Edge Transport servers to a separate Active Directory forest on the perimeter network
Join the Hub Transport servers to the internal Active Directory forest.

Answer: A

Question: 149

A corporate environment includes Active Directory Domain Services (AD DS). The environment consists of an internal network and a perimeter network. AD DS is deployed only on the internal network. The company intends to utilize a service providers cloud-based Exchange Server 2010 SP1 email service. You have the following requirements:

- Maximize the security of the design.
- Use the minimum permissions required to perform directory synchronization.

You need to recommend a solution for directory synchronization between the corporate environment and the service providers environment. Which two actions should you recommend? (Each correct answer presents part of the solution. Choose two.)

- A. Install the directory synchronization tool on a computer in the perimeter network.
- B. Install the directory synchronization tool on a computer on the internal network.
- C. Create a directory synchronization service account with membership in the Domain Users group.
- D. Create a directory synchronization service account with membership in the Domain Admins group.

Answer: B, C

Question: 150

A corporate environment includes Exchange Server 2007 SP2 and Active Directory Domain Services (AD DS). Journaling is in use for all inbound and outbound email messages. The company intends to transition to Exchange Server 2010 SP1. During the coexistence, you will have the following requirements:

- Export new journal and transport rules created in the Exchange Server 2007 SP2 system.
- Ensure that the exported rules are available for import in the Exchange Server 2010 SP1 environment.

You need to recommend a solution that meets the requirements. Which two actions should you recommend? (Each correct answer presents part of the solution. Choose two.)

- A. From the Exchange Server 2010 SP1 Hub Transport server, export the journal rules.
- B. From the Exchange Server 2007 SP2 Hub Transport server, export the transport rules.
- C. From the Exchange Server 2010 SP1 Hub Transport server, export the transport rules.
- D. From the Exchange Server 2007 SP2 Hub Transport server, export the journal rules.

Answer: A, C

Question: 151

A company has an Exchange Server 2010 environment that includes several shared mailboxes. You need to recommend a solution for enabling multiple users to act as the mailbox owner when sending mail from a shared mailbox. What should you recommend?

- A. Assign FullAccess permissions for the shared mailbox to the users
- B. Assign SendAs permissions for the shared mailbox to the users
- C. Add the users to a management role group as delegates
- D. Add the users to the shared mailbox as delegates

Answer: B

Question: 152

A corporate environment includes Exchange Server 2010 SP1 and Active Directory Domain Services (AD DS). Members of the Legal security group must be able to do the following:

- Perform keyword searches across all mailboxes.
- Store the search results in a secure mailbox.

You need to recommend a solution that meets the requirements. Which two actions should you recommend? (Each correct answer presents part of the solution. Choose two.)

- A. Perform searches from the Exchange Control Panel, and export search results to a discovery mailbox.
- B. Add members of the Legal security group to the Organization Management role group.
- C. Perform searches by running the Export-Mailbox cmdlet, and export search results to a discovery mailbox.
- D. Add members of the Legal security group to the Discovery Management role group.

Answer: A, D

Question: 153

A corporate environment includes Exchange Server 2010. You need to recommend a solution that enables only support technicians to manage their Exchange Server 2010 distribution group configurations. What should you recommend?

- A. Replace the default role assignment policy.
- B. Add a management role group delegate.
- C. Create a management role assignment policy.
- D. Add a management role.

Answer: C

Question: 154

A corporate environment includes Exchange Server 2010. The Exchange Server environment includes two Client Access servers that are load balanced by a hardware load balancer. The load balancer is configured to perform SSL offloading only when users access Outlook Web App (OWA). You need to recommend a solution for ensuring that passwords are never transmitted in clear text when users access OWA . What should you recommend?

- A. Modify the internal URI on the Client Access servers.
- B. Enable integrated Windows authentication.
- C. Modify the external URI on the Client Access servers.
- D. Enable forms-based authentication.

Answer: B

Question: 155

A corporate environment includes client computers that run Windows 7 and Microsoft Outlook 2010. The client computers are joined to an Active Directory Domain Services (AD DS) domain. Email services are provided by a cloud-

based Exchange Server 2010 SP1 service provider. You need to recommend a method for automatically protecting email messages that contain the phrase Top Secret in the subject line from being read by unauthorized users. In addition, you need to ensure that those messages are protected in the message senders Sent Items folder. What should you recommend?

- A. Implement message classification and an associated transport rule.
- B. Use Active Directory Rights Management Services (AD RMS) and Information Rights Management (IRM) transport rules.
- C. Use Active Directory Rights Management Services (AD RMS) and Outlook protection rules.
- D. Use Secure/Multipurpose Internet Mail Extensions (S/MIME).

Answer: C

Question: 156

A corporate environment includes Exchange Server 2010 and Active Directory Domain Services (AD DS). Client computers run Windows 7 and Microsoft Outlook 2010. A transport rule is configured to apply a disclaimer to all outbound email messages. The transport rule is not applying the disclaimer to encrypted email messages. You need to recommend a solution that allows the existing transport rule to apply the disclaimer to encrypted email messages. What should you recommend?

- A. Mutual Transport Layer Security (MTLS)
- B. message classification
- C. Active Directory Rights Management Services (AD RMS)
- D. Secure/Multipurpose Internet Mail Extensions (S/MIME)

Answer: C

Explanation:

Information workers exchange sensitive information such as financial reports and data, customer and employee information, and confidential product information and specifications, by e-mail everyday. In Microsoft Exchange Server 2010, Microsoft Outlook, and Microsoft Office Outlook Web App, users can apply Information Rights Management (IRM) protection to messages by applying an Active Directory Rights Management Services (AD RMS) rights policy template. This requires an AD RMS deployment in the organization. For more information about AD RMS, see Active Directory Rights Management Services.

However, when left to the discretion of users, messages may be sent in clear text without IRM protection. In organizations that use e-mail as a hosted service, there's a risk of information leakage as a message leaves the client and is routed and stored outside the boundaries of an organization. Although e-mail hosting companies may have well-defined procedures and checks to help mitigate the risk of information leakage, after a message leaves the boundary of an organization, the organization loses control of the information. Outlook protection rules can help protect against this type of information leakage.

Automatic IRM Protection in Outlook 2010

In Exchange 2010, Outlook protection rules help your organization protect against the risk of information leakage by automatically applying IRM-protection to messages in Outlook 2010. Messages are IRM-protected before they leave the Outlook client. This protection is also applied to any attachments using supported file formats. When you create Outlook protection rules on an Exchange 2010 server, the rules are automatically distributed to Outlook 2010 by using Exchange Web Services. For Outlook 2010 to apply the rule, the AD RMS rights policy template you specify must be available on users' computers.

Important: If a rights policy template is removed from the AD RMS server, you must modify any Outlook protection rules that use the removed template. If an Outlook protection rule continues to use a rights policy template that's

been removed, and transport decryption is enabled in the organization, the Decryption agent will fail to decrypt the message protected with a template that's no longer available. If transport decryption is configured as mandatory, the Hub Transport server will reject the message and send a non-delivery report (NDR) to the sender. For more details about transport decryption, see Understanding Transport Decryption. For more details about AD RMS rights policy templates, see AD RMS Policy Template Considerations.

In Windows Server 2008, rights policy templates can be archived instead of deleted. Archived templates can still be used to license content, but when you create or modify an Outlook protection rule, archived templates aren't included in the list of templates.

Outlook protection rules are similar to transport protection rules. Both are applied based on message conditions, and both protect messages by applying an AD RMS rights protection template. However, transport protection rules are applied on the Hub Transport server by the Transport Rules agent. Outlook protection rules are applied in Outlook 2010, before the message leaves the user's computer. Messages protected by an Outlook protection rule enter the transport pipeline with IRM protection already applied. Additionally, messages protected with an Outlook protection rule are also saved in an encrypted format in the Sent Items folder of the sender's mailbox.

Question: 157

A corporate environment includes an on-premise deployment of Exchange Server 2010 SP1 with stand-alone Edge Transport servers in a perimeter network. The company plans to move a subset of Exchange users to a cloud-based Exchange Server 2010 SP1 service. The security team has the following requirements:

- Manage mailbox audit logging for the on-premise and cloud-based Exchange servers.
- Search message tracking logs for all on-premise Exchange servers.

You need to recommend a solution that meets the requirements. What should you recommend?

- A. Use group policy to manage audit settings. Add the security team members to the local Administrators group on each of the on-premise Exchange servers.
- B. Add the security team members to the Organization Management, Recipient Management, and Records Management management role groups in both environments. Add the security team members to the local Administrators group on each of the on-premise Exchange servers.
- C. Use group policy to manage audit settings. Add the security team members to the Server Management management role group in both environments.
- D. Add the security team members to the Organization Management, Recipient Management, Records Management, and Server Management management role groups in both environments.

Answer: B

Question: 158

A corporate environment includes Exchange Server 2010. Users currently access mailboxes remotely by using Outlook Web App (OWA). You need to recommend a method of identifying the browser types and versions used to access OWA . What should you recommend?

- A. Analyze the message tracking log files.
- B. Analyze the IIS log files.
- C. Run the Exchange Remote Connectivity Analyzer.
- D. Run the Tracking Log Explorer.

Answer: B

Question: 159

A corporate environment includes an on-premise deployment of Exchange Server 2010 SP1.

The company intends to migrate to a cloud-based Exchange Server 2010 SP1 service. The security team needs to perform the following tasks:

- Search multiple mailboxes for messages that meet specific criteria.
- Store search results in a specific mailbox.

You need to recommend a solution for enabling security team members to perform the tasks. To which group should you recommend the security team members be assigned?

- A. the Domain Admins security group
- B. the Discovery Management role-based access control (RBAC) role group
- C. the Enterprise Admins security group
- D. the Records Management role-based access control (RBAC) role group

Answer: B

Question: 160

A corporate environment includes Exchange Server 2010. The Exchange Server environment includes one Mailbox server, one Client Access server, one Hub Transport server, and one Edge Transport server. You need to recommend a solution for inserting specific text in every email message as it is sent. What should you recommend?

- A. Create a transport rule on the Hub Transport server.
- B. Create a send connector on the Hub Transport server.
- C. Create a transport rule by using an Active Directory Rights Management Services (AD RMS) template.
- D. Create a transport rule on the Edge Transport server.

Answer: A

Question: 161

A corporate environment will include Exchange Server 2010. You are designing a deployment plan for the Mailbox servers. You need to recommend the minimum amount of physical memory that supports the following requirements:

- Use single-role Mailbox servers.
- Each Mailbox server must support 22.5 GB of database cache.

How much memory should you recommend?

- A. 64 GB
- B. 24 GB
- C. 48 GB
- D. 32 GB

Answer: D

Explanation:

Default mailbox database cache sizes

Server physical memory (RAM)	Database cache size: (Mailbox role only)
2GB	512 MB
4GB	1 GB
8GB	3.6 GB
16GB	10.4 GB
24GB	17.6 GB
32GB	24.4 GB
48GB	39.2 GB
64GB	53.6 GB
96GB	82.4 GB
128GB	111.2 GB

Question: 162

You are designing an Exchange organization for a company named Contoso, Ltd. All servers in the organization will have Exchange Server 2010 Service Pack 1 (SP1) installed. Contoso has a partner company named Fabrikam, Inc. Fabrikam has an Exchange organization that contains only Exchange Server 2010 SP1 servers. You plan to configure a federation trust between Fabrikam and Contoso. You need to recommend a certificate for the federation trust. Which of the following certificates is the best recommendation? (More than one answer choice may achieve the goal. Select the BEST answer.)

- A. a certificate from a third-party certification authority (CA)
- B. the self-signed certificate automatically generated by the Exchange 2010 Setup wizard
- C. the self-signed certificate automatically generated by the New Federation Trust wizard
- D. a certificate from an internal certification authority (CA)

Answer: C

Explanation:

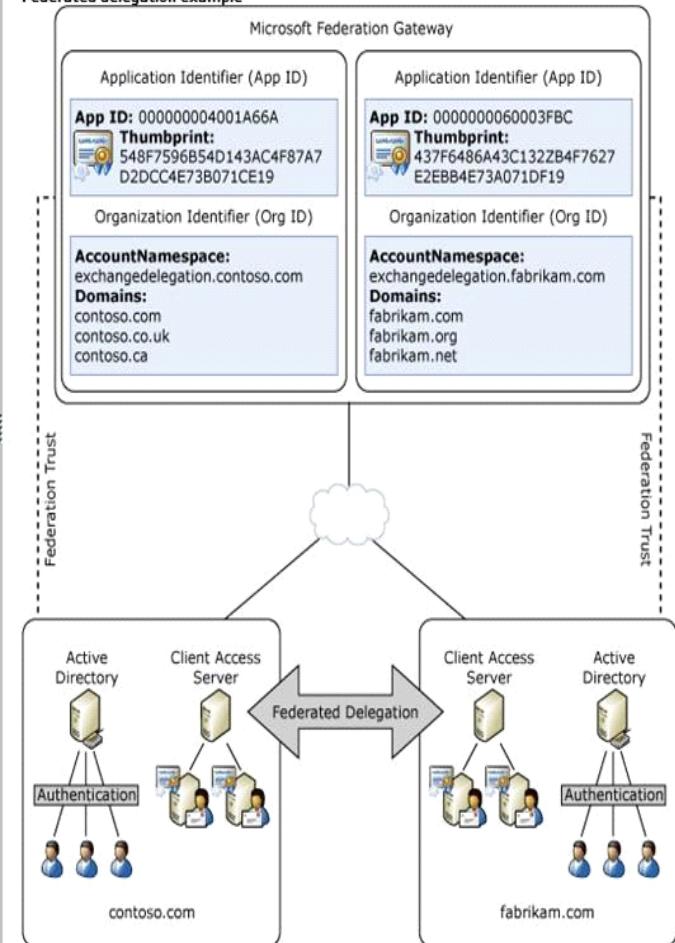
Federation Example

Two Exchange organizations, Contoso, Ltd. and Fabrikam, Inc., want their users to be able to share free/busy information with each other. Each organization creates and configures its account namespace to include the domain used for its user's e-mail address domain.

Contoso employees use one of the following e-mail address domains: contoso.com, contoso.co.uk, or contoso.ca. Fabrikam employees use one of the following: fabrikam.org, or fabrikam.net. Both organizations make sure that all accepted e-mail domains are included in the account namespace for their federation trust without requiring a complex Active Directory forest or domain trust configuration between the two organizations, both organizations configure an organization relationship.

The following figure illustrates the federation configuration between Contoso, Ltd. and Fabrikam, Inc.

Federated delegation example



Certificate Requirements for Federation

To establish a federation trust with the Microsoft Federation Gateway, either a self-signed certificate or an X.509 certificate signed by a certification authority (CA) server used to create the trust. We recommend using a self-signed certificate, which can be automatically created and installed using the New Federation Trust wizard and encrypt delegation tokens used for federated delegation. Only one certificate is required for the federation trust. Exchange 2010 automatically distributes the organization.

Question: 163

You are the enterprise administrator for an Exchange Server 2010 organization. All users run Microsoft Office Outlook 2010. You are designing a sharing solution for your organization and a partner organization. The partner organization also uses Exchange Server 2010. You need to recommend a strategy for sharing information with the partner organization to meet the following requirements:

- Provide cross-organizational access to user contacts
- Provide cross-organizational access to free\busy information

- A. Implementing Microsoft Identify Lifecycle Manager (ILM) 2007
- B. Implementing Federated Delegation
- C. Running the Microsoft Exchange Inter-Organization Replication tool
- D. Creating cross-forest trusts

Answer: B

Explanation:

Information workers frequently need to collaborate with external recipients, vendors, partners, and customers and share their free/busy (also known as calendar availability) and contact information. Federation in Microsoft Exchange Server 2010 helps with these collaboration efforts. Federation refers to the underlying trust infrastructure that supports federated delegation, an easy method for users to share calendar and contact information with recipients in other external federated organizations. To learn more about federated delegation, see Understanding Federated Delegation.

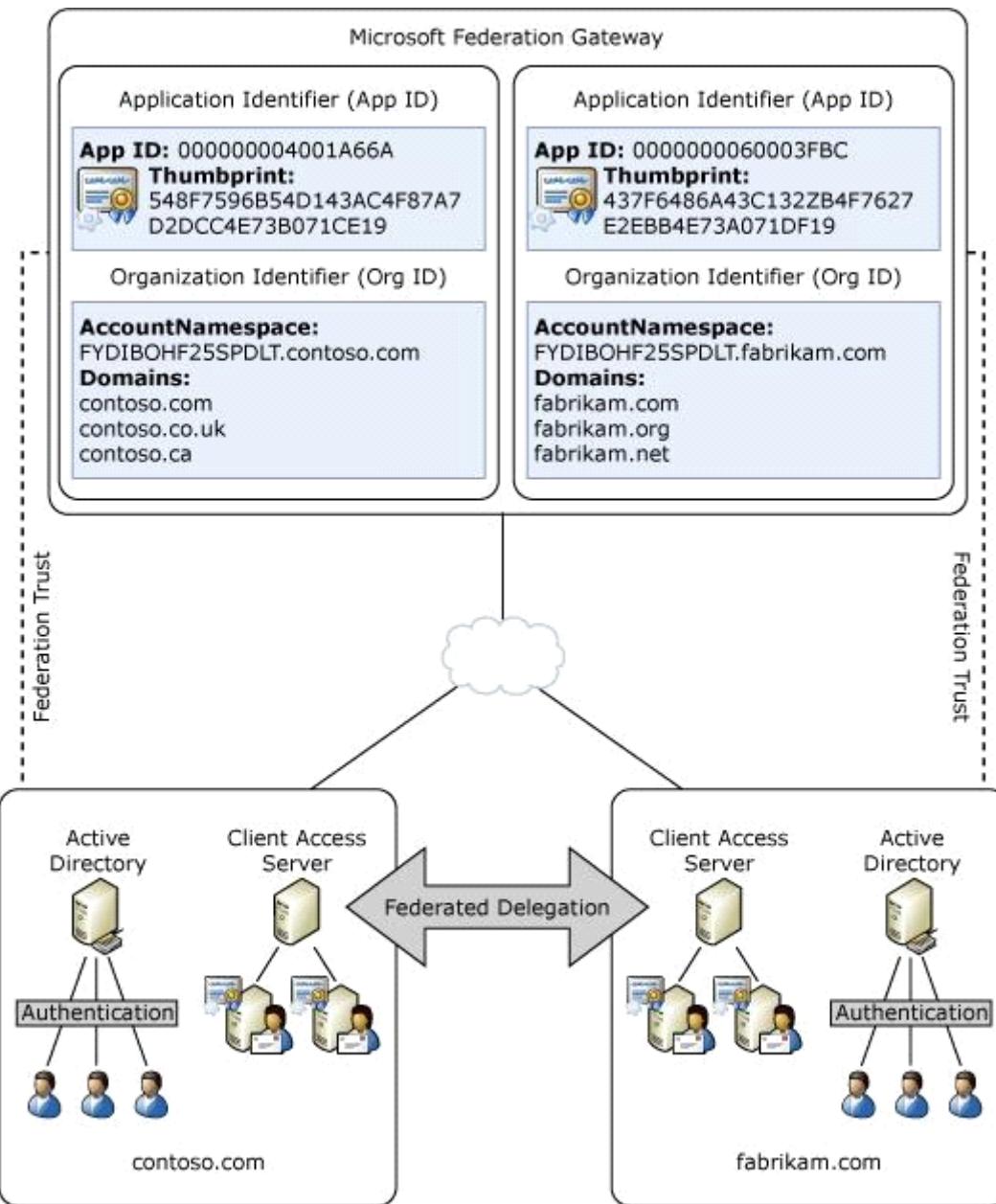
Example:

Two Exchange organizations, Contoso, Ltd. and Fabrikam, Inc., want their users to be able to share free/busy information with each other. Each organization creates a federation trust with the Microsoft Federation Gateway and configures its account namespace to include the domain used for its user's e-mail address domain.

Contoso employees use one of the following e-mail address domains:

contoso.com, contoso.co.uk, or contoso.ca. Fabrikam employees use one of the following e-mail address domains: fabrikam.com, fabrikam.org, or fabrikam.net. Both organizations make sure that all accepted e-mail domains are included in the account namespace for their federation trust with the Microsoft Federation Gateway. Rather than requiring a complex Active Directory forest or domain trust configuration between the two organizations, both organizations configure an organization relationship with each other to enable free/busy sharing.

The following figure illustrates the federation configuration between Contoso, Ltd. and Fabrikam, Inc.



Question: 164

Contoso, Ltd. has an Exchange Server 2010 environment that accepts email for the contoso.com email domain. Fabrikam, Inc. has an Exchange Server 2010 environment that accepts mail for the fabrikam.com email domain. Contoso acquires Fabrikam and establishes an internal network connection between the two companies. After the acquisition, only the Contoso Exchange Server environment accepts external email. You have the following requirements:

- Retain existing fabrikam.com email addresses.
- Enable users in both Exchange Server environments to receive mail at contoso.com email addresses.

You need to recommend a solution that meets the requirements. Which two actions should you recommend? (Each correct answer presents part of the solution. Choose two.)

- Create an internal relay accepted domain for contoso.com.
- Create an external relay accepted domain for contoso.com.
- Create an internal receive connector.

D. Create an internal send connector.

Answer: A, D

Question: 165

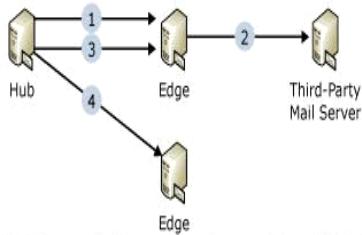
A corporate environment includes Exchange Server 2010 SP1. The Exchange Server environment includes two Client Access servers, two Hub Transport servers, and two Mailbox servers on the internal network, and two Edge Transport servers in a perimeter network. An edge subscription is in place between the Hub Transport servers and the Edge Transport servers. When an Edge Transport server fails, messages accepted by that server are not delivered. You need to recommend a solution for ensuring that messages accepted by either Edge Transport server are attempted for delivery if either Edge Transport server fails. What should you recommend?

- A. Enable shadow redundancy.
- B. Create a new remote domain.
- C. Create a new send connector.
- D. Enable back pressure.

Answer: A

Explanation:

Message flow with shadow redundancy



In this scenario, the message flow goes through following stages:

1. The Hub Transport server delivers a message to the Edge Transport server.
 - a. The Hub Transport server opens an SMTP session with the Edge Transport server.
 - b. The Edge Transport server advertises shadow redundancy support.
 - c. The Hub Transport server notifies the Edge Transport server to track discard status.
 - d. The Hub Transport server submits the message to the Edge Transport server.
 - e. The Edge Transport server acknowledges the receipt of the message and records the Hub Transport server identity for sending discard information.
 - f. The Hub Transport server moves the message to the shadow queue for the Edge Transport server and marks the Edge Transport server as the primary server. The server becomes the shadow server.
2. The Edge Transport server delivers the message to the next hop.
 - a. The Edge Transport server submits the message to a third-party mail server.
 - b. The third-party mail server acknowledges the receipt of the message.
 - c. The Edge Transport server updates the discard status for the message as delivery complete.
3. The Hub Transport server queries the Edge Transport server for discard status (success case).
 - a. At the end of each SMTP session with the Edge Transport server, the Hub Transport server queries the Edge Transport server for discard status. If the Hub Transport server hasn't opened any SMTP sessions with the Edge Transport server after the initial message submission, it will open another Transport server just to query for the discard status after a specific amount of time.
 - b. The Edge Transport server checks the local discard status and sends back the list of messages that have been delivered, and removes the discarded messages.
 - c. The Hub Transport server deletes the list of messages from its shadow queue.
4. The Hub Transport server queries the Edge Transport server for the discard status and resubmits the message (failure case).
 - a. If the Hub Transport server can't contact the Edge Transport server, the Hub Transport server resumes the primary server role and resubmits the message.
 - b. Resubmitted messages are delivered to another Edge Transport server and the workflow starts from stage 1.

Question: 166

Your company has offices in New York and Miami. The offices connect to each other by using a dedicated WAN link. Each office has a direct connection to the Internet. An Active Directory site exists for each office. Each office contains one Mailbox server, two Hub Transport servers, and two Client Access servers. All servers have Exchange Server 2010 Service Pack 1 (SP1) installed and run Windows Server 2008 R2. The Mailbox servers are configured as shown in the following table.

Mailbox server name	Mailbox database name	Number of mailboxes	Office location
MBX-01	MDB-01	300	New York
MBX-02	MDB-02	1,000	Miami

You need to recommend a high-availability solution for the Mailbox servers that meets the following requirements:

- The mailbox databases must be automatically available if a single Mailbox server fails.
- The mailbox databases must be automatically available if the WAN link between the offices fails.
- The mailbox databases must be available if all of the Exchange servers in an office become unavailable, after an administrator performs a manual failover.

Which of the following solutions is the best recommendation? (More than one answer choice may achieve the goal. Select the BEST answer.)

A. Add a Mailbox server to each office.

Create one database availability group (DAG).

Add all Mailbox servers to the DAG.

Add a file share witness to the Miami office.

Create a copy of each mailbox database.

B. Add a Mailbox server to each office.

Create two database availability groups (DAGs).

Add one Mailbox server from each office to each DAG.

Add a file share witness to each office.

Create a copy of each mailbox database.

C. Add two Mailbox servers to the Miami office.

Add one Mailbox server to the New York office.

Create two database availability groups (DAGs).

Add all of the Mailbox servers in the Miami office to one of the DAGs.

Add all of the Mailbox servers in the New York office to the other DAG.

Add a file share witness to each office. Create a copy of each mailbox database.

D. Add two Mailbox servers to each office.

Create one database availability group (DAG).

Add all of the Mailbox servers in the Miami office to the DAG.

Add a file share witness to the New York office.

Create a copy of each mailbox database.

Answer: A

Question: 167

A corporate environment will include Exchange Server 2010 in two Active Directory Domain Services (AD DS) sites. You need to recommend a solution that provides a single connection point for all Outlook Web App (OWA) connections. What should you recommend?

A. Deploy one Client Access server array for each AD DS site.

B. Deploy one Client Access server array.

- C. Configure a hardware load balancer for the Client Access servers.
- D. Configure Autodiscover in each AD DS site for a common internal URL.

Answer: C

Explanation:

In an organization that has multiple Active Directory sites and multiple Client Access in each site, you can use Network Load Balancing (NLB) to load balance traffic proxies between the Client Access servers in each site and for users directly accessing those servers. Just deploying a load balancer isn't enough ensure traffic is balanced effectively. You must also perform some additional configuration of the InternalURL and ExternalURL properties. We recommend you include only Client Access servers within the same Active Directory site in a load-balancing array. You can deploy NLB in an Internet-facing Active Directory site and in a non-Internet-facing Active Directory site.

Question: 168

A corporate environment will include Exchange Server 2010. You need to recommend a solution that meets the following client access requirements:

- Automatic failover of specific client access protocols
- Distribution of client access traffic across multiple Client Access servers
- Secure Sockets Layer (SSL) session ID for client-to-Client Access server affinity

What should you recommend?

- A. Deploy a Client Access server array.
- B. Deploy Microsoft Forefront Unified Access Gateway (UAG) as a reverse proxy.
- C. Deploy a hardware load balancer for the Client Access servers.
- D. Deploy Microsoft Forefront Threat Management Gateway (TMG) as a reverse proxy.

Answer: C

Explanation:

Hardware Load Balancing

If you have more than eight Client Access servers in a single Active Directory site, your organization will need a more robust load balancing solution. Although software load balancing solutions available, a hardware load balancing solution provides the most capacity solutions, see Microsoft Unified Communications Hardware Load Balancer Deployment. For more information about Exchange 2010 server solution, see Microsoft Unified Hardware Load Balancing Hardware Load Balancer Deployment. Hardware load balancers support very high traffic throughput and can be configured to load balance in many ways. Most hardware load balancer vendors have documentation about how their product works with Exchange 2010. The simplest way to configure hardware load balancers is to create a fallback list of the be applied by the load balancer. For example, the load balancer will try cookie-based affinity first, then SSL session ID, and then source IP affinity.

Question: 169

A corporate environment includes a two-node Exchange Server 2010 Client Access server array. You are designing a disaster recovery plan for the Client Access servers. The plan must meet the following requirements:

- Back up the SSL certificates.
- Back up the Windows Network Load Balancing (NLB) configuration.
- Back up only the minimum amount of data.

You need to recommend the components to back up on each Client Access server. What should you recommend?

- A. the system state and the registry
- B. only the system state
- C. the registry and the system volume
- D. the system state and the system volume

Answer: B

Explanation:

However not all of the settings for these Client Access server features are stored in Active Directory.

System State – the system state of the Client Access server stores important information such as the SSL certificates installed on the server, and service configuration information (eg dependencies and startup options). If the server is a member of an [Exchange 2010 CAS array](#) the NLB configuration is also stored in the system state. Finally if there are other applications installed on the server then those will likely have settings stored in the registry as well.

Question: 170

A company deploys Exchange Server 2010. The environment includes three datacenters located in New York, Dallas and Miami. Each datacenter is configured as an Active Directory Domain Services (AD DS) site. Each site has one Client Access server, one Hub Transport server and one Mailbox server. The Mailbox servers in New York and Dallas are configured in a database availability group (DAG). You have the following requirements:

- Ensure that mail flow is not interrupted if any one Hub Transport server fails.
- Deploy the minimum number of additional servers.

You need to recommend a solution that meets the requirements. What should you recommend?

- A. Deploy one additional Hub Transport server in New York and one additional Hub Transport server in Dallas.
- B. Add the Hub Transport role to the Client Access server in Miami.
- C. Deploy one additional Hub Transport server in each site.
- D. Deploy one additional Hub Transport server in Miami.

Answer: C

Question: 171

A corporate environment will include Exchange Server 2010. You are planning capacity for the Mailbox servers. You require 800 GB of disk space for mailbox content. You need to recommend the minimum amount of additional space required for content indexing. What should you recommend?

- A. 160 GB
- B. 96 GB
- C. 120 GB
- D. 80 GB

Answer: D

Explanation:

Content Indexing

Content indexing creates an index, or catalog, that allows users to easily and quickly search through their mail items

rather than manually search through the mailbox, Which is placed on the same LUN as the database. Therefore, an additional 10 percent needs to be factored into the database LUN size for content indexing.

Question: 172

You have an Exchange organization. All servers in the organization have Exchange Server 2010 Service Pack 1 (SP1) installed. The organization contains the servers configured as shown in the following table.

Server name	Server role
Edge1	Edge Transport
Edge2	Edge Transport
Hub1	Hub Transport
Hub2	Hub Transport
CAS1	Client Access
CAS2	Client Access
MBX1	Mailbox
MBX2	Mailbox

You plan to deploy a line-of-business application named App1. App1 will have a built-in SMTP service that will send e-mail messages to users in the Exchange organization. You need to recommend a message routing solution that meets the following requirements:

- Ensures that App1 can send e-mail messages to internal users.
- Prevents other servers on the internal network from sending e-mail messages to internal users.
- Ensures that each e-mail message received by the Exchange organization is scanned for viruses.

You install Microsoft Forefront Protection 2010 for Exchange Server on both Edge Transport servers. Which of the following solutions is the best recommendation? (More than one answer choice may achieve the goal. Select the BEST answer.)

- A. On Edge1, create a new internal Receive connector. From the properties of the new Receive connector, configure the Remote Network settings to include the IP address of App1, and then add the Anonymous users permission group to the Receive connector. From the properties of the default internal Receive connector on Edge1, exclude the IP addresses of the internal network. On the server that hosts App1, configure the SMTP service to relay e-mail to Edge1.
- B. On Hub1, install Forefront Protection 2010 for Exchange Server. On Hub1, create a new internal Receive connector, and then configure the Remote Network settings to include the IP address of App1. On the server that hosts App1, configure the SMTP service to relay e-mail directly to Hub1.
- C. From the properties of the default Receive connector on Edge1, configure the Remote Network settings to include the IP address of App1, and then add the Anonymous users permission group to the Receive connector. On the server that hosts App1, configure the SMTP service to relay e-mail to Edge1.
- D. On Hub1, install Forefront Protection 2010 for Exchange Server. On Hub1, add the Anonymous users permission group to the default Receive connector. On an internal DNS server, create a Mail Exchanger (MX) record that points to Hub1. On the server that hosts App1, configure the SMTP service to relay e-mail by using DNS name resolution.

Answer: B

Question: 173

A company has an on-premise Exchange Server 2010 SP1 environment. Client computers are joined to an Active Directory Domain Services (AD DS) domain. Some users are hosted in a cloud-based Exchange Server 2010 SP1 environment. An organization relationship exists between the on-premise and cloud-based environments. Administrative assistants with mailboxes in the on-premise environment must be able to view contacts in cloud-based user mailboxes. You need to recommend a solution that meets the requirement. What should you recommend?

- A. a federation trust
- B. a sharing policy
- C. a remote domain
- D. an Outlook protection rule

Answer: B

Explanation:

Create a Sharing Policy

Applies to: Exchange Server 2010 SP1

Topic Last Modified: 2011-03-19

You can use sharing policies to control how users in your organization can share calendar and contact information with users outside your Exchange organization, external non-federated organizations, and individuals with Internet access. To configure recipients to use a specific sharing policy, see Apply a Sharing Policy to Mailboxes.

Question: 174

An organization plans to deploy Exchange Server 2010 in multiple Active Directory Domain Services (AD DS) sites. The locations of the Client Access servers are as shown in the following table.

Server name	AD DS site	Internet facing
CAS01	Chicago	Yes
CAS02	New York	No

Users will access Autodiscover, Outlook Web App (OWA), Exchange ActiveSync, and Outlook Anywhere only over the Internet through the URL mail.contoso.com. Users must be able to connect to all of the services via an SSL connection without receiving errors or warning messages. You need to recommend an SSL certificate configuration. In addition, you need to minimize the number of certificates purchased. Which two actions should you recommend? (Each correct answer presents part of the solution. Choose two.)

- A. Use the existing self-signed certificate on CAS02.
- B. Use the existing self-signed certificate on CAS01.
- C. Purchase a third-party SSL certificate for CAS01 containing the autodiscover.contoso.com and mail.contoso.com FQDNs.
- D. Purchase a third-party SSL certificate for CAS02 containing the autodiscover.contoso.com and mail.contoso.com FQDNs.

Answer: A, C

Question: 175

Contoso, Ltd. has an Exchange Server 2010 environment. Fabrikam, Inc. has an Exchange Server 2007 environment. Contoso acquires Fabrikam. Contoso plans to migrate the email accounts of the Fabrikam employees to the existing Contoso Exchange Server environment. Fabrikam employees will have new Contoso email addresses and will also maintain their existing Fabrikam email addresses for a period of time. You need to recommend a solution for ensuring that replies to email messages sent by Fabrikam employees prior to the migration are directed to the migrated mailboxes. What should you recommend?

- A. In the Exchange Management Console (EMC) in the Contoso Exchange Server environment, set the primary email address to the Fabrikam email address.

- B. After the mailbox migration, run the Update-EmailAddressPolicy cmdlet for each email address policy.
- C. Export the legacyExchangeDN attributes from the Fabrikam mailboxes and add them as custom X500 addresses on the new Contoso mailboxes.
- D. In the Exchange Management Console (EMC) in the Contoso Exchange Server environment, add the Fabrikam domain name to the Accepted Domains list as an authoritative domain.

Answer: C

Explanation:

Things you need to know if you are moving from an external Exchange environment to Rackspace's Hosted Exchange 2007. An Exchange server uses an internal addressing scheme that routes messages between mailboxes it hosts. These addresses are known as LegacyExchangeDN addresses or they are sometimes referred to as x500 addresses. When you send and receive messages on your current providers Exchange service these LegacyExchangeDN addresses are saved with sent and received messages in your inbox. They are also saved within your AutoComplete cache in Outlook. When you reply to or forward existing emails that are migrated over to our system, without first importing the x500 addresses, a bounce will likely be returned if Outlook uses the old x500 address. The bounce will resemble the following non-delivery report:

Diagnostic information for administrators:

```
Generating server: IAD2HUB06.mex02.mlsvr.com
IMCEAEX-_O=FIRST+20ORGANIZATION_OU=FIRST+20ADMINISTRATIVE
+20GROUP_CN=RECIPIENTS_CN=user@mex02.mlsvr.com
#550 5.1.1 RESOLVER.ADR.ExRecipNotFound; not found ##
~~~~~
```

If you still have access to your old Exchange server, you or your current provider will need to export your LegacyExchangeDN and provide the CSV file to us via a support ticket. We will then get our Exchange engineering specialists to upload the LegacyExchangeDN export into our environment. This will ensure that when you reply to or forward existing messages, even if the x500 is referenced, it will deliver to the correponding mailbox. For a quick reference the following can be keyed into a Exchange server to retrieve the legacy data:

Question: 176

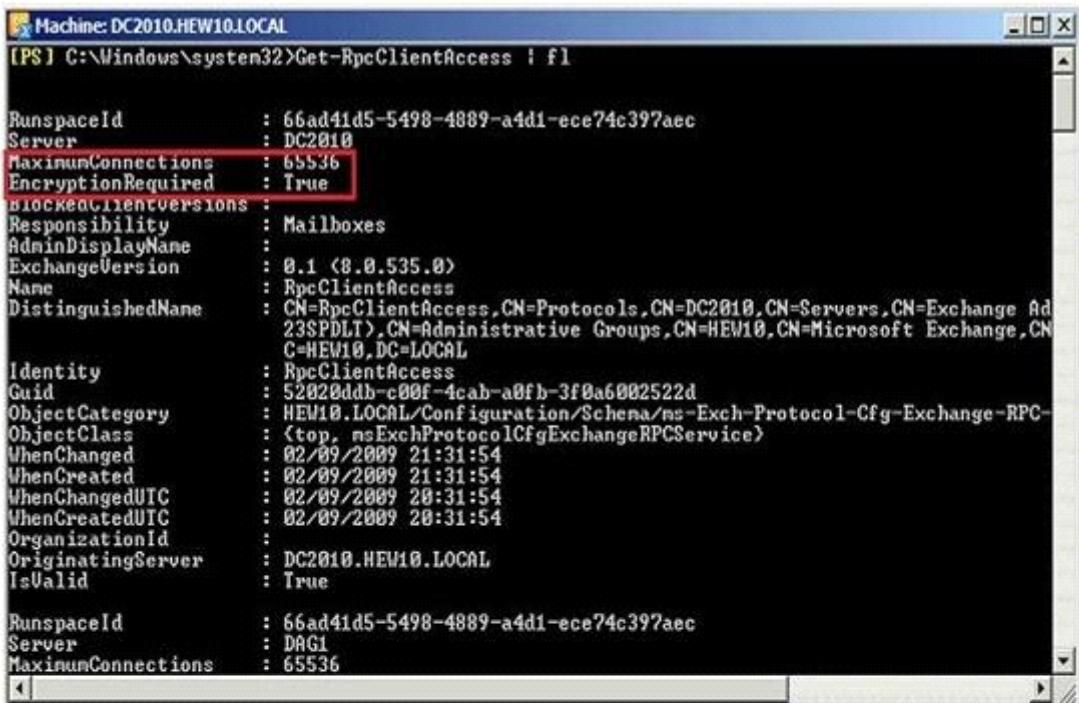
A corporate environment includes Exchange Server 2003 SP2. Client computers run Microsoft Office Outlook 2003. You deploy Exchange Server 2010 in the existing Exchange organization, and then install Exchange Server 2010 SP1 on all the Exchange Server 2010 servers. The company intends to move mailboxes from Exchange Server 2003 SP2 to Exchange Server 2010 SP1. You need to recommend a solution for ensuring that after their mailboxes are moved, users can open their mailboxes by using Outlook 2003. What should you recommend?

- A. Obtain and install an SSL certificate for each Exchange Server 2010 SP1 Client Access server.
- B. Configure Outlook 2003 to encrypt data between Outlook and the Exchange server.
- C. Obtain and install an SSL certificate for each Exchange Server 2010 SP1 Mailbox server.
- D. Configure Outlook 2003 to use NTLM authentication.

Answer: B

Explanation:

Now that we know about the new RPC Client Service running on the 2010 CAS Server, lets bring up the full info by running Get-RpcClientAccess | fl



```
[PS] C:\Windows\system32>Get-RpcClientAccess | fl

RunspaceId      : 66ad41d5-5498-4889-a4d1-ece74c397aec
Server          : DC2010
MaximumConnections : 65536
EncryptionRequired : True
BlockNonClientVersions :
Responsibility   : Mailboxes
AdminDisplayName  :
ExchangeVersion  : 0.1 <8.0.535.0>
Name             : RpcClientAccess
DistinguishedName: CN=RpcClientAccess,CN=Protocols,CN=DC2010,CN=Servers,CN=Exchange Admins,CN=SPDLT,CN=Administrative Groups,CN=HEW10,CN=Microsoft Exchange,CN=C=HEW10,DC=LOCAL
Identity         : RpcClientAccess
Guid             : 52020ddb-c00f-4cab-a0fb-3f0a6002522d
ObjectCategory   : HEW10.LOCAL\Configuration\Schema\ms-Exch-Protocol-Cfg-Exchange-RPC-Service
ObjectClass      : <top, msExchProtocolCfgExchangeRPCService>
WhenChanged      : 02/09/2009 21:31:54
WhenCreated      : 02/09/2009 21:31:54
WhenChangedUIC   : 02/09/2009 20:31:54
WhenCreatedUIC   : 02/09/2009 20:31:54
OrganizationId   :
OriginatingServer: DC2010.HEW10.LOCAL
IsValid          : True

RunspaceId      : 66ad41d5-5498-4889-a4d1-ece74c397aec
Server          : DAG1
MaximumConnections : 65536
```

We can see that this service needs rpc encryption and it is set to True by default. Same is the case with Outlook 2007 & 2010 profiles! Encryption between Outlook and Exchange is enabled by default, which explains why these clients can connect to Exchange 2010 without any issues. Outlook 2003 profiles don't enable encryption by default.



Question: 177

A corporate environment will include client computers that run Microsoft Outlook 2010. Email services will be provided to some users by a cloud-based Exchange Server 2010 SP1 service provider and to other users by an on-premise deployment of Exchange Server 2010 SP1. You need to recommend a solution that will allow users in the cloud-based environment to receive internal Out of Office replies from users in the on-premise environment. What should you recommend?

- A. Create an accepted domain.
- B. Create a transport rule.

- C. Create a remote domain.
- D. Create an organization relationship.

Answer: D

Explanation:

You can create an organization relationship with an external federated Microsoft Exchange Server 2010 organization for the purpose of sharing calendar availability (free/busy) information. Note: Creating an organization relationship is one of several steps in setting up federated delegation in your Exchange 2010 organization. To review all the steps, see Configure Federated Delegation.

Question: 178

A corporate environment includes Exchange Server 2010. The Exchange Server environment includes two Hub Transport servers, two Client Access servers, and two Mailbox servers on the internal network and two stand-alone Edge Transport servers in the perimeter network. The Mailbox servers are in a database availability group (DAG). You are designing a solution to allow a third-party application to send email messages to both internal users and external users.

You have the following requirements:

- Ensure that the third-party application can use domain-based NTLM authentication method for outgoing messages.
- Ensure that if only one server has a hardware failure, all outgoing messages are accepted for delivery.
- Minimize the cost of the solution.

You need to recommend a solution that meets the requirements. What should you recommend?

- A. Configure DNS round-robin rotation for SMTP connections to the Mailbox servers
- B. Deploy a hardware load balancer for SMTP connections to the Edge Transport servers
- C. Configure DNS round-robin rotation for SMTP connections to the Edge Transport servers
- D. Deploy a hardware load balancer for SMTP connections to the Hub Transport servers

Answer: D

Question: 179

You are designing an Exchange Server 2010 environment. The environment will include three datacenters, located in Seattle, Dallas, and Miami. Each datacenter will have a separate Active Directory Domain Services (AD DS) site. The Seattle and Miami datacenters will each contain two Mailbox servers. The Dallas datacenter will not contain Mailbox servers. All Mailbox servers will be members of a single database availability group (DAG). You need to recommend the minimum file share witness configuration necessary to ensure that if the Seattle datacenter fails, the DAG will continue to function. What should you recommend?

- A. No file share witnesses are necessary.
- B. Place one file share witness in the Seattle datacenter.
- C. Place one file share witness in the Seattle datacenter and one alternate file share witness in the Miami datacenter.
- D. Place one file share witness in the Dallas datacenter.

Answer: D

Explanation:

DAG Witness Server and Witness Directory

When creating a DAG, you need to specify a name for the DAG no longer than 15 characters that's unique within the Active Directory forest. In addition, each DAG is configured with a witness server and witness directory. The witness server and its directory are used only for quorum purposes where there's an even number of members in the DAG. You don't need to create the witness directory in advance. Exchange automatically creates and secures the directory for you on the witness server. The directory shouldn't be used for any purpose other than for the DAG witness server.

The requirements for the witness server are as follows:

- The witness server can't be a member of the DAG.
- The witness server must be in the same Active Directory forest as the DAG.
- The witness server must be running Windows Server 2008 R2, Windows Server 2008, Windows Server 2003 R2, or Windows Server 2003.
- A single server can serve as a witness for multiple DAGs. However, each DAG requires its own witness directory.

We recommend that you use an Exchange 2010 Hub Transport server in the Active Directory site containing the DAG. This allows the witness server and directory to remain under the control of an Exchange administrator. Regardless of what server is used as the witness server, if the Windows Firewall is enabled on the intended witness server, you must enable the Windows Firewall exception for File and Printer Sharing.

Note:

You can also use the **Set-DatabaseAvailabilityGroup** cmdlet to configure the witness server and witness directory in the original location if the witness server lost its storage or if someone changed the witness directory or share permissions.

 As a best practice, in an environment where a DAG is extended across multiple datacenters (and Active Directory sites) and configured for site resilience, we recommend that you use a witness server in your primary data center (the data center containing the majority of your user population). If each data center has a similar number of users, the data center you choose to host the witness server is considered to be the primary datacenter from the solution's perspective. If the witness server is in the datacenter with the majority of the client population, the majority of clients retain access after a failure.

 Although it's supported to use a witness server in a third datacenter, we don't recommend this scenario. From an Exchange perspective, this configuration doesn't provide you with greater availability. It's important that you examine the critical path factors if you use a witness server in a third datacenter. For example, if the WAN connection between the primary datacenter and the second and third datacenter fails, the solution in the primary datacenter becomes unavailable.

Question: 180

A corporate environment includes Exchange Server 2010. The Exchange Server environment includes two Edge Transport servers and two Hub Transport servers. The Edge Transport servers process Safe Sender List information from Exchange users and have multiple IP Allow list entries. An edge subscription is in place between the Edge Transport servers and the Hub Transport servers. You need to recommend a solution for configuring a replacement Edge Transport server.

You have the following requirements:

- Recover all the send connector, receive connector, and accepted domains settings.
- Recover all the IP Allow list entries.
- Continue to process Safe Sender List information.

What should you recommend?

- A. Configure a new Edge Transport server, restore from a Windows system state backup, and then use cloned configuration scripts.
- B. Configure a new Edge Transport server, create and import a new edge subscription, and then use cloned configuration scripts.
- C. Configure a new Edge Transport server, create and import a new edge subscription, and then restore from a Windows system state backup.
- D. Restore from a Windows system state backup, configure a new Edge Transport server, and then use cloned configuration scripts.

Answer: B

Explanation:

Collapse All Language Filter : All

Configure Edge Transport Server Using Cloned Configuration

Applies to: Exchange Server 2010 SP1

Topic Last Modified: 2011-04-23

You can use the provided Shell scripts to duplicate the configuration of a computer that has the Microsoft Exchange Server 2010 Edge Transport server role installed. This process is referred to as *cloned configuration*. *Cloned configuration* is the practice of deploying new Edge Transport servers based on the configuration information from a previously configured source server. The configuration information from the previously configured source server is copied and exported to an XML file, which is then imported to the target server.

Edge Transport server configuration information is stored in Active Directory Lightweight Directory Services (AD LDS) and isn't replicated among multiple Edge Transport servers. By using cloned configuration, you can make sure that every Edge Transport server that's deployed in the perimeter network is operating by using the same configuration.

More Resources

Related Help Top

[Configure Edge Tra](#)
[Microsoft Exchange](#)
[Overview of the Ed](#)

Related Blog Arti

[Visit the Exchange](#)

Related Forum Di

[Ask a question](#)
[Visit the forums](#)

[Exchange 2007](#)

[Exchange 2010](#)

Important:

Cloned configuration doesn't duplicate the Edge Subscription settings of a server. The certificates used by the Microsoft Exchange EdgeSync service aren't cloned. You must run the EdgeSync process separately for each Edge Transport server. The Microsoft Exchange EdgeSync service overwrites any settings included in both the configuration information and in EdgeSync replication information.

Question: 181

A corporate environment includes Exchange Server 2010. The Exchange Server environment includes one Client Access server, one Edge Transport server, one Hub Transport server, and one Mailbox server. Email communication between employees in two specific departments is not permitted. You need to recommend a solution for ensuring that email messages from employees in either department are never sent to employees in the other department. What should you recommend?

- A. Create a journal rule.
- B. Create a transport rule on the Hub Transport server.
- C. Create a transport rule on the Edge Transport server.
- D. Configure litigation hold on the mailboxes of the employees in both departments.

Answer: B

Question: 182

A corporate environment includes Exchange Server 2010 SP1. You need to recommend a solution for recording which administrators access specific mailboxes. What should you recommend?

- A. Enable administrator audit logging.
- B. Increase the mailbox logging level.
- C. Enable mailbox audit logging.
- D. Enable object access auditing.

Answer: C

Explanation:

Understanding Mailbox Audit Logging

Applies to: Exchange Server 2010 SP1

Topic Last Modified: 2010-11-17

Because mailboxes can potentially contain sensitive, high business impact (HBI) information and personally identifiable information (PII), it's important that you track who logs on to the mailboxes in your organization and what actions are taken. It's especially important to track access to mailboxes by users other than the mailbox owner. These users are referred to as delegate users.

Using **mailbox audit logging**, you can log mailbox access by mailbox owners, delegates (including administrators with full mailbox access permissions), and administrators. Mailboxes are considered to be accessed by an administrator only in the following scenarios:

- Discovery search is used to search a mailbox.
- The **New-MailboxExportRequest** cmdlet is used to export a mailbox.
- Microsoft Exchange Server MAPI Editor is used to access the mailbox.

When you enable audit logging for a mailbox, you can specify which user actions (for example, accessing, moving, or deleting a message) should be logged for a logon type (administrator, delegate user, or owner). The audit log entries also include important information such as the client IP address, host name, and process or client used to access the mailbox. For items that are moved, the entry includes the name of the destination folder.



For mailboxes such as the Discovery Search Mailbox, which may contain more sensitive information, consider enabling mailbox audit logging for mailbox owner actions such as message deletion.

More Resources

Related Help Topics

[Securing Mailbox Servers: Exch...](#)
[Create a Mailbox Audit Log Sea...](#)
[Mailbox Audit Logging: Exchang...](#)

[more...](#)

Related Blog Articles

[Visit the Exchange Team Blog](#)

Related Forum Discussions

[Ask a question](#)
[Visit the forums](#)

Question: 183

A corporate environment includes Exchange Server 2010 SP1. Client computers run Microsoft Outlook 2010. You have the following requirements:

- Minimize the amount of effort required to apply retention tags to email messages.
- Ensure that the solution functions across all folders in a mailbox.

You need to recommend a solution that meets the requirements. What should you recommend?

- A. Enable AutoTagging for mailboxes.
- B. Implement personal tags for each users mailbox.
- C. Use the Managed Folder Assistant to process mailbox folders.
- D. Modify the retention policy tag by reducing the age limit for retention.

Answer: C

Explanation:

Managed Folder Assistant

The Managed Folder Assistant is a process that runs on Mailbox servers and applies managed folder mailbox policies to mailboxes located on that server. The assistant retrieves the list of managed folders associated with a policy, provisions managed folders in mailboxes, and processes items in those folders. Items for which retention is enabled are stamped with the retention age. The retention action specified in applicable managed content settings is taken on items that have reached their retention age.

In Exchange 2010 SP1, the Managed Folder Assistant is a throttle-based assistant. Throttle-based assistants don't run on a schedule. Instead, they're configured to process all mailboxes on a Mailbox server within a certain period of time (known as a work cycle). Additionally, at a specified interval known as the work cycle checkpoint, the Managed Folder Assistant refreshes the list of mailboxes to be processed. During the refresh, the assistant adds newly created or

moved mailboxes to the queue. It also reprioritizes existing mailboxes that haven't been processed successfully for awhile due to failures and moves them higher in the queue so they can be processed during the same work cycle. In Exchange 2010, the Managed Folder Assistant is a schedule-based assistant that's scheduled to run from 01:00 through 09:00 (1:00 A.M. through 9:00 A.M.) every day. You can modify the assistant's schedule to make sure there's minimal user impact. You can also start and stop the assistant manually by using the Exchange Management Shell. To learn more about scheduling the assistant, see Configure the Managed Folder Assistant.

Note:

In Exchange 2010, the Managed Folder Assistant also applies retention policies for MRM. You can apply either a retention policy or a managed folder mailbox policy to a mailbox. If you modify the Managed Folder Assistant schedule, it impacts both MRM features.

Question: 184

A corporate environment includes Exchange Server 2010 SP1. The company plans to implement messaging records management (MRM). You need to recommend an implementation plan that meets the following requirements:

- Enable users to mark their own messages for retention.
- Delete messages that have no retention value.

What should you recommend?

- A. Apply a default policy tag to each user's mailbox and use personal tags.
- B. Apply a litigation hold to each user's mailbox and configure transport rules.
- C. Apply a litigation hold to each user's mailbox and configure Outlook rules.
- D. Apply a default policy tag only to each user's Inbox and use personal tags.

Answer: A

Question: 185

A corporate environment includes Exchange Server 2007 SP2 and an Active Directory Domain Services (AD DS) domain named contoso.com. The Client Access server, cas01.contoso.com, has an SSL certificate. The SSL certificate includes mail.contoso.com and autodiscover.contoso.com. Outlook Anywhere is disabled. Client computers run Microsoft Office Outlook 2007. After you transition the Exchange Server environment to Exchange Server 2010, Outlook displays a warning message indicating that the SSL certificate is not trusted for connections to cas01.contoso.com. You need to recommend an approach to resolving the problem. What should you recommend?

- A. Set the Client Access server AutoDiscoverServiceInternalUri property to autodiscover.contoso.com.
- B. Set the Client Access server array FQDN property to mail.contoso.com.
- C. Set the Autodiscover virtual directory ExternalUrl property to autodiscover.contoso.com.
- D. Set the Autodiscover virtual directory InternalUrl property to mail.contoso.com.

Answer: A

Question: 186

A corporate environment includes Exchange Server 2010 and client computers that run Microsoft Outlook 2010. The Exchange Server environment includes public folders. Specific users must be able to perform the following tasks:

- Create subfolders in the public folder hierarchy
- Delete only items they create in the subfolders

You need to recommend a solution that enables the users to perform the tasks. What should you recommend?

- A. Assign the users to the Editor role.
- B. Assign the users to the Owner role.
- C. Assign the users to the PublishingEditor role.
- D. Assign the users to the PublishingAuthor role.

Answer: D

Explanation:

Note:

The **FolderOwner** access right and the Owner role have different permissions as shown in the following table.

Access rights included with each predefined public folder role

Role	Create Items	Read Item s	CreateSubfolders	Folder Owner	Folder Contact	FolderVisible	EditOwnedItems	EditAllItems	DeleteOwnedItems	DeleteAllItems
None						X				
Owner	X	X	X	X	X	X	X	X	X	X
PublishingEdit or	X	X	X			X	X	X	X	X
Editor	X	X				X	X	X	X	X
PublishingAuth or	X	X	X			X	X		X	X
Author	X	X				X	X		X	
Non-EditingAuthor	X	X				X				
Reviewer		X				X				
Contributor	X					X				

Question: 187

A corporate environment includes Exchange Server 2010. Users access mailboxes by using Microsoft Office Outlook 2003 in Cached Exchange Mode. You need to recommend a solution for enabling users to access the global address list (GAL) when working offline. What should you recommend?

- A. Configure public folder distribution of the offline address book.
- B. Configure web-based distribution of the offline address book.
- C. Add the All Users address list to the offline address book.
- D. Modify the offline address book update schedule.

Answer: A

Question: 188

A corporate environment includes an on-premise deployment of Exchange Server 2010 SP1. The environment is configured as shown in the following table.

Location	Domain	Comments
North America	wingtiptoys.com	Includes Edge Transport server
Europe	tailspintoys.com	Includes Edge Transport server

The company plans to move the European employee email accounts to a cloud-based Exchange Server 2010 SP1 service provider. You have the following requirements:

- Route incoming messages to the appropriate Exchange Server environment.
- Ensure that all employees retain their current email addresses.
- Ensure that MX records do not change.

You need to recommend a solution for meeting the requirements. What should you recommend?

- A. Configure address rewriting. Configure send connectors for the on-premise Edge Transport server and the cloud-based servers.
- B. Configure an external relay domain for tailspintoys.com. Configure send connectors for the on-premise and cloud-based servers.
- C. Configure address rewriting. Configure send connectors for the on-premise Hub Transport server and the cloud-based servers.
- D. Configure an external relay domain for wingtiptoys.com. Configure send connectors for the on-premise and cloud-based servers.

Answer: B

Question: 189

A corporate environment includes Exchange Server 2003 SP2 and an Active Directory Domain Services (AD DS) forest with two domains. The forest functional level is set to Windows 2000. The domain functional level of Domain1 is set to Windows 2000 mixed. The domain functional level of Domain2 is set to Windows 2000 native. The AD DS infrastructure is shown in the following table.

Server	Domain	Operating system
DC1	Domain1	Windows Server 2008
DC2	Domain1	Windows Server 2003 SP1
DC3	Domain2	Windows 2000 Server SP4
DC4	Domain2	Windows 2000 Server SP2

The company plans to transition to Exchange Server 2010 SP1. The new infrastructure must support Windows Server 2003 SP1 domain controllers. You need to recommend a solution for preparing the existing AD DS infrastructure to support Exchange Server 2010 SP1. Which two actions should you recommend? (Each correct answer presents part of the solutions. Choose two.)

- A. Raise the functional level of Domain1 to Windows 2000 native. Raise the functional level of the forest to Windows

- Server 2003.
- B. Replace DC3 and DC4 with domain controllers running Windows Server 2008.
 - C. Raise the functional level of Domain1 to Windows 2008 R2. Raise the functional level of the forest to Windows Server 2008.
 - D. Replace DC2 and DC4 with domain controllers running Windows Server 2008 R2.

Answer: A, B

Question: 190

A company has an on-premise Exchange Server 2010 SP1 environment and an Active Directory Domain Services (AD DS) domain. Client computers run Microsoft Office Outlook 2003. The company plans to migrate mailboxes to a cloud-based Exchange Server 2010 SP1 service. You need to recommend a solution for ensuring that the global address list (GAL) in the on-premise and cloud-based environments are identical. What should you recommend?

- A. Synchronize the AD DS directory from the cloud-based environment.
- B. Install and configure the Exchange Online Connector for Office Outlook 2003 in the on-premise environment.
- C. Install and configure an SMTP connector in the cloud-based environment.
- D. Synchronize the AD DS directory from the on-premise environment.

Answer: D

Question: 191

A company named Contoso Ltd. has three offices. Each office is configured as an Active Directory site and contains multiple Exchange servers. Each office has a team of network support technicians. You are designing an Exchange organization for Contoso. All servers in the organization will have Exchange Server 2010 Service Pack 1 (SP1) installed. You need to implement a security solution to ensure that the team of network support technicians can manage the Exchange servers in its respective office only. Which of the following solutions is the best recommendation? (More than one answer choice may achieve the goal. Select the BEST answer.)

- A. Three custom scopes and three management role groups
- B. One management role and three Active Directory security groups
- C. One custom scope and one management role group
- D. Three custom scopes, three management roles, and three Active Directory security groups

Answer: A

Question: 192

An organization plans to utilize an on-premise Exchange Server 2010 SP1 environment for employees and a cloud-based Exchange Server 2010 SP1 service for contractors. You need to recommend an anti-spam solution that meets the following requirements:

- Minimize the amount of spam received by the on-premise servers.
 - Ensure that internal and external email delivery remains fully functional.
- What should you recommend?

- A. Point the MX records for the domain to the cloud-based servers. Configure the allowed IP addresses on the send connector of the on-premise servers.

- B. Point the MX records for the domain to the on-premise servers. Configure the allowed IP addresses on the send connector of the cloud-based servers.
- C. Point the MX records for the domain to the on-premise servers. Restrict the allowed IP addresses on the receive connector of the cloud-based servers.
- D. Point the MX records for the domain to the cloud-based servers. Restrict the allowed IP addresses on the receive connector of the on-premise servers.

Answer: D

Question: 193

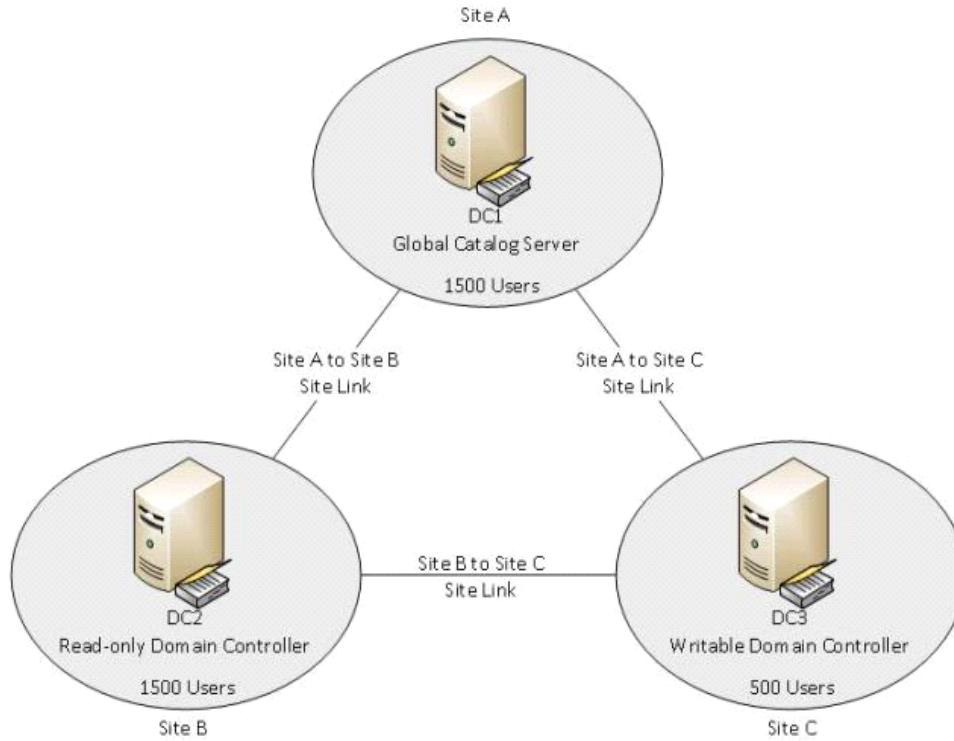
A corporate environment includes an on-premise deployment of Exchange Server 2010 SP1. The company needs to share calendar availability information with a partner. The partner is using a cloud-based Exchange Server 2010 SP1 service. You need to recommend a solution for sharing calendar availability information for all employees with the partner. What should you recommend?

- A. Create a federation trust and a TXT DNS record. Then create an organization relationship with the partner.
- B. Create a federation trust and a CNAME DNS record. Then create an organization relationship with the partner.
- C. Add the partner's domain as an accepted domain. Then create a TXT DNS record and a transport rule.
- D. Add the partner's domain as an accepted domain. Then create a CNAME DNS record and a group policy for all users.

Answer: A

Question: 194

A corporate environment will include Exchange Server 2010 in a single Active Directory Domain Services (AD DS) domain. The AD DS site topology is configured as shown in the exhibit. (Click the Exhibit button.)



You are designing the Exchange Server deployment plan. You have the following requirements:

- Deploy Exchange Server 2010 servers in two AD DS sites.
- Maximize the security of the Exchange Server deployment.

You need to recommend a solution that meets the requirements. Which two actions should you recommend? (Each correct answer presents part of the solution. Choose two.)

- A. Configure DC2 as a read-only global catalog server.
- B. Configure DC3 as a writable global catalog server.
- C. Deploy a Mailbox server, a Hub Transport server, and a Client Access server in Site A and in Site B.
- D. Deploy a Mailbox server, a Hub Transport server, and a Client Access server in Site A and in Site C.

Answer: B, D

Question: 195

A company named Contoso, Ltd. has offices in Montreal, Seattle, and Denver. An Active Directory site exists for each office. Only the Montreal site is connected to the Internet. You are designing an Exchange organization for Contoso. All servers in the organization will have Exchange Server 2010 Service Pack 1 (SP1) installed. Each office will contain two Exchange servers that each has the Mailbox, Hub Transport, and Client Access server roles installed. You need to recommend a deployment solution for the Client Access servers. Which of the following solutions is the best recommendation? (More than one answer choice may achieve the goal. Select the BEST answer.)

- A. One Client Access server array in each office
Round-robin DNS in each office
- B. A load balancing solution in each office
Round-robin DNS in the Montreal office
- C. One Client Access server array in each office
A load balancing solution in each office
- D. One Client Access server array that contains all of the Client Access servers
A load balancing solution in the Montreal office

Answer: C

Question: 196

A corporate environment includes Exchange Server 2010 with multiple Client Access servers. Employees connect to the Exchange Server environment from their Exchange ActiveSync-enabled mobile devices. You need to recommend a solution for preventing the mobile devices from using removable storage. What should you recommend?

- A. Configure the ActiveSync virtual directory on all Client Access servers.
- B. Create an Exchange ActiveSync mailbox policy and apply the policy to all mailboxes.
- C. Create a Group Policy Object (GPO) that enforces the use of BitLocker To Go and apply the GPO to all users.
- D. Create a Group Policy Object (GPO) that enforces the use of BitLocker To Go and apply the GPO to all member servers.

Answer: B

Question: 197

A corporate environment includes an on-premise implementation of Exchange Server 2010 SP1. The company intends

to use a cloud-based Exchange Server 2010 SP1 provider to provide email service for the Sales team. All other mailboxes will remain in the on-premise environment. You have the following requirements:

- Ensure that all users can access mailboxes by using corporate Active Directory Domain Services (AD DS) credentials.
- Ensure that all users can access a global address list (GAL) that includes all email addresses.

You need to recommend a coexistence solution that meets the requirements. Which two actions should you recommend? (Each correct answer presents part of the solution. Choose two.)

- A. Implement Active Directory Federation Services 2.0 (AD FS 2.0).
- B. Implement Microsoft Forefront Unified Access Gateway 2010 (UAG 2010).
- C. Synchronize AD DS from the on-premise environment to the cloud-based environment.
- D. Synchronize AD DS from the cloud-based environment to the on-premise environment.

Answer: A, C

Question: 198

A corporate environment includes Exchange Server 2010. Client computers run Windows 7 and Microsoft Outlook 2010. The client computers are joined to an Active Directory Domain Services (AD DS) domain. You need to recommend an email security solution that meets the following requirements:

- Protect email messages from being read by unauthorized users.
- Protect attachments, including text files, PDF files, and XPS files.
- Encrypt selected email messages when they are sent.

What should you recommend?

- A. message classification
- B. Mutual Transport Layer Security (MTLS)
- C. Secure/Multipurpose Internet Mail Extensions (S/MIME)
- D. Active Directory Rights Management Services (AD RMS)

Answer: C

Question: 199

You are designing an Exchange organization for a company named Contoso, Ltd. All servers in the organization will have Exchange Server 2010 Service Pack 1 (SP1) installed. Users connect to their mailboxes by using either Microsoft Office Outlook 2003, Microsoft Office Outlook 2007, or Microsoft Outlook 2010. You need to recommend a solution that protects confidential e-mail messages against eavesdropping and tampering. The e-mail messages must be protected while they are in transit and once they are stored. Which of the following solutions is the best recommendation? (More than one answer choice may achieve the goal. Select the BEST answer.)

- A. Deploy Active Directory Rights Management Services (AD RMS), and then create transport rules based on message classifications.
- B. Deploy certificates from a trusted root certification authority (CA) on all transport servers, and then configure Domain Security.
- C. Issue X.509 digital certificates to all users, and then instruct the users to protect their confidential e-mail messages by using S/MIME.
- D. Require RPC encryption for all mailbox databases, and then instruct all Outlook 2003 users to connect by using Outlook Web App (OWA) only.
- E. Deploy Active Directory Rights Management Services (AD RMS), and then instruct users to protect their confidential e-mail messages by using Outlook Protection Rules.

Answer: C

Question: 200

You have a Microsoft Forefront Threat Management Gateway (TMG) 2010 server that provides all Internet access for your company. You have two Mailbox servers configured in a database availability group (DAG), two Client Access servers, and two Hub Transport servers. You need to recommend changes to the environment to ensure that users can access Outlook Web App (OWA) from the Internet if any single server fails. What should you recommend?

- A. Configure a Client Access server array.
- B. Deploy a second TMG server and create a TMG array.
- C. Implement Windows Network Load Balancing for the Client Access servers.
- D. Deploy two Edge Transport servers that are configured to use EdgeSync synchronization.

Answer: B

Question: 201

A corporate environment includes Exchange Server 2010 SP1. The Exchange Server environment includes one Hub Transport server, one Client Access server, and one Mailbox server. You are designing an infrastructure for a secondary datacenter that will provide site resiliency for the primary datacenter that contains the existing Exchange Server environment. You have the following requirements:

- Ensure that employees can access email if the primary datacenter fails.
- Ensure that each Mailbox database is active in only one datacenter at a time.
- Minimize the number of Exchange servers required.

You need to recommend a solution that meets the requirements. Which two actions should you recommend? (Each correct answer presents part of the solution. Choose two.)

- A. In the secondary datacenter, deploy one server with the Hub Transport, Client Access, and Mailbox roles. Create a database availability group (DAG) that spans both datacenters.
- B. In the secondary datacenter, deploy one server with the Hub Transport and Client Access roles, and one server with the Mailbox role. Create a database availability group (DAG) that spans both datacenters.
- C. Enable datacenter activation coordination (DAC) mode.
- D. Disable datacenter activation coordination (DAC) mode.

Answer: A, C

Question: 202

A corporate environment includes Exchange Server 2010 and an Active Directory Domain Services (AD DS) domain. Client computers run Windows 7 and Microsoft Outlook 2010. You have the following requirements:

- Inspect all sent email messages.
- Automatically apply Information Rights Management (IRM) protection to all email messages marked as Company Confidential.

You need to recommend a solution that meets the requirements. What should you recommend?

- A. Deploy Active Directory Rights Management Services (AD RMS) and then create a transport rule.
- B. Deploy Active Directory Rights Management Services (AD RMS) and then create an Outlook protection rule.

- C. Deploy a digital certificate to each Exchange server and then implement Mutual Transport Layer Security (MTLS).
- D. Deploy a digital certificate to each Outlook user and then use Secure/Multipurpose Internet Mail Extensions (S/MIME).

Answer: A

Question: 203

A corporate environment includes Exchange Server 2010. The Exchange Server environment includes one Mailbox server, one Client Access server, one Hub Transport server, and one Edge Transport server. The Mailbox server has a single database with multiple mailboxes.

You have the following requirements:

- Record all email messages sent to and from only specific users.
- Store copies of only the recorded messages in one designated mailbox.

You need to recommend a solution that meets the requirements. What should you recommend?

- A. Create a journal rule.
- B. Configure journaling on the Mailbox server database.
- C. Create a transport rule on the Edge Transport server.
- D. Configure a litigation hold on the mailbox of each affected employee.

Answer: A

Question: 204

DRAG DROP

Your network contains two Active Directory forests. The forests contain domain controllers that run Windows Server 2008 R2. The forests are configured as shown in the following table.

Forest name	Number of domains	Number of users
Contoso.com	3	3,000
Fabrikam.com	1	5,000

An external trust exists from contoso.com to fabrikam.com.

You plan to deploy an Exchange Server 2010 Service Pack 1 (SP1) organization. The organization will contain Mailbox servers in fabrikam.com. You need to ensure that users in contoso.com can access the mailboxes in the Exchange organization. What should you do?

To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Answer Area

Answer:

Answer Area

Explanation:

Answer Area

Question: 205**DRAG DROP**

You plan to implement an Exchange Server 2010 Service Pack 1 (SP1) organization. You are planning the compliance infrastructure for the organization. You need to identify which permissions or management roles must be assigned to achieve your compliance requirements. The solution must minimize the number of rights assigned to users. What should you identify?

To answer, drag the appropriate permission or management role to the correct compliance requirement in the answer

area.

Permission/Management Role	Answer Area
Full Mailbox Access permission to an arbitration mailbox	Provide members of a security group named Legal with the ability to search for email messages in multiple mailboxes.
Full Mailbox Access permission to the Discovery Search Mailbox	Provide members of a security group named Legal with the ability to change message classification settings and retention policy tags.
the Discovery Management management role	Provide members of a security group named Legal Management with the ability to view the results of searches performed across multiple mailboxes.
the Organization Management management role	
the Records Management management role	
the Server Management management role	

Answer:

Permission/Management Role	Answer Area
Full Mailbox Access permission to an arbitration mailbox	Provide members of a security group named Legal with the ability to search for email messages in multiple mailboxes.
the Organization Management management role	Provide members of a security group named Legal with the ability to change message classification settings and retention policy tags.
the Server Management management role	Provide members of a security group named Legal Management with the ability to view the results of searches performed across multiple mailboxes.

Explanation:

Permission/Management Role	Answer Area
Full Mailbox Access permission to an arbitration mailbox	the Discovery Management management role Provide members of a security group named Legal with the ability to search for email messages in multiple mailboxes.
	the Records Management management role Provide members of a security group named Legal with the ability to change message classification settings and retention policy tags.
the Organization Management management role	
the Server Management management role	Full Mailbox Access permission to the Discovery Search Mailbox Provide members of a security group named Legal Management with the ability to view the results of searches performed across multiple mailboxes.

Question: 206

DRAG DROP

Your network contains an Active Directory forest. The forest contains two domains named contoso.com and east.contoso.com. The functional level of the contoso.com domain is Windows Server 2003 interim. The functional level of the east.contoso.com domain is Windows Server 2003. The contoso.com domain contains a domain controller named DC1. DC1 runs Windows Server 2003 Service Pack 2 (SP2). DC1 is configured as a global catalog server. The east.contoso.com domain contains a domain controller named DC2. DC2 runs Windows Server 2003 RTM. You need to recommend changes to the Active Directory forest to ensure that servers that run Exchange Server 2010 Service Pack 1 (SP1) can be deployed to both domains. You plan to raise the functional level of the forest to Windows Server 2003. Which other actions should you plan to perform?

To answer, drag the appropriate actions to the correct location or locations in the answer area.

Action	Answer Area
Enable the global catalog.	
Upgrade the operating system.	
Raise the functional level of the domain.	
Enable universal group membership caching.	 DC1 Action  DC2 Action

Answer:

Action	Answer Area
Enable the global catalog.	DC1  Raise the functional level of the domain.
Enable universal group membership caching.	DC2  Upgrade the operating system.

Explanation:

Action	Answer Area
Enable the global catalog.	DC1  Raise the functional level of the domain.
Upgrade the operating system.	DC2  Upgrade the operating system.
Raise the functional level of the domain.	
Enable universal group membership caching.	

Question: 207

Your network contains an Active Directory forest named contoso.com and two Active Directory sites named Site1 and Site2. You plan to deploy an Exchange Server 2010 Service Pack 1 (SP1) organization. An independent consultant recommends a design for the Exchange Server 2010 SP1 deployment as shown in the following table.

Server name	Server role	Database name	Site name
DC1	Domain controller Global catalog Certification authority (CA) DNS	Not applicable	Site1
DC2	Domain controller Global catalog	Not applicable	Site2
EX1	Mailbox Client Access Hub Transport	Mailbox Database 1	Site1
EX2	Mailbox	Mailbox Database 2	Site1
EX3	Mailbox Client Access Hub Transport	Mailbox Database 3	Site2
EX4	Mailbox	Mailbox Database 4	Site2

You are evaluating the implementation of the Hub Transport server role on EX4. You need to identify which Exchange server configuration will minimize the loss of email messages sent between users of the organization if a Hub Transport server fails. What should you identify?

- A. DNS round robin on DC1 and DC2
- B. Datacenter Activation Coordination (DAC) mode
- C. shadow redundancy

- D. delayed acknowledgments (ACKs)
- E. a Hosts file on EX1, EX2, EX3, and EX4
- F. a database availability group (DAG)
- G. a single copy cluster (SCC)
- H. an activation preference for a database
- I. EdgeSync synchronization
- J. a DNS server on DC2
- K. Edge Transport server cloned configuration
- L. local continuous replication (LCR) on EX1, EX2, EX3, and EX4

Answer: C

Explanation:

High availability strategies for Exchange have focused on the availability and recoverability of data stored in mailbox databases. When you implement a highly available solution for your Mailbox servers, the e-mail messages won't be lost, and they can easily be recovered after a failure, after they arrive in a mailbox.

However, these strategies didn't extend to messages while they're in transit. If a Hub Transport server fails while processing messages and can't be recovered, data loss could occur. As the volume of messages processed by Hub Transport servers increases, potential data loss becomes an increasing concern for administrators.

Microsoft Exchange Server 2007 introduced the transport dumpster feature for the Hub Transport server role.

An Exchange 2007 Hub Transport server maintains a queue of messages delivered recently to recipients whose mailboxes are on a clustered mailbox server. When a failover is experienced, the clustered mailbox server automatically requests every Hub Transport server in the Active Directory site to resubmit mail from the transport dumpster queue. This prevents mail from being lost during the time taken for the cluster to fail over.

While this does provide a basic level of transport redundancy, it's only available for message delivery in a cluster continuous replication (CCR) environment and doesn't address potential message loss when messages are in transit between Hub Transport and Edge Transport servers.

Exchange Server 2010 introduces the shadow redundancy feature to provide redundancy for messages for the entire time they're in transit. The solution involves a technique similar to the transport dumpster. With shadow redundancy, the deletion of a message from the transport databases is delayed until the transport server verifies that all of the next hops for that message have completed delivery. If any of the next hops fail before reporting back successful delivery, the message is resubmitted for delivery to that next hop.

Shadow redundancy provides the following benefits:

- It eliminates the reliance on the state of any specific Hub Transport or Edge Transport server. As long as redundant message paths exist in your routing topology, any transport server becomes disposable.
- If a transport server fails, you can remove it from production without emptying its queues or losing messages.
- If you want to upgrade a Hub Transport or Edge Transport server, you can bring that server offline at any time without the risk of losing messages.
- It eliminates the need for storage hardware redundancy for transport servers.
- It consumes less bandwidth than creating duplicate copies of messages on multiple servers. The only additional network traffic generated with shadow redundancy is the exchange of discard status between transport servers. Discard status is the information each transport server maintains. It indicates when a message is ready to be discarded from the transport database.
- It provides resilience and simplifies recovery from a transport server failure.

Question: 208

DRAG DROP

You have an Exchange Server 2010 Service Pack 1 (SP1) organization. You need to recommend tools that can be used to monitor the Exchange organization. Which tool or cmdlet should you use to perform each task?

To answer, drag the appropriate tool or cmdlet to the correct task in the answer area.

Tool/Cmdlet	Answer Area
Get-LogonStatistics	Tool/ Identify the largest mailboxes in the organization.
Get-Mailbox	Tool/ Identify the last time users accessed their Personal Archive.
Get-MailboxDatabase	Tool/ Identify the space available on the hard disks that contain the mailbox database.
Get-MailboxStatistics	
Performance Monitor	
Queue Viewer	
the Microsoft Exchange Troubleshooting Assistant	

Answer:

Tool/Cmdlet	Answer Area
	Get-MailboxStatistics Identify the largest mailboxes in the organization.
Get-Mailbox	Get-LogonStatistics Identify the last time users accessed their Personal Archive.
Get-MailboxDatabase	Queue Viewer Identify the space available on the hard disks that contain the mailbox database.
Performance Monitor	
the Microsoft Exchange Troubleshooting Assistant	

Explanation:

Tool/Cmdlet	Answer Area
Get-Mailbox	Get-MailboxStatistics
Get-MailboxDatabase	Get-LogonStatistics
Performance Monitor	Queue Viewer
the Microsoft Exchange Troubleshooting Assistant	Identify the largest mailboxes in the organization.
	Identify the last time users accessed their Personal Archive.
	Identify the space available on the hard disks that contain the mailbox database.

Question: 209

You have an Exchange Server 2010 Service Pack 1 (SP1) organization. The network contains two Active Directory sites named Site1 and Site2. Site1 contains an Edge Transport server named Server1. Each site has a direct connection to the Internet. Server1 receives all of the email sent to the Exchange organization from the Internet. You need to recommend a solution that meets the following requirements:

- Prevents an email message from being returned to the sender if Server1 fails.
 - Prevents an email message from being returned to the sender if the connection to the Internet in Site1 fails.
- What should you include in the recommendation? (Each correct answer presents a complete solution. Choose all that apply.)

- A. Deploy a new Edge Transport server named Server2 to Site2. Create a Network Load Balancing cluster that contains Server1 and Server2. Create a mail exchange (MX) record for the cluster.
- B. Deploy a new Edge Transport server named Server2 to Site2. Create a failover cluster that contains Server1 and Server2. Create a mail exchange (MX) record for the cluster.
- C. Create a mail exchange (MX) record that points to an Exchange Hosted Service. Configure the Exchange Hosted Service to accept email messages for your SMTP domain.
- D. Deploy a new Edge Transport server named Server2 to Site2. Create a mail exchange (MX) record for Server2.

Answer: C, D

Explanation:

This question had both c and d as the answers however I disagree with that. From what I can see there is no Exchange Host Service . The only way to meet the requirements of the question you will need to deploy a second edge server in site 2 and create the MX record. As both sites have a direct link to the Internet each Edge Server will load balance across the 2 servers

Question: 210

DRAG DROP

Your network contains an Active Directory domain named contoso.com. All domain controllers run Windows Server 2008 R2. The network contains an Exchange Server 2010 Service Pack 1 (SP1) organization. Corporate security policy

states that all user connections from the Internet to the Exchange organization must be encrypted. You plan to deploy the following client connection methods for the Exchange organization:

- POP3
- IMAP4
- Outlook Web App
- Outlook Anywhere

You need to identify which firewall ports must be opened to meet the security policy. The solution must use the default TCP ports of each connection method. Which TCP ports should you identify?

To answer, drag the appropriate TCP port to the correct connection method in the answer area.

TCP Port	Answer Area
110	TCP port POP3
135	TCP port IMAP4
443	TCP port Outlook Web App
993	TCP port Outlook Anywhere
995	
50636	

Answer:

TCP Port	Answer Area
110	993 POP3
	135 IMAP4
	443 Outlook Web App
50636	995 Outlook Anywhere

Explanation:

Secure ports to be open

Pop = 995

IMAP = 993

Outlook Web App = 443

If you already use Outlook Web App with SSL or Exchange ActiveSync with SSL, you don't have to open any additional ports from the Internet.

<http://technet.microsoft.com/en-us/library/bb123741.aspx>

Question: 211

DRAG DROP

You plan to implement Exchange Server 2010 Service Pack 1 (SP1) in your organization.

You need to plan the security model for the organization to meet the following requirements:

- A minimum number of permissions must be assigned.
- Members of a group named Support must be able to configure all the properties of mailbox-enabled users, distribution groups, and servers.
- Members of a security group named IT-Consultants must be able to generate a report that contains information about mailbox-enabled users, distribution groups, and server configurations.

Which management roles should you assign?

To answer, drag the appropriate management roles to the correct security group in the answer area.

Management Role		Answer Area
Help Desk		
Organization Management		
Recipient Management		
Server Management		
View-Only Organization Management		

IT-Consultants Support

Management Role
Management Role

Management Role
Management Role

Answer:

Management Role		Answer Area
Help Desk		

IT-Consultants Support

View-Only Organization Management
Organization Management

Server Management
Recipient Management

Explanation:

Management Role		Answer Area
Help Desk		

IT-Consultants Support

View-Only Organization Management
Organization Management

Server Management
Recipient Management

I am not sure if IT Consultants require - View-Only Organization Management along with Organization Management. The question states the least amount of permissions and to me - Organization Management does give the required permissions to perform almost any task. I do not see how View-Only Organization Management is required. I believe the screen shot above is not correct and IT Consultants only require Organization Management.

Organization Management

Administrators who are members of the Organization Management role group have administrative access to the entire Exchange 2010 organization and can perform almost any task against any Exchange 2010 object.

View-Only Organization Management

Administrators who are members of the View Only Organization Management role group can view the properties of any object in the Exchange organization.

Recipient Management

Administrators who are members of the Recipient Management role group have administrative access to create or modify Exchange 2010 recipients within the Exchange 2010 organization.

Server Management

Administrators who are members of the Server Management role group have administrative access to Exchange 2010 server configuration. They don't have access to administer Exchange 2010 recipient configuration.

Help Desk

Users who are members of the Help Desk role group can perform limited recipient management of Exchange 2010 recipients.

Question: 212

You are a messaging administrator for a company named Contoso, Ltd. Contoso has a UNIX-based email system for the contoso.com SMTP domain. Contoso has a perimeter network and an internal network.

Corporate security policy states that only TCP port 25 is allowed from the perimeter network to the internal network.

You plan to change the UNIX-based email infrastructure to Exchange Server 2010 Service Pack 1 (SP1). The UNIX-based infrastructure will not coexist with the Exchange Server 2010 SP1 organization.

Contoso has a partner company named Fabrikam, Inc. All recipients at Fabrikam are hosted on an Exchange Server 2003 organization. Fabrikam uses the fabrikam.com SMTP domain.

You need to plan the configuration of the Exchange Server 2010 SP1 accepted domains to meet the following requirements:

- Ensure that all email messages sent to Contoso and Fabrikam can be received by the Contoso servers.
- Ensure that the Contoso servers can then relay the email messages to the Fabrikam servers.
- Prevent email messages sent to Fabrikam recipients from being relayed to the internal network.

What should you include in the plan? (Each correct answer presents part of the solution. Choose all that apply.)

- A. an authoritative accepted domain for contoso.com
- B. an internal relay accepted domain for fabrikam.com
- C. an authoritative accepted domain for fabrikam.com
- D. an external relay accepted domain for contoso.com
- E. an external relay accepted domain for fabrikam.com

Answer: A, E

Question: 213

Your network contains an Active Directory domain named contoso.com. All domain controllers run Windows Server 2008 R2. The network contains two Active Directory sites named Los Angeles and San Francisco. All traffic to and from the Internet is routed through Los Angeles. You have an Exchange Server 2010 Service Pack 1 (SP1) organization that contains three servers. The servers are configured as shown in the following table.

Server name	Server role	Server site
Server1	Client Access	Los Angeles
	Mailbox	
	Hub Transport	
Server2	Client Access	San Francisco
	Mailbox	
	Hub Transport	
Server3	Mailbox	San Francisco

Server1 has Windows Integrated Authentication enabled for the default OWA virtual directory. You need to configure the Exchange environment to meet the following requirements. Ensure that users can access their mailbox from the Internet by using the light version of Outlook Web App. Prevent users from being prompted for a username and a password when they connect to Outlook Web App from a domain-joined client computer on the internal network. What should you do? (Choose all that apply.)

- A. From the Exchange Management Console (EMC), enable Windows Integrated Authentication for OWA2.

- B. From the Exchange Management Console (EMC) on Server1, enable forms-based authentication for the default OWA virtual directory on Server1.
- C. Create a new OWA virtual directory named OWA2 on Server1.
- D. From Internet Information Services (IIS) Manager on Server2, enable forms-based authentication for the default OWA virtual directory.
- E. From Internet Information Services (IIS) Manager on Server1, enable forms-based authentication for the default OWA virtual directory.
- F. From the Exchange Management Console (EMC), enable Windows Integrated Authentication for the default OWA virtual directory on Server2.

Answer: F

Explanation:

This question had A, B, C and F as the answer however I do not see how that is correct.

As I understand the question Windows Integrated Authentication has already been enabled on Server 1 default OWA directory. I do not see a need to create a second OWA directory named OWA2 as it is Los Angeles that excepts all connections so it should use either Client Access Proxy, or a redirection to the Client Access Server in San Francisco.

I also don't see how forms - based authentication will achieve anything. The Light Version of Outlook Web App will be supported regardless as it is based not on the authentication methods but what browser is being used. If you do not use a supported browser then only the light version will be available.

Forms Based Authentication

Forms-based authentication enables a sign-in page for Exchange Server 2010 Outlook Web App that uses a cookie to store a user's encrypted sign-in credentials in the Internet browser. Tracking the use of this cookie enables the Exchange server to monitor the activity of Outlook Web App sessions on public and private computers. If a session is inactive for too long, the server blocks access until the user re-authenticates. The first time that the user name and password are sent to the Client Access server to authenticate an Outlook Web App session, an encrypted cookie is created that's used to track user activity. When the user closes the Internet browser or clicks Sign Out to sign out of their Outlook Web App session, the cookie is cleared. The user name and password are sent to the Client Access server only for the initial user sign-in. After the initial sign-in is complete, only the cookie is used for authentication between the client computer and the Client Access server.

Setting the Value for Cookie Time-Out on Public Computers

By default, when a user selects the This is a public or shared computer option on the Outlook Web App sign-in page, the cookie on the computer expires automatically and the user is signed out when they haven't used Outlook Web App for 15 minutes.

Automatic time-out is valuable because it helps protect users' accounts from unauthorized access. To match the security requirements of your organization, you can configure the inactivity time-out values on the Exchange Client Access server.

Although automatic time-out greatly reduces the risk of unauthorized access, it doesn't eliminate the possibility that an unauthorized user might access an Outlook Web App account if a session is left running on a public computer. Therefore, make sure to warn users to take precautions to avoid risks. For example, tell them to sign out from Outlook Web App and close the Web browser when they've finished using Outlook Web App. For more information about how to configure cookie time-out values for public computers, see Set the Forms-Based Authentication Public Computer Cookie Time-Out Value.

Integrated Windows Authentication

You can configure Integrated Windows authentication for Outlook Web App in Microsoft Exchange Server

2010. Integrated Windows authentication enables the server to authenticate users who are signed in to the network without prompting them for their user name and password and without transmitting information that isn't encrypted over the network.

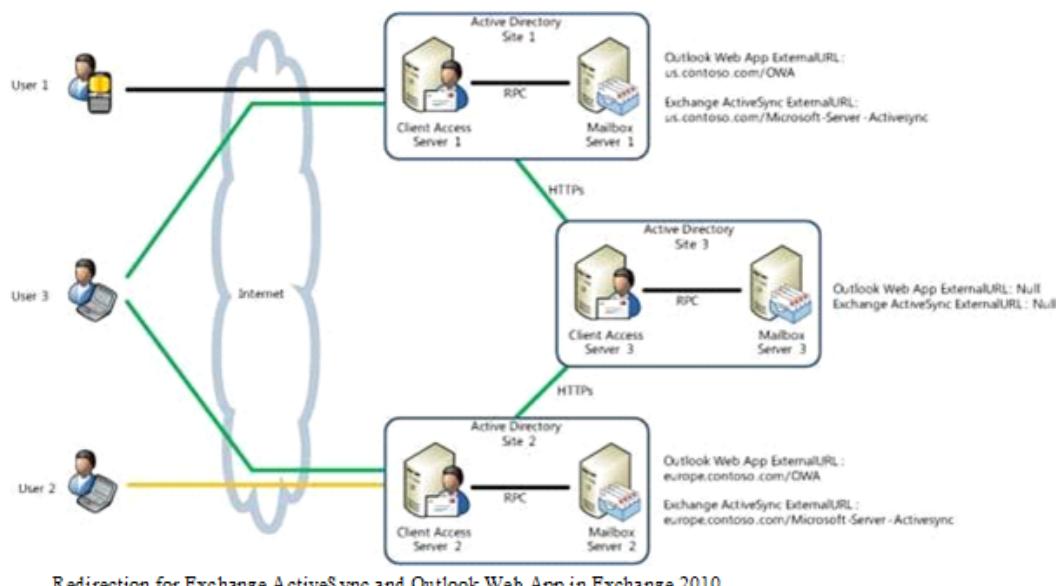
Understanding Proxying and Redirection

In a Microsoft Exchange Server 2010 organization, a Client Access server can act as a proxy for other Client Access

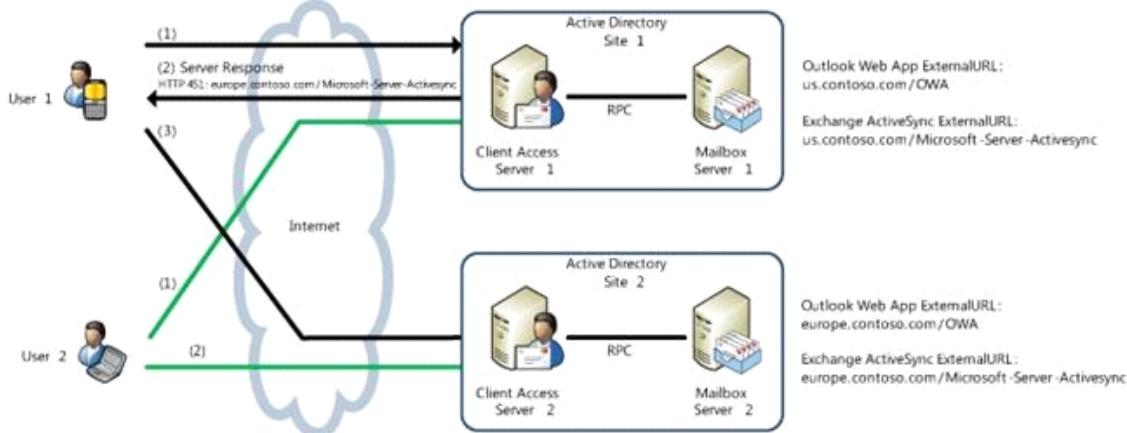
servers within the organization. This is useful when multiple Client Access servers are present in different Active Directory sites in an organization and at least one of those sites isn't exposed to the Internet. A Client Access server can also perform redirection for Microsoft Office Outlook Web App URLs and for Exchange ActiveSync devices. Redirection is useful when a user connects to a Client Access server that isn't in their local Active Directory site or if a mailbox has moved between Active Directory sites. It's also useful if the user should be using a better URL, for example, one that's closer to the Active Directory site their mailbox resides in.

Although the Client Access server's response can vary by protocol, when a Client Access server receives a request for a user whose mailbox is in an Active Directory site other than the one the Client Access server belongs to, it looks for the presence of an ExternalURL property on the relevant virtual directory on a Client Access server that's in the same Active Directory site as the user's mailbox. If the ExternalURL property exists, and the client type supports redirection (for example, Outlook Web App or Exchange ActiveSync), the Client Access server will issue a redirect to that client. If there's no ExternalURL property present, or if the client type doesn't support redirection (for example, POP3 or IMAP4), the Client Access server will try to proxy the connection to the target Active Directory site.

Client Access Proxy



Redirection for Exchange ActiveSync and Outlook Web App in Exchange 2010



I think the correct answer is just F as the Client Access Server in Los Angeles should perform either a Client Access Proxy or a redirection to the Client Access Server in San Francisco.

Question: 214

DRAG DROP

Your network contains a single Active Directory domain named contoso.com. You plan to deploy a new Exchange

Server 2010 Service Pack 1 (SP1) organization. You identify the administrative model for the Exchange organization as shown in the following table.

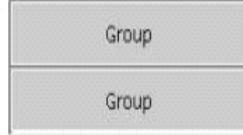
Group name	Group tasks
Group1	<ul style="list-style-type: none"> • Restore mailboxes • Stop and restart servers • Stop and restart services • Create mailbox databases • Install operating system updates • Manage Exchange server certificates
Group2	<ul style="list-style-type: none"> • Create mailbox-enabled users • Create mail-enabled distribution groups • Delete mail-enabled distribution groups

You need to identify which groups must be assigned to Group1 and Group2 to support the planned administrative model. The solution must minimize the number of rights assigned to each group. Which security groups and role groups should you assign to Group1 and Group2?

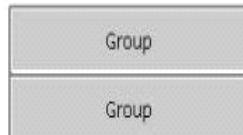
To answer, drag the appropriate security groups or role groups to the correct group in the answer area.

Group	Answer Area
Account Operators group in the domain	
Administrators group on each Exchange server	
Domain Admins group in the domain	
Help Desk role group	
Organization Management role group	
Recipient Management role group	

Group1



Group2



Answer:

Group	Answer Area
Domain Admins group in the domain	Group1 Account Operators group in the domain Recipient Management role group
Help Desk role group	Group2 Organization Management role group Administrators group on each Exchange server

Explanation:

Group	Answer Area
Domain Admins group in the domain	Group1 Account Operators group in the domain Recipient Management role group
Help Desk role group	Group2 Organization Management role group Administrators group on each Exchange server

Group 1 needs to be able to do the following:

- Restore mailboxes
- Stop and Restart both Servers and Services
- Create mailbox database
- Install Operating System Updates
- Manage Certificates

I don't agree with the need for this group to be a member of the Account Operators group. This is a domain account that allows local logon to domain controllers and they can create user account accounts. Group 1 as I read the question needs to logon to exchange servers and manage the local exchange server. Therefore I think they just need to be members of the Administrative Group on each Exchange Server.

Group 2 needs to be able to do the following:

- Create mail - enabled users
- Create distribution lists
- Delete distribution lists

In order for group 2 to complete their tasks they will need to have recipient management role and the Organization Role

Account Operators is a local group that grants limited account creation privileges to a user. Members of this group can create and modify most types of accounts, including those of users, local groups, and global groups. They can also log on locally to domain controllers. However, Account Operators can't manage the Administrator user account, the user

accounts of administrators, or the group accounts Administrators, Server Operators, Account Operators, Backup Operators, and Print Operators. Account Operators also can't modify user rights. The Recipient Management management role group is one of several built-in role groups that make up the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Role groups are assigned one or more management roles that contain the permissions required to perform a given set of tasks. The members of a role group are granted access to the management roles assigned to the role group. For more information about role groups, see Understanding Management Role Groups.

Administrators who are members of the Recipient Management role group have administrative access to create or modify Microsoft Exchange Server 2010 recipients within the Exchange 2010 organization.

Help Desk - The Help Desk management role group gives members permissions that are typically required by members of a help desk, such as modifying users' details such as their address and phone number.

Organization Management

The Organization Management role group is synonymous with the

Exchange Full Administrator role in Exchange 2003 and the Exchange Organization Administrators role in Exchange 2007. Essentially, membership of this management role group gives the user the ability to perform pretty much any task in Exchange 2010, with the main missing task being the ability to perform mailbox searches; that itself is achieved via the Discovery Management role group.

Domain Admins - This group is automatically added to the corresponding Administrators group in every domain in the forest. It has complete control over all domain controllers and all directory content stored in the domain and it can modify the membership of all administrative accounts in the domain.

The permissions granularity issue was improved in Exchange 2007. The Exchange Full Administrator role found in Exchange 2000 and Exchange 2003 became known as the Exchange Organization Administrators role in Exchange 2007 and still gave administrators full access to all Exchange objects in the entire organization.

The Exchange View-Only Administrators role also remained, giving administrators read-only access to the entire Exchange organization.

There were effectively three new additions to the Exchange 2007 roles:

Exchange Recipient Administrators - Allowed administrators to modify Exchange settings on users, groups, contacts and public folders

Exchange Public Folder Administrators - Was introduced in Exchange 2007 Service Pack 1 and as its name suggests allowed administrators to manage public folders

Exchange Server Administrators - Allowed administrators to fully manage a particular Exchange 2007 server as long as they were also a member of the local Administrators group on that server

Although the permissions model in Exchange 2007 was a vast improvement over those models found in earlier versions of Exchange, it still wasn't able to satisfy a lot of the administrative scenarios found in various organizations. Essentially, the roles in Exchange 2007 still offered too much administrative power to administrators in a decentralized Exchange organization and it was therefore difficult to limit the permissions available to certain administrators. Although it was possible to implement a split permissions model in Exchange 2007 by modifying Access Control Lists (ACLs), this was a complex procedure that could sometimes result in errors and issues that were difficult to troubleshoot.

The design of Exchange 2010 has needed to take into account the more demanding and granular permissions requirements of organizations. Exchange 2010 now supports a model where specialist users can be granted specific Exchange permissions required to perform their duties. For example, there may be the scenario where a compliance officer within a company needs to conduct a search across all employees' mailboxes for legal reasons, or perhaps a member of the Human Resources department needs to update user information in Active Directory that is seen on the properties of users' mailboxes. In these example cases, the relevant specialist user should only be given the rights to perform the required task and should not be assigned, for example, additional rights that could allow them to affect the overall configuration of the Exchange environment.

Management Role Groups - In Exchange 2010, Microsoft has made the task of assigning a series of common permissions to administrative and specialist users very easy by providing 11 default management role groups. By placing a user or group into a management role group, the management roles associated with that management role group are assigned accordingly thereby giving the user or group the relevant permissions.

The term role holder is used by Microsoft to denote the administrative or specialist user that is added to the management role group. These 11 default management role groups are created during Exchange 2010 setup. Specifically, these management role groups are created when Exchange 2010 setup runs the Active Directory preparation steps that can be performed individually by running the Exchange 2010 setup.com program with the /PrepareAD switch. The management role groups can be seen in the Microsoft Exchange Security Groups Organizational Unit (OU) that is created in the root domain during the Exchange setup process. You can see this OU and the groups within it in Figure 1. Note that of the 16 groups shown in Figure 1, only 11 are management role groups; these are highlighted.

Microsoft Exchange Security Groups 16 objects		
Name	Type	Description
Delegated Setup	Security Group ...	Members of this management role...
Discovery Management	Security Group ...	Members of this management role...
Exchange All Hosted Organizations	Security Group ...	This group contains all the Exchange...
Exchange Servers	Security Group ...	This group contains all the Exchange...
Exchange Trusted Subsystem	Security Group ...	This group contains Exchange ser...
Exchange Windows Permissions	Security Group ...	This group contains Exchange ser...
ExchangeLegacyInterop	Security Group ...	This group is for interoperability ...
Help Desk	Security Group ...	Members of this management role...
Hygiene Management	Security Group ...	Members of this management role...
Organization Management	Security Group ...	Members of this management role...
Public Folder Management	Security Group ...	Members of this management role...
Recipient Management	Security Group ...	Members of this management role...
Records Management	Security Group ...	Members of this management role...
Server Management	Security Group ...	Members of this management role...
UM Management	Security Group ...	Members of this management role...
View-Only Organization Management	Security Group ...	Members of this management role...

A member of LOCAL\Administrators is a far cry from a BUILTIN\Administrators, and here are the two primary reasons why:

One - BUILTIN\Administrators is not stored locally to a single DC - its membership is in the Active Directory, in the CN=Builtin,DC=domain,DC=com container. The contents of this container are replicated to all domain controllers. Therefore, adding a user to a member of this group on one DC makes them a member of the group on all DCs. (A member server has a local accounts database called a SAM that is not visible to the domain.)

Two - Since BUILTIN\Administrators gives local Administrator permissions to its members - they can do anything on any DC in the domain. Anything. Making themselves a Domain Administrator is a trivial exercise.

A final note of caution: it is now widely recognized that forests are the security boundaries in Active Directory, not domains (regardless of what the original Windows 2000 Server A/D documentation said). Domains are simply administrative boundaries. As a corollary to item two above, once a person is a domain administrator, it is fairly easy to become an enterprise administrator.

Question: 215

DRAG DROP

You have an Exchange Server 2010 Service Pack 1 (SP1) organization named contoso.com.

Remote users connect to the organization by using Microsoft Outlook 2010. Your network includes four servers. The servers are configured as shown in the following table.

Server name	Server role	IP address
Server1.contoso.com	Mailbox, Client Access Hub Transport	192.168.100.21
Server2.contoso.com	Mailbox Client Access Hub Transport	192.168.100.22
Server3.contoso.com	Edge Transport	131.107.10.33
Server4.contoso.com	Edge Transport	131.107.10.34

You create a Hosts file on Server3 and Server4 that contains the IP addresses and server names of Server1 and Server2. You need to recommend which DNS records must be created to meet the following requirements:

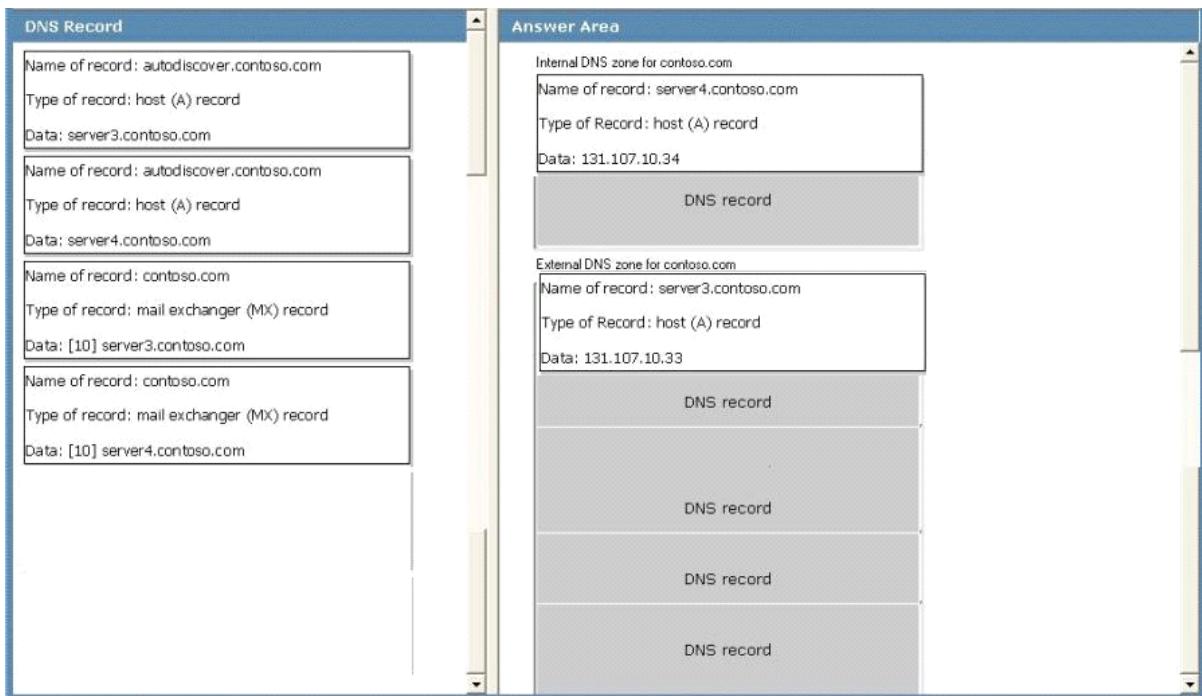
- Support Edge Subscriptions.
- Provide load balancing for email traffic received from the Internet.
- Ensure that email can be received from the Internet if a single Edge Transport server fails.

What should you do?

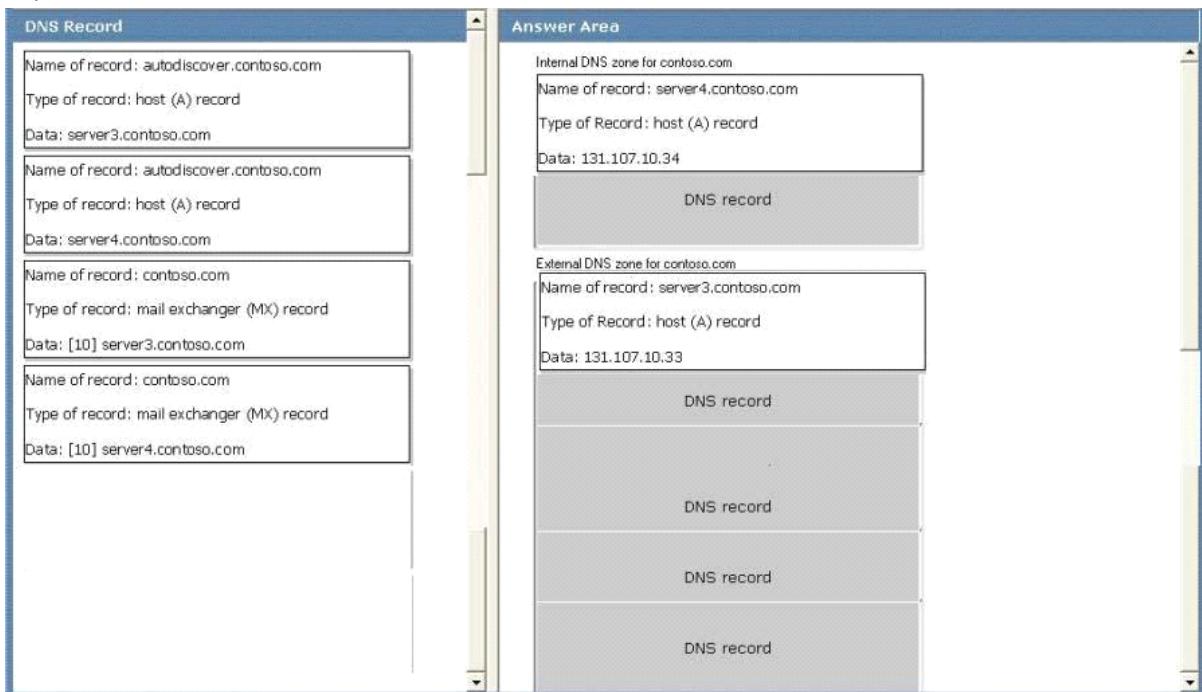
To answer, drag the appropriate DNS records to the correct DNS zone in the answer area.

DNS Record	Answer Area
Name of record: autodiscover.contoso.com Type of record: host (A) record Data: server3.contoso.com	Internal DNS zone for contoso.com DNS record DNS record
Name of record: autodiscover.contoso.com Type of record: host (A) record Data: server4.contoso.com	External DNS zone for contoso.com DNS record DNS record
Name of record: contoso.com Type of record: mail exchanger (MX) record Data: [10] server3.contoso.com	DNS record
Name of record: contoso.com Type of record: mail exchanger (MX) record Data: [10] server4.contoso.com	DNS record
Name of record: server3.contoso.com Type of Record: host (A) record Data: 131.107.10.33	DNS record
Name of record: server4.contoso.com Type of Record: host (A) record Data: 131.107.10.34	DNS record

Answer:



Explanation:



This solution makes no sense and certainly does not meet the requirements of the Question.

- Support Edge Subscriptions.
- Provide load balancing for email traffic received from the Internet.
- Ensure that email can be received from the Internet if a single Edge Transport server fails.

To support load balancing of the edge servers you will need to create external MX records for both Edge Servers - this will also insure that email can be received if a single edge server fails. To support Edge Subscriptions you will need to create A records on the internal network.

Question: 216

DRAG DROP

You have an Exchange Server 2007 organization.

You deploy servers that run Exchange Server 2010 Service Pack 1 (SP1) to the organization. Your network contains two Active Directory sites named Site1 and Site2. The organization contains five servers. The servers are configured as shown in the following table.

Server name	Server role	Server location	Server configuration
Server1	Client Access Hub Transport	Site1	Exchange Server 2007
Server2	Mailbox	Site1	Exchange Server 2007
Server3	Edge Transport	Perimeter	Exchange Server 2007
Server4	Client Access Hub Transport	Site2	Exchange Server 2010 SP1
Server5	Mailbox	Site2	Exchange Server 2010 SP1

You plan to move all mailboxes to Servers and to decommission Server1 and Server2. You need to recommend the process to decommission Server1 and Server2. The solution must prevent interruptions to the mail flow. What should you do?

To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Answer Area

Modify the mail exchange (MX) records.

Uninstall Exchange Server 2007 from Server1.

Uninstall Exchange Server 2007 from Server2.

Create an Edge Subscription from Server4 to Server3.

Upgrade Active Directory Application Mode (ADAM) to Active Directory Lightweight Directory Services (AD LDS) on Server3.

Answer:

Answer Area

Uninstall Exchange Server 2007 from Server2.

Uninstall Exchange Server 2007 from Server1.

Create an Edge Subscription from Server4 to Server3.

Explanation:

The screenshot shows a configuration interface with a left pane containing a list of actions and a right pane labeled "Answer Area".

Left Pane (List of Actions):

- Modify the mail exchange (MX) records.
- (Empty box)
- (Empty box)
- (Empty box)
- Upgrade Active Directory Application Mode (ADAM) to Active Directory Lightweight Directory Services (AD LDS) on Server3.

Right Pane (Answer Area):

- Uninstall Exchange Server 2007 from Server2.
- Uninstall Exchange Server 2007 from Server1.
- Create an Edge Subscription from Server4 to Server3.

There are navigation arrows between the two panes.

You will need to uninstall Exchange 2007 and create the Edge subscription.

In a typical deployment scenario, the computer that has the Edge Transport server role installed doesn't have access to Active Directory. All the configuration and recipient information that the Edge Transport server has to process messages is stored in AD LDS. Creating an Edge Subscription establishes secure, automatic replication of information from Active Directory to AD LDS. The Edge Subscription process provisions the credentials that are used to establish a secure LDAP connection between Hub Transport servers and a subscribed Edge Transport server. The Microsoft Exchange EdgeSync service that runs on Hub Transport servers then performs periodic one-way synchronization to transfer data to AD LDS and keep that data up to date. This process reduces the administration that you must perform in the perimeter network by letting you perform required configuration on the Hub Transport server role and then write that information to the Edge Transport server.

You subscribe an Edge Transport server to the Active Directory site that contains the Hub Transport servers that will directly exchange messages with your Edge Transport servers. The Edge Subscription process creates an Active Directory site membership affiliation for the Edge Transport server. The site affiliation enables Hub Transport servers in the Exchange organization to relay messages to the Edge Transport server for delivery to the Internet without having to configure explicit Send connectors.

Question: 217

DRAG DROP

You have an Exchange Server 2010 Service Pack 1 (SP1) organization that contains four servers. The servers are configured as shown in the following table.

Server name	Server role	Server site	Server DAG
Server1	Mailbox	Site1	DAG1
Server2	Mailbox	Site1	DAG1
Server3	Mailbox	Site2	DAG1
Server4	Mailbox	Site2	DAG1
Server5	Client Access Hub Transport	Site1	Not applicable
Server6	Client Access Hub Transport	Site1	Not applicable
Server7	Client Access Hub Transport	Site2	Not applicable
Server8	Client Access Hub Transport	Site2	Not applicable

Datacenter Activation Coordination (DAC) node is enabled for DAG1, The file share witness is located on Servers and the alternate file share witness is located on Server7. Domain controllers are available in both sites. You need to recommend a solution to activate the databases in Site2 if Site1 becomes unavailable for an extended period of time. What should you recommend running before you activate the mailbox databases?

To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct

order.

Answer:

Question: 218

DRAG DROP

You have an Exchange Server 2010 Service Pack 1 (SP1) organization named contoso.com.

You are planning the anti-spam infrastructure for the organization. You need to identify which Exchange Server 2010 SP1 anti-spam technologies achieve your anti-spam requirements. Which technologies should you identify? To answer, drag the appropriate anti-spam technology to the correct anti-spam requirement in the answer area.

Anti-spam Technology	Answer Area
content filtering	Anti-spam technology Minimize the possibility of receiving email messages from impersonated servers.
recipient filtering	Anti-spam technology Prevent the organization from accepting email messages that contain administrator-defined keywords.
sender filtering	Anti-spam technology Prevent the organization from receiving email from a domain named fabrikam.com.
Sender ID	Anti-spam technology Prevent the organization from receiving email sent to addresses that are not on the global address list (GAL).
sender reputation	

Answer:

Anti-spam Technology	Answer Area
	content filtering Minimize the possibility of receiving email messages from impersonated servers.
	Sender ID Prevent the organization from accepting email messages that contain administrator-defined keywords.
	sender filtering Prevent the organization from receiving email from a domain named fabrikam.com.
sender reputation	recipient filtering Prevent the organization from receiving email sent to addresses that are not on the global address list (GAL).

Explanation:

Content Filtering - Content filtering provides another tool to help manage the flow of messages entering and exiting your enterprise mail stream. Content filtering enables you to filter messages using a variety of filtering tools. These include:

Sender-domains filtering (for Realtime and Manual scan jobs), **Subject line filtering** (for Realtime and Manual scan jobs). **Filter set templates** (simplify the creation and management of file and content filters on all scan jobs) **Sender ID** - The Sender ID Framework is an e-mail authentication technology protocol that helps address the problem of spoofing and phishing by verifying the domain name from which e-mail messages are sent. Sender ID validates the origin of e-mail messages by verifying the IP address of the sender against the alleged owner of the sending domain. Now adopted by more than 10 million domains worldwide, Sender ID is providing brand owners, senders, and receiving networks with significant business and technical value **Sender Filtering** - The Sender Filter agent is an anti-spam filter that's enabled on computers that have the Microsoft Exchange Server 2010 Edge Transport server role installed. The Sender Filter agent relies on the MAIL FROM: SMTP header to determine what action, if any, to take on an inbound e-mail message. When you configure anti-spam filters on an Edge Transport server, the filters act on messages cumulatively to reduce the number of unsolicited messages that enter the enterprise. For more information about how to plan and deploy the anti-spam features, see Understanding Anti-Spam and Antivirus Functionality. The Sender Filter agent acts on messages from specific senders outside the organization. Administrators of Edge Transport servers maintain a list of senders who are blocked from sending messages to the organization. As an administrator, you can block single senders (kim@contoso.com), whole domains (*.contoso.com), or domains and all subdomains (*.contoso.com). You can also configure what action the Sender Filter agent should take when a message that has a blocked sender is found.

You can configure the following actions:

The Sender Filter agent rejects the SMTP request with a "554 5.1.0 Sender Denied" SMTP session error and closes the connection.

The Sender Filter agent accepts the message and updates the message to indicate that the message came from a blocked sender. Because the message came from a blocked sender and it's marked as such, the Content Filter agent will use this information when it calculates the spam confidence level (SCL). Recipient Filtering - The Recipient Filter agent blocks messages according to the characteristics of the intended recipient in the organization.

The Recipient Filter agent can help you prevent the acceptance of messages in the following scenarios:

Nonexistent recipients

You can prevent delivery to recipients that are not in the organization's address book. For example, you may want to stop delivery to frequently misused account names, such as administrator@contoso.com or support@contoso.com.

Restricted distribution lists

You can prevent delivery of Internet mail to distribution lists that should be used only by internal users.

Mailboxes that should never receive messages from the Internet You can prevent delivery of Internet mail to a specific mailbox or alias that is typically used inside the organization, such as Helpdesk.

The Recipient Filter agent acts on recipients that are stored in one or both of the following data sources:

Recipient Block list An administrator-defined list of recipients for which inbound messages from the Internet should never be accepted.

Recipient Lookup Verification that the recipient is in the organization. Recipient Lookup requires access to Active Directory directory service information that is provided by EdgeSync to Active Directory Application Mode (ADAM).

Sender Reputation - Sender reputation weighs each of these statistics and calculates an SRL for each sender. The SRL is a number from 0 through 9 that predicts the probability that a specific sender is a spammer or otherwise malicious user. A value of 0 indicates that the sender isn't likely to be a spammer; a value of 9 indicates that the sender is likely to be a spammer.

You can configure a block threshold from 0 through 9 at which sender reputation issues a request to the Sender Filter agent, and, therefore, blocks the sender from sending a message into the organization. When a sender is blocked, the sender is added to the Blocked Senders list for a configurable period. How blocked messages are handled depends on the configuration of the Sender Filter agent.

The following actions are the options for handling blocked messages:

- Reject
- Delete and archive
- Accept and mark as a blocked sender
- If a sender is included in the IP Block list or Microsoft IP Reputation Service, sender reputation issues an immediate request to the Sender Filter agent to block the sender. To take advantage of this functionality, you must enable and configure the Microsoft Exchange Anti-spam Update Service.

By default, the Edge Transport server sets a rating of 0 for senders that haven't been analyzed. After a sender has sent 20 or more messages, sender reputation calculates an SRL that's based on the statistics listed earlier in this topic.

Question: 219

You have an Exchange Server 2010 Service Pack 1 (SP1) organization. You plan to implement a redundancy solution for Exchange dependencies. You need to identify which services must be available for the Exchange organization to function correctly for all users. Which service or services should you identify? (Choose all that apply.)

- A. domain naming master
- B. DNS server
- C. primary domain controller (PDC) emulator
- D. certification authority (CA)
- E. global catalog
- F. WINS server
- G. infrastructure master

Answer: B, E

Question: 220

Your network contains an Active Directory domain named contoso.com. All domain controllers run Windows Server 2003 Service Pack 2 (SP2). You have an Exchange Server 2003 organization. The organization contains servers that run Exchange Server 2003 Service Pack 1 (SP1) and servers that run Exchange 2000 Server Service Pack 4 (SP4). The organization contains three routing groups. You need to prepare the Exchange organization for the installation of the first Exchange Server 2010 SP1 server. The solution must not affect message flow between the Exchange servers. What should you do? (Choose all that apply.)

- A. Move all of the Exchange Server 2003 servers to a single administrative group.
- B. Suppress link state updates.
- C. Perform an in-place upgrade of the Exchange Server 2003 servers to Exchange Server 2007 SP2.
- D. Remove the Exchange 2000 Server servers.
- E. Install Exchange Server 2003 SP2.

Answer: B, D, E

Question: 221

Your network contains an Active Directory forest. The forest contains two domains named fabrikam.com and eu.fabrikam.com. The functional level of the fabrikam.com domain is Windows Server 2003 interim. The functional level of the eu.fabrikam.com domain is Windows Server 2003. The fabrikam.com domain contains a domain controller named DC1. DC1 runs Windows Server 2003 Service Pack 2 (SP2). DC1 is configured as a global catalog server. The eu.fabrikam.com domain contains a domain controller named DC2. DC2 runs Windows Server 2003 RTM. You need to recommend changes to the Active Directory forest to ensure that servers that run Exchange Server 2010 Service Pack 1 (SP1) can be deployed to both domains. What should you do?

- A. Upgrade the operating system on DC2. Raise the functional level of the fabrikam.com domain. Raise the functional level of the forest.
- B. Upgrade the operating system on DC1 and DC2. Enable universal group membership caching in each site.
- C. Raise the functional level of the fabrikam.com domain and the eu.fabrikam.com domain. Enable universal group membership caching in all sites.
- D. Upgrade the operating system on DC1 and DC2. Raise the functional level of the fabrikam.com domain.

Answer: A

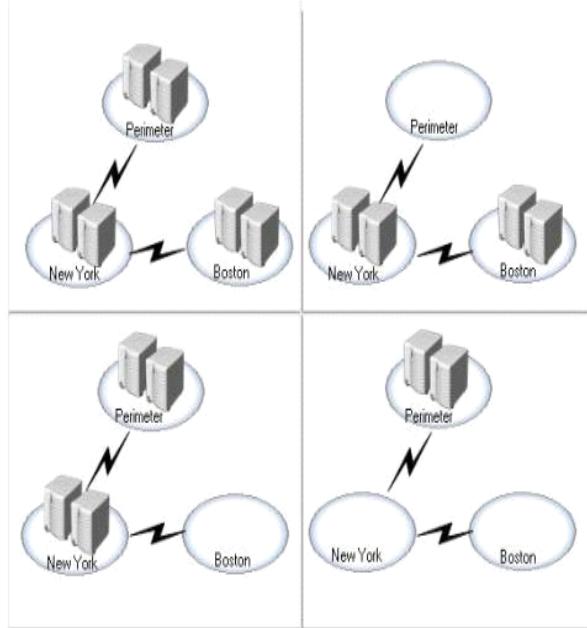
Question: 222

HOTSPOT

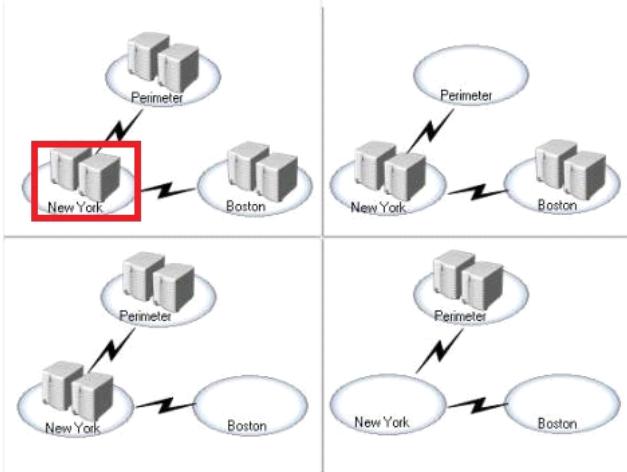
You are a network administrator for a company named Contoso, Ltd. The company has offices in New York and Boston. Each office contains an Active Directory site. The New York office also contains a perimeter network. All access to the Internet is routed through the perimeter network. Only TCP ports 80, 25, and 443 are allowed from the perimeter network to the internal network. You plan to deploy an Exchange Server 2010 Service Pack 1 (SP1) organization. Each site will contain a Mailbox server and a Hub Transport server. You need to recommend the appropriate placement of the Client Access servers for the organization. The solution must minimize the number of servers deployed. What should you recommend?

To answer, select the appropriate Client Access server design in the answer area.

Answer Area

**Answer:**

Answer Area

**Question: 223**

You are a network administrator for a school named Graphic Design Institute. The network contains an Exchange Server 2010 Service Pack 1 (SP1) organization named `graphicdesigninstitute.com`. Approximately 50,000 students enroll at the school each year. The students use Outlook Anywhere. At the beginning of each academic year, you plan to create 25 new mailbox databases to host all of the student mailboxes. You need to recommend which configurations must be performed on each new mailbox database. The solution must meet the following requirements:

- Minimize the amount of disk space required on the Mailbox servers.
- Ensure that the students can search for email addresses and office locations of teachers when they cannot access the school network.

What should you include in the recommendation? (Choose all that apply.)

- A. Modify the maintenance schedule of each mailbox database.
- B. Enable local continuous replication (LCR).
- C. Enable circular logging for each mailbox database.
- D. Configure the offline address book (OAB) properties of each mailbox database.
- E. Enable disk quotas for each volume.
- F. Create an offline address book (OAB) virtual directory for each mailbox database.

Answer: C, D

Explanation:

C and D are the best answers however please note that depending on how you will distribute your offline address books you might create a OAB virtual directory.

Although it is not recommended as a best practice, you can configure Exchange to save disk space by enabling circular logging. Circular logging allows Exchange to overwrite transaction log files after the data that the log files contain has been committed to the database.

In Exchange 2010, circular logging is disabled by default. By enabling it, you reduce drive storage space requirements. However, without a complete set of transaction log files, you can't recover any data more recent than the last full backup. Therefore, in a normal production environment, circular logging isn't recommended.

An offline address book (OAB) in Exchange Server 2010 is a copy of an address book that's been downloaded so that an Outlook user can access the information it contains while disconnected from the server. Exchange administrators can choose which address books are made available to users who work offline, and they can also configure the method by which the address books are distributed (Web-based distribution or public folder distribution).

Use the EMC to configure OAB properties

You need to be assigned permissions before you can perform this procedure. To see what permissions you need, see the "Offline address books" entry in the Mailbox Permissions topic.

In the console tree, navigate to Organization Configuration > Mailbox.

In the result pane, click the Offline Address Book tab, and then select the offline address book that you want to configure.

In the action pane, click Properties.

Use the General tab to view OAB properties and to set the update interval for the OAB.

Name This unlabeled box at the top of the tab displays the OAB name. You can modify this name. **Generation server** This read-only field displays the OAB generation server. The OAB generation server is the Mailbox server on which the OABs are generated. If you want to specify a different generation server, use the Move-OfflineAddressBook cmdlet with the Server parameter. For more information, see Move-OfflineAddressBook.

Default offline address book This read-only field displays a True or False status to indicate whether the selected OAB is the default OAB. If this isn't the default OAB, and you want to set it as the default, right-click the OAB in the result pane, and then click Set as Default.

Modified This read-only field displays the last date and time that the OAB was modified.

Update Schedule This list displays the time and interval for the regularly scheduled update.

To customize the schedule, select Use Custom Schedule from the list, and then click Customize to open the Schedule dialog box and specify the schedule you want.

Use the Address Lists tab to select the address lists you want to include in the OAB. If you want to include a global address list (GAL) other than the default GAL, you must use the Shell.

Include the default Global Address List Select this check box to include the default GAL in the OAB.

Include the following address lists Select this check box to add address lists to or remove address lists from the OAB.

Click Add to select one or more address lists to add to the OAB.

Click to remove the selected address list from the OAB.

Use the Distribution tab to specify the client support and OAB distribution points for the OAB.

Client Support Select the OAB version that will be generated for the version of Outlook that is used by your Exchange organization. If you have more than one version of Outlook in your organization, you can select one or more of the

following versions:

Outlook 98 SP1 or earlier (Version 2)

Outlook 98 SP2 or later (Version 3)

Outlook 2003 SP2 or later (Version 4)

If you don't select one of the Client Support options, Version 4 will be generated.

Distribution Points OAB distribution is the method by which the OAB can be accessed by users when they are working remotely or over a dial-up connection. To distribute the OAB, administrators can use Web-based distribution, public folder distribution, or both. An OAB distribution point is the HTTP Web address or public folder where client computers can download an OAB.

You can select one or both of the following check boxes:

Enable Web-based distribution Select this check box to enable Web-based distribution. Web-based distribution is the distribution method by which Outlook 2007 or later clients that are working offline or through a dial-up connection access the OAB. With Web-based distribution, a Client Access server will contain an OAB virtual directory for Web distribution purposes.

Click Add to specify the virtual directory or directories from which you want to distribute the OAB.

Click to remove the selected virtual directory from the OAB.

Enable public folder distribution Select this check box to enable public folder distribution. Public folder distribution is the distribution method by which Outlook 2003 or earlier clients that are working offline or through a dial-up connection access OABs.

Question: 224

DRAG DROP

You have an Exchange Server 2007 organization. All servers in the organization run Exchange Server 2007 Service Pack 1 (SP1). Your network contains two Active Directory sites named SiteA and SiteB. Only SiteA has a direct connection to the Internet. You plan to transition the organization to Exchange Server 2010 SP1. You need to recommend a transition solution to ensure that all of the mailboxes in SiteA can be moved to the Exchange Server 2010 SP1 servers. The solution must ensure that users in SiteB can send email messages to users in SiteA during the coexistence phase. What should you include in the recommendation?

Answer Area

- Upgrade all of the Exchange Server 2007 servers to Exchange Server 2010 RTM.
- Upgrade all of the Exchange Server 2007 servers to Exchange Server 2007 Service Pack 2 (SP2).
- Deploy an Exchange Server 2010 SP1 Client Access server to SiteA.
- Deploy an Exchange Server 2010 SP1 Client Access server to SiteB.
- Deploy an Exchange Server 2010 SP1 Hub Transport server to SiteB.
- Deploy an Exchange Server 2010 SP1 Hub Transport server and an Exchange Server 2010 SP1 Mailbox server to SiteA.

Answer

Question: 225

You have an Exchange Server 2010 Service Pack 1 (SP1) organization. You need to recommend a solution to ensure that an administrator is notified when the following events occur:

- Mailbox databases are dismounted.
 - The Microsoft Exchange Replication service stops.
- What should you include in the recommendation? (Each correct answer presents a complete solution. Choose all that apply.)
- A. Event Viewer tasks
 B. the Exchange Best Practice Analyzer
 C. the Microsoft Exchange Troubleshooting Assistant
 D. Microsoft System Center Configuration Manager
 E. Microsoft System Center Operations Manager
 F. administrator audit logging

Answer: A, D

Question: 226

DRAG DROP

You are planning an Exchange Server 2010 Service Pack (SP1) organization for a company named Contoso, Ltd. Your network contains two sites named Site1 and Site2. Site1 has an Internet connection. Site2 connects to the Internet through Site1. Each site will contain Client Access servers and Client Access arrays. The Client Access servers and the Client Access arrays will be configured as shown in the following table.

Server name	Server location	Array name
Server1.contoso.com	Site1	Array1
Server2.contoso.com	Site1	Array1
Server3.contoso.com	Site2	Array2
Server4.contoso.com	Site2	Array2

You plan to purchase SAN certificates for the Client Access servers. You need to identify the names for each SAN certificate for the Client Access methods in the following table.

Connection method	Name
RPC for MAPI clients in Site1	Array1.contoso.com
RPC for MAPI clients in Site2	Array2.contoso.com
Outlook Web App in Site1	Owa.contoso.com
Outlook Web App in Site2	Owa2.contoso.com
Autodiscover	Autodiscover.contoso.com

Which names should you identify?

To answer, drag the appropriate names to the correct certificate in the answer area.

Name	Answer Area
array1.contoso.com	Certificate for Site1 Name Name
array2.contoso.com	Certificate for Site2 Name Name
autodiscover.contoso.com	
owa.contoso.com	
owa2.contoso.com	
server1.contoso.com	
server2.contoso.com	
server3.contoso.com	
server4.contoso.com	

Answer:

Name	Answer Area
array1.contoso.com	Certificate for Site1 server4.contoso.com owa.contoso.com
array2.contoso.com	Certificate for Site2 autodiscover.contoso.com owa2.contoso.com
autodiscover.contoso.com	
owa.contoso.com	
owa2.contoso.com	
server1.contoso.com	
server2.contoso.com	
server3.contoso.com	
server4.contoso.com	

Question: 227

You have an Exchange Server 2010 Service Pack 1 (SP1) organization. All users access their mailbox by using Microsoft Outlook 2010. You plan to implement two Client Access servers. You need to design a Client Access server solution that meets the following requirements:

- Ensures that all of the users can access their mailbox if a Client Access server fails.

- Ensure that all of the users can access their mailbox if a Client Access server service fails.
What should you include in the design? (Choose all that apply.)

- a hardware based load balancer
- a Client Access array
- DNS round robin
- a Network Load Balancing cluster
- multiple MX records
- an SMTP relay

Answer: A, B

Question: 228

DRAG DROP

You have an Exchange Server 2010 Service Pack 1 (SP1) organization. You are planning the compliance infrastructure for the organization. You need to identify which Exchange technologies achieve the compliance requirements. What should you identify?

To answer, drag the appropriate technology to the correct compliance requirement in the answer area.

Technology	Answer Area
a cmdlet Extension Agent	Technology Automatically enable single item recovery for each new mailbox.
a litigation hold	Technology Provide an administrator with the ability to perform cross-mailbox searches from the Exchange Control Panel (ECP).
managed folders	Technology Prevent specific users from permanently deleting email messages and calendar items from their mailbox.
Outlook Web App mailbox policies	
retention policies	
Role Based Access Control (RBAC)	

Answer

Technology	Answer Area
	a cmdlet Extension Agent Automatically enable single item recovery for each new mailbox.
	Role Based Access Control (RBAC) Provide an administrator with the ability to perform cross-mailbox searches from the Exchange Control Panel (ECP).
managed folders	a litigation hold Prevent specific users from permanently deleting email messages and calendar items from their mailbox.
Outlook Web App mailbox policies	
retention policies	

Question: 229

You plan to implement an Exchange Server 2010 Service Pack 1 (SP1) organization. You identify the following compliance requirements for the Exchange organization:

- Provide members of a security group named Legal with the ability to change message classification settings and retention policy tags.
- Provide members of a security group named Legal Management with the ability to view the results from searches performed across multiple mailboxes.

You need to identify which permissions or management roles must be assigned to achieve the compliance requirements. The solution must minimize the number of rights assigned to users. What should you identify? (Choose all that apply.)

- A. the Records Management management role
- B. the Discovery Management management role
- C. the Server Management management role
- D. Full Mailbox Access permission to an arbitration mailbox
- E. Full Mailbox Access permission to the Discovery Search Mailbox
- F. the Organization Management management role

Answer: A, E

Explanation:

The Records Management management role group is one of several built-in role groups that make up the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2010. Role groups are assigned one or more management roles that contain the permissions required to perform a given set of tasks.

The members of a role group are granted access to the management roles assigned to the role group. For more information about role groups, see Understanding Management Role Groups.

Users who are members of the Records Management role group can configure compliance features, such as retention policy tags, message classifications, and transport rules.

Question: 230

DRAG DROP

You have an Exchange Server 2010 Service Pack 1 (SP1) organization. The organization contains 1,000 mailbox-enabled users. The maximum mailbox size for each user is 500 MB. The users have Personal Archives. You plan to deploy a new Mailbox server that will host multiple mailbox databases. The disks on the new server are configured as shown in the following table.

Disk set name	Storage type	Disk size	Hard disk speed
Set1	RAID 1	100 GB	10,000 RPM
Set2	RAID 1	100 GB	15,000 RPM
Set3	RAID 5	750 GB	15,000 RPM
Set4	RAID 5	2 terabytes	10,000 RPM

You need to recommend configurations for the hard disk of the Mailbox server. The configurations must meet the following requirements:

- Minimize impact if a single disk fails.
- Maximize the speed of read and write operations to the mailbox databases.

Which server configurations should you recommend?

To answer, drag the appropriate configuration to the correct disk set in the answer area.

Configuration	Answer Area
mailbox database	Set1 Configuration
mailbox database transaction logs	Set2 Configuration
operating system	Set3 Configuration
Personal Archive database	Set4 Configuration

Answer

Configuration	Answer Area
	Set1 mailbox database
	Set2 mailbox database transaction logs
	Set3 operating system
	Set4 Personal Archive database

Question: 231 DRAG**DROP**

You are planning the audit and discovery infrastructure for an Exchange Server 2010 Service Pack 1 (SP1) organization. You need to identify which Exchange technologies achieve your audit and discovery requirements. What should you identify?

To answer, drag the appropriate technology to the correct audit and discovery requirement in the answer area.

Technology	Answer Area
a litigation hold	Technology Identify which user account deletes a specified mailbox.
a multi-mailbox search	Technology Identify which user sent an email message as another user.
administrator audit logging	Technology Discover email messages in specified mailboxes by using keywords.
mailbox audit logging	Technology Automatically move items to a specified location based on a specified criterion.
retention policies	

Answer

Technology	Answer Area
a litigation hold	administrator audit logging Identify which user account deletes a specified mailbox.
	mailbox audit logging Identify which user sent an email message as another user.
	a multi-mailbox search Discover email messages in specified mailboxes by using keywords.
	retention policies Automatically move items to a specified location based on a specified criterion.

Question: 232 DRAG DROP

You have an Exchange Server 2010 Service Pack 1 (SP1) organization named contoso.com. A partner company named Fabrikam, Inc., has an Exchange Server 2010 (SP1) organization named fabrikam.com. All client computers in contoso.com and fabrikam.com run Microsoft Outlook 2010. You need to ensure that users in fabrikam.com can view the availability information of users in contoso.com. What should you do?

Answer Area
Create a forest trust from contoso.com to fabrikam.com.
Create a forest trust from fabrikam.com to contoso.com.
From contoso.com, create a federated trust.
From fabrikam.com, create a federated trust.
From contoso.com, create an organization relationship.
From fabrikam.com, create an organization relationship.
From contoso.com, modify the authentication settings of the EWS virtual directory.
From fabrikam.com, modify the authentication settings of the EWS virtual directory.

Answer:

Answer Area
From contoso.com, create a federated trust.
From fabrikam.com, create a federated trust.
From contoso.com, create an organization relationship.

Explanation:

I think this answer is wrong and the correct answer is that Fabrikam should created the trust and the organization relationship

Implementing Federated Sharing

With federated sharing, you can use federation technologies to establish trusted relationships and hence enable secure Internet communications between organizations. This requires that you use Microsoft Federation Gateway as a trust broker, that each participating organization establish and manage its trust, and that federated sharing is supported for all messaging clients. To establish a federation trust, organizations exchange security certificates with public keys with each other or with a trusted third party and use those certificates to authenticate and secure all interorganizational communications.

The Microsoft Federation Gateway The Microsoft Federation Gateway is an identity service that runs over the Internet and functions as a trust broker for federated sharing. It provides a broker service to establish the communication between the organizations but does not authenticate individual users or store any user account information from either organization. To enable federated sharing, you need to register your organization with the Federation Gateway and then configure a federated sharing relationship with another organization that also registers with the Federation Gateway. The Federation Gateway then acts as a hub for all connections that the organizations make with each other. For example, Client Access servers in each organization connect through the Federation Gateway to exchange availability information and enable calendar sharing. These Client Access servers use the federated trust that you configure with the Federation Gateway to verify your partner's Client Access servers and to encrypt traffic sent between the organizations. Users can also send encrypted and authenticated email messages between the organizations.

In federated sharing, each organization needs only to manage its trust relationship with the Federation Gateway and its own user accounts. After an organization establishes a trust relationship with the Federation Gateway, you can identify other trusted organizations and the types of information you want to share with them.

When you enable federation sharing, all interorganizational communication is sent through your organization's Exchange Server 2010 servers. This traffic is transparent to the messaging clients so that federated sharing works with any client that can connect to Exchange Server 2010, including Microsoft Outlook Web Access, Outlook 2003, Outlook 2007, and Outlook 2010.

Note:

FEDERATION GATEWAY

For more information about the Federation Gateway, see <http://msdn.microsoft.com/en-us/library/cc287610.aspx>. For information about how to connect to and use the Federation Gateway, see <http://msdn.microsoft.com/en-us/library/dd164396.aspx>.

Federated Sharing Requirements

To implement federated sharing, you need to establish and configure the following components in Exchange Server 2010:

A federation trust A federation trust configures the Federation Gateway as a federation partner with the Exchange Server organization, which enables Exchange Server 2010 Web Services on the Client Access servers to validate all Federation Gateway authentication requests. You establish a federation trust by submitting your organization's public key and a valid X.509 certificate issued by a Certificate Authority (CA) trusted by Windows Live Domain Services to the Federation Gateway and downloading the Federation Gateway public key and certificate.

An organization identifier An organization identifier defines what authoritative domains in an Exchange organization are available for federation. If your organization supports multiple SMTP domains, you can include one or all of your domain names in your organization identifier. Users can participate in Federated Sharing only if they have email addresses in the domains that you configure with the organization identifier. The first domain you specify with the organization identifier is known as the account namespace. Federation Gateway creates federated user identifiers within this namespace when the Client Access server requests a delegation token for a user. This process is transparent to the Exchange Server organization.

Create a new organisational relationship

To enable free/busy sharing between two cloud-based organisations, run the following command:

```
Get-FederationInformation -DomainName <the other cloud-based organization> | New-OrganizationRelationship -Name <the other tenant domain> -FreeBusyAccessEnabled $true -FreeBusyAccessLevel LimitedDetails
```

Here's an example of what the command would look like in the Contoso scenario, where the administrator for the

Contoso organisation configures an organisational relationship with Fabrikam College:

```
Get-FederationInformation -DomainName fabrikam.edu | New-OrganizationRelationship -Name Fabrikam -FreeBusyAccessEnabled $true -FreeBusyAccessLevel LimitedDetails
```

Question: 233

Your network contains an Active Directory forest named contoso.com and two Active Directory sites named Site1 and Site2.

You plan to deploy an Exchange Server 2010 Service Pack 1 (SP1) organization.

An independent consultant recommends a design for the Exchange Server 2010 SP1 deployment as shown in the following table.

Server name	Server role	Database name	Site name
DC1	Domain controller Global catalog Certification authority (CA) DNS	Not applicable	Site1
DC2	Domain controller Global catalog	Not applicable	Site2
EX1	Mailbox Client Access Hub Transport	Mailbox Database 1	Site1
EX2	Mailbox	Mailbox Database 2	Site1
EX3	Mailbox Client Access Hub Transport	Mailbox Database 3	Site2
EX4	Mailbox	Mailbox Database 4	Site2

You need to recommend a change to the current Exchange Server 2010 SP1 design that will ensure that all users can access their mailbox if DC1 or DC2 fails.

Which change should you recommend?

- A. shadow redundancy
- B. an activation preference for a database
- C. a database availability group (DAG)
- D. Datacenter Activation Coordination (DAC) mode
- E. a DNS server on DC2
- F. delayed acknowledgments (ACKs)
- G. local continuous replication (LCR) on EX1, EX2, EX3, and EX4
- H. a single copy cluster (SCC)
- I. DNS round robin on DC1 and DC2
- J. Edge Transport server cloned configuration
- K. EdgeSync synchronization
- L. a Hosts file on EX1, EX2, EX3, and EX4

Answer: E

Explanation:

Test4Sure had e as the correct answer however I do not see how that even makes sense. If it is a domain controller then it has DNS running as there is no way to install a domain controller without it. However it is the only answer that does seem to work.

Question: 234

You have an Exchange Server 2010 Service Pack 1 (SP1) organization that contains one Mailbox server. The organization has 4,000 users. All users connect to their mailbox by using Microsoft Outlook 2010. You plan to switch the Mailbox server for a new server. You purchase a new server that runs Windows Server 2008 R2. You install Exchange Server 2010 SP1 on the new server. You need to recommend which tools can identify whether the new server can adequately support the 4,000 mailboxes. Which tools should you recommend? (Choose all that apply.)

- A. Exchange Pre-deployment Analyzer
- B. Exchange Load Generator
- C. Exchange Server Profile Analyzer
- D. Deployment Assistant
- E. Exchange Server Jetstress 2010

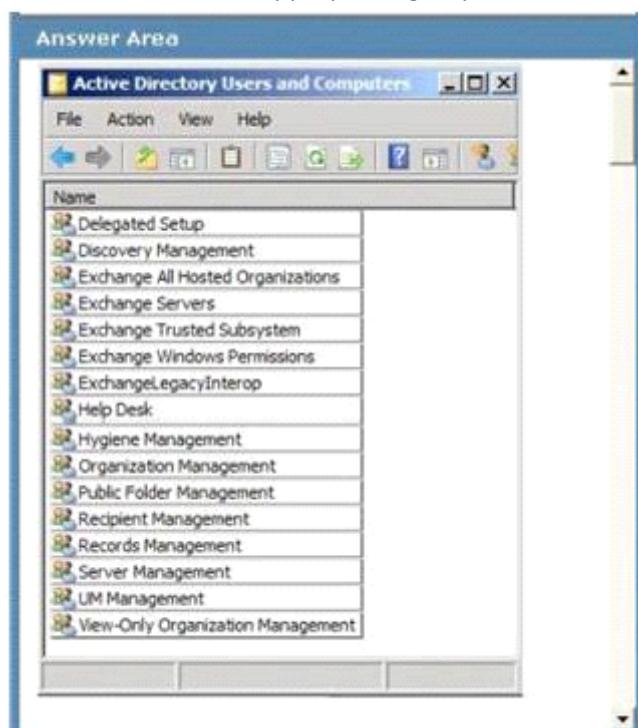
Answer: B, E

Question: 235

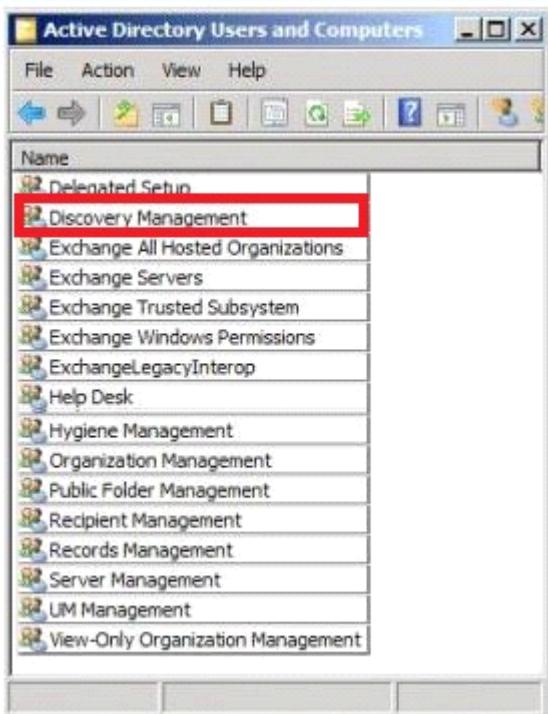
HOTSPOT

You have an Exchange Server 2010 Service Pack 1 (SP1) organization. Corporate security policy states that the members of a security group named Legal must be able to search all mailbox content in the organization. You plan to add the Legal group to an another security group that has the required permissions. You need to identify which group must be used to meet the requirement of the security policy. Which group should you identify?

To answer, select the appropriate group in the answer area.



Answer:



The Discovery management is the correct answer

Question: 236

You have an Exchange Server 2010 Service Pack 1 (SP1) organization. You identify the following compliance requirements for the organization:

- Provide an administrator with the ability to perform cross-mailbox searches from the Exchange Control Panel (ECP).
- Prevent specific users from permanently deleting email messages and calendar items from their mailbox.

You need to identify which Exchange technologies meet the compliance requirements. Which technologies should you identify? (Choose all that apply.)

- A. a cmdlet Extension Agent
- B. Role Based Access Control (RBAC)
- C. retention policies
- D. a litigation hold
- E. outlook Web App mailbox policies
- F. managed folders

Answer: B, D

Question: 237

DRAG DROP

Your network contains four Active Directory sites. The sites are configured as shown in the following table.

Site name	Number of users
New York	800
Montreal	2,000
Seattle	50
Miami	50

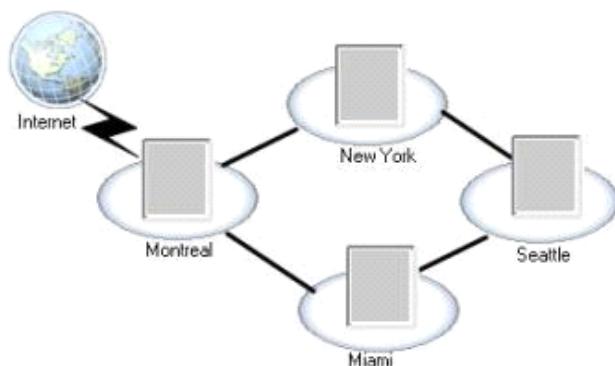
You plan to deploy a new Exchange Server 2010 Service Pack 1 (SP1) organization named fabrikam.com. You plan to

deploy Mailbox servers to the New York site and the Montreal site. You need to plan the deployment of Client Access servers to meet the following requirements:

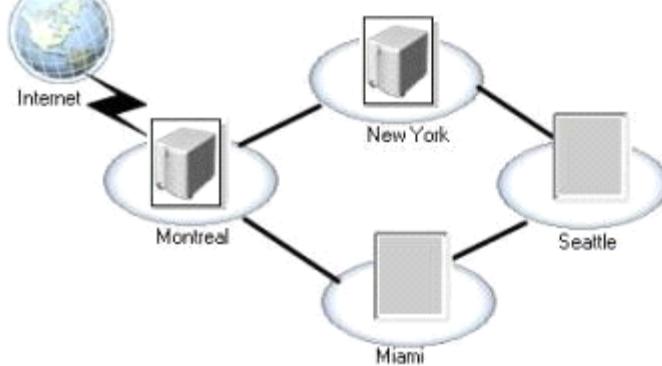
- Support users who use Outlook Web App to access their mailbox from the Internet through Montreal.
- Support users who use Outlook Anywhere to access their mailbox from the Internet through Montreal.
- Minimize the number of Exchange server roles deployed.

Where should you deploy the Client Access servers?

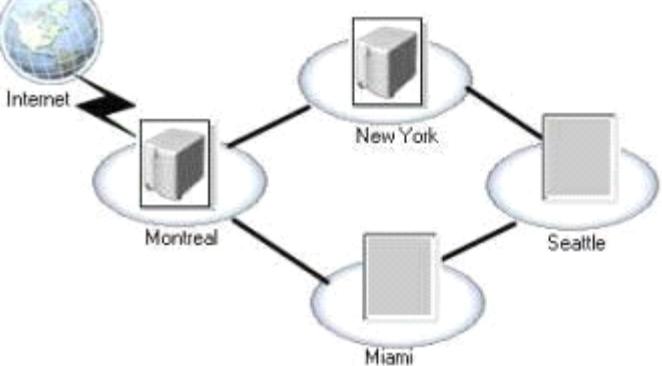
To answer, drag the Client Access server to the correct site or sites in the answer area.

Client Access server	Answer Area
	

Answer

Client Access server	Answer Area
	

Explanation:

Client Access server	Answer Area
	

Question: 238

You have an Exchange Server 2010 Service Pack 1 (SP1) organization. You need to ensure that when a new mailbox-enabled user is created, the configurations shown in the following table are set by default.

Configuration	State
POP3	Disabled
IMAP4	Disabled
Single item recovery	Enabled
Exchange ActiveSync	Disabled

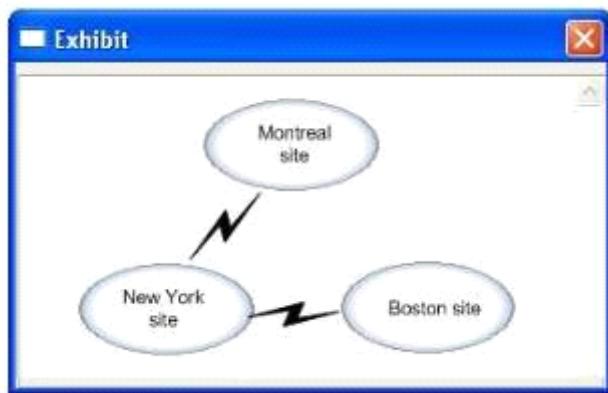
What should you use? (Each correct answer presents a complete solution. Choose all that apply.)

- A. Microsoft System Center Configuration Manager
- B. email address policies
- C. a template user account
- D. Microsoft System Center Operations Manager
- E. a Windows PowerShell script
- F. cmdlet extension agents

Answer: E, F

Question: 239

You are a network administrator for a company named Contoso, Ltd. The company has offices in New York, Boston and Montreal. Each office contains an Active Directory site as show in the exhibit. (Click the Exhibit button.)



All access to the Internet is routed through the Montreal office. Only TCP ports 80, 25, and 443 are allowed from the Internet to the internal network. You plan to deploy an Exchange Server 2010 Service Pack 1 (SP1) organization. Each site will contain a Mailbox server and a Hub Transport server. You need to recommend where to place the Client Access servers for the organization. The solution must minimize software costs. Where should you recommend placing the Client Access servers?

- A. in the Boston site and the New York site
- B. in the Montreal site and the New York site
- C. in the Montreal site only
- D. in the Montreal site, the New York site, and the Boston site

Answer: D

Question: 240**DRAG DROP**

Your network contains an Active Directory domain named contoso.com. The domain contains a single Active Directory site. The network contains a server named Server1 that runs Exchange Server 2003. Server1 uses forms-based authentication for Outlook Web Access (OWA). Users access OWA from the corporate network and from the Internet by using the URL <https://owa.contoso.com/exchange>.

You plan to deploy a server named Server2 to the current Exchange organization. Server2 will run Exchange Server 2010 Service Pack 1 (SP1) and will have the following server roles installed:

- Mailbox
- Client Access
- Hub Transport

During the next three months, you plan to move the users to Server2. You need to recommend changes to the Exchange organization to ensure that all of the users can access OWA and Outlook Web App by using <https://mail.contoso.com/owa>.

Which changes should you recommend?

To answer, drag the appropriate changes to the correct location or locations in the answer area.

Configuration	Answer Area
Disable forms-based authentication.	Server1 Configuration Configuration
Configure the Exchange2003URL property.	Server2 Configuration Configuration
Replace the Web server certificate with a certificate that has the mail.contoso.com host name.	

Answer:

Configuration	Answer Area
Disable forms-based authentication.	Server1 Replace the Web server certificate with a certificate that has the mail.contoso.com host name. Replace the Web server certificate with a certificate that has the mail.contoso.com host name.
Configure the Exchange2003URL property.	Server2 Configure the Exchange2003URL property. Configure the Exchange2003URL property.
Replace the Web server certificate with a certificate that has the mail.contoso.com host name.	

Explanation:

I am not sure on this question however I do feel that you will need to the following

Change the URL on the Exchange 2003 Server and replace the Certificate.

As I read the question you plan to deploy server 2? That tells me it is not deployed so what is there to configure?

Question: 241

Your company plans to deploy Exchange Server 2010 Service Pack 1 (SP1). The company's security policy has the following requirements:

- Users who access the Exchange organization from the Internet must use a smart card or an X.509 certificate for authentication.
- All access to the Exchange organization from the Internet must pass through Microsoft Forefront Threat Management Gateway (TMG).

You need to identify which client connection methods can be implemented based on the security policy. What should you identify? (Choose all that apply.)

- A. Outlook Web App
- B. POP3
- C. IMAP4
- D. Exchange ActiveSync
- E. the Exchange Control Panel (ECP)

Answer: A, D, E

Explanation:

The Exchange Control Panel is a Web application that runs on a Client Access Server providing services for the Exchange organization. This Exchange Control Panel is installed automatically when you install a Client Access server. To manage Exchange from just about anywhere, you simply need to enter the URL path for the application in your browser's Address field. You can then access the Exchange Control Panel. By default, the Exchange Control Panel URL is <https://yourserver.yourdomain.com/ecp>.

The Client Access server to which you connect processes your remote actions via the ECP application running on the default Web site. The physical directory for this application is %ExchangeInstallPath%\ClientAccess\ECp. And it runs in the context of an application pool named MSExchangeECPAppPool. In the % ExchangeInstallPath%\ClientAccess\ECp directory on your server, you'll find a web.config file that defines the settings for the ECP application.

When you install an Exchange server, the setup process creates a self-signed Security certificate. Because this default certificate is not issued by a trusted authority, you will see a related error message when you use HTTPS to access services hosted by your Client Access servers. By default, Client Access servers are configured to use Secure HTTP (HTTPS) for Outlook Web App. When you install Exchange Server 2010, a self-signed security certificate is automatically issued for the Client Access server. Since this default certificate is not issued by a trusted certificate authority, users will see a warning when they access OWA stating that there is a problem with the Web site's security certificate.

At the warning prompt, the user simply needs to click the Continue To This Website link to access the Outlook Web App. Of course, this warning can be disconcerting to the user and have users click to continue anyway sets a bad precedent, training users to ignore online security warnings.

The user will see this warning continuously until you install a certificate from a trusted source on the server.

X 509 Certificate What are colloquially known as SSL certificates should be referred to as X.509 certificates. The term SSL certificate became common due to the adoption of the X.509 (one of the ITU X.500 Directory standards) certificate format by Netscape when it designed the original versions of the SSL protocol, eons ago, when the world was still young and the Internet was a friendly place. The term 'SSL certificate' persisted simply because given the choice of saying SSL certificate or 'X.509 certificate' which would you choose?

<http://www.zytrax.com/tech/survival/ssl.html#x509-overview>

Question: 242

Your network contains an Active Directory forest named contoso.com and two Active Directory sites named Site1 and Site2. You plan to deploy an Exchange Server 2010 Service Pack 1 (SP1) organization. An independent consultant recommends a design for the Exchange Server 2010 SP1 deployment as shown in the following table.

Server name	Server role	Database name	Site name
DC1	Domain controller Global catalog Certification authority (CA) DNS	Not applicable	Site1
DC2	Domain controller Global catalog	Not applicable	Site2
EX1	Mailbox Client Access Hub Transport	Mailbox Database 1	Site1
EX2	Mailbox	Mailbox Database 2	Site1
EX3	Mailbox Client Access Hub Transport	Mailbox Database 3	Site2
EX4	Mailbox	Mailbox Database 4	Site2

You are evaluating the implementation of a Network Load Balancing cluster on the Exchange servers. You need to identify which potential Exchange server configuration will prevent the implementation of the Network Load Balancing cluster. What should you identify?

- A. DNS round robin on DC1 and DC2
- B. a database availability group (DAG)
- C. an activation preference for a database
- D. shadow redundancy
- E. EdgeSync synchronization
- F. a single copy cluster (SCC)
- G. Edge Transport server cloned configuration
- H. local continuous replication (LCR) on EX1, EX2, EX3, and EX4
- I. a Hosts file on EX1, EX2, EX3, and EX4
- J. Datacenter Activation Coordination (DAC) mode
- K. a DNS server on DC2
- L. delayed acknowledgments (ACKs)

Answer: B

Explanation:

Before we continue, we need to discuss an important design consideration regarding the load balancing of the Client Access Server role. In the configuration presented above, the Client Access Server role is coexisting on the same servers as the Mailbox server role. Since the mailbox servers are part of a DAG, which itself uses Windows Failover Clustering, it is not possible to implement Windows Network Load Balancing (WNLB) as the high availability mechanism for the Client Access Server role. As explained in the Exchange 2010 product documentation, under the section titled “Two-member DAG in Single Datacenter/Active Directory Site”, this is because WNLB and Windows Failover Clustering cannot be installed on the same server. Therefore, in this particular configuration, an external load balancing solution will be required, although that particular facet of configuration is outside the scope of this article.

<http://www.simple-talk.com/sysadmin/exchange/exchange-2010-dag-creation-and-configuration-part-1/>

Question: 243

DRAG DROP

Your network contains an Active Directory domain named litwareinc.com. The domain contains two sites named Montreal and Toronto. Only Toronto has a direct connection to the Internet. The network contains an Exchange Server 2010 Service Pack 1 (SP1) organization that has two Client Access servers in each site. Each site contains an internal load balancing solution and an external load balancing solution. The relevant host records for the load balancing

solutions are configured as shown in the following table.

IP address	Host name	Network	Site
10.0.0.1	Cas.litwareinc.com	Internet	Not applicable
192.168.1.1	Cas1.litwareinc.com	Internal	Montreal
192.168.2.1	Cas2.litwareinc.com	Internal	Toronto

The company uses a split DNS zone. You need to identify which internal URLs and external URLs must be configured for Outlook Web App in both sites. Which URLs should you identify?

To answer, drag the appropriate URL or URLs to the correct site or sites in the answer area.

URL

- \$null
- https://cas.litwareinc.com/owa
- https://cas1.litwareinc.com/owa
- https://cas2.litwareinc.com/owa
- https://cas.litwareinc.local/owa

Answer Area

Internet

Toronto

Montreal

Toronto i

URL

Toronto

URL

Montreal

URL

Montreal

\$null

Answer:

URL

-
-
-
-
- https://cas.litwareinc.local/owa

Answer Area

Internet

Toronto

Montreal

Toronto i

URL

Toronto

URL

Montreal

URL

Montreal

\$null

Question: 244

Your network contains two Active Directory forests. The forests contain domain controllers that run Windows Server 2008 R2. The forests are configured as shown in the following table.

Forest name	Number of domains	Number of users
Adatum.com	4	6,000
Litwareinc.com	1	2,000

A one-way forest trust exists from adatum.com to litwareinc.com. You plan to deploy an Exchange Server 2010 Service

Pack 1 (SP1) organization. The organization will contain Mailbox servers in litwareinc.com. You need to ensure that users in adatum.com can access the mailboxes in the Exchange organization. What should you do?

- A. Create a forest trust from litwareinc.com to adatum.com. Create linked mailboxes in litwareinc.com.
- B. Create a forest trust from litwareinc.com to adatum.com. Create resource mailboxes in litwareinc.com.
- C. Change the forest trust to an external trust. Create linked mailboxes in litwareinc.com.
- D. Deploy Mailbox servers to adatum.com. Create resource mailboxes in litwareinc.com.

Answer: A

Explanation:

Linked mailboxes are user mailboxes that are accessed by users in a separate, trusted forest

http://forums.msexchange.org/m_1800450025/mpage_1/key_tm.htm#1800553199

Question: 245

Your network contains one Active Directory site. You have an Exchange Server 2010 organization that contains the following servers:

- A Client Access server named CAS1.
- A Hub Transport server named Hub1.
- Two servers named Server1 and Server2. Both Server1 and Server2 have the Mailbox server role installed, the Client Access server role installed, and are members of a database availability group (DAG).

You need to ensure that users can send e-mail messages to the Internet if a single server fails. What should you recommend?

- A. Add the Hub Transport server role to CAS1. Modify the Send connector.
- B. Add an Edge Transport server. Create a new Edge subscription.
- C. Add the Client Access server role to Hub1. Create a Client Access server array.
- D. Add an Edge Transport server. Configure a Network Load Balancing cluster.

Answer: A

Explanation:

Pass4Sure did not have an answer for this question

The question is asking that users can send mail if a single server fails. As I read the question I see only one Hub Transport Server which is Hub1

So I feel that A - adding another hub server to Cas1 will provide the solution

Question: 246

Your network contains an Active Directory forest named contoso.com and two Active Directory sites named Site1 and Site2. You plan to deploy an Exchange Server 2010 Service Pack 1 (SP1) organization. An independent consultant recommends a design for the Exchange Server 2010 SP1 deployment as shown in the following table.

Server name	Server role	Database name	Site name
DC1	Domain controller Global catalog Certification authority (CA) DNS	Not applicable	Site1
DC2	Domain controller Global catalog	Not applicable	Site2
EX1	Mailbox Client Access Hub Transport	Mailbox Database 1	Site1
EX2	Mailbox	Mailbox Database 2	Site1
EX3	Mailbox Client Access Hub Transport	Mailbox Database 3	Site2
EX4	Mailbox	Mailbox Database 4	Site2

You plan to replicate the mailbox databases from Site1 to Site2. You need to identify which Exchange server configuration will provide the ability to replicate the mailbox databases. What should you identify?

- A. a Hosts file on EX1, EX2, EX3, and EX4
- B. delayed acknowledgments (ACKs)
- C. local continuous replication (LCR) on EX1, EX2, EX3, and EX4
- D. a single copy cluster (SCC)
- E. Edge Transport server cloned configuration
- F. Datacenter Activation Coordination (DAC) mode
- G. an activation preference for a database
- H. shadow redundancy
- I. a DNS server on DC2
- J. DNS round robin on DC1 and DC2
- K. EdgeSync synchronization
- L. a database availability group (DAG)

Answer: L

Question: 247

You have an Exchange Server 2010 Service Pack 1 (SP1) organization named fabrikam.com.

All users access their mailbox by using Microsoft Outlook 2010. You identify the following compliance requirements for the Exchange organization:

- Ensure that all of the users can prevent confidential email messages from being forwarded to other recipients.
- Ensure that all of the users receive a warning message before they send email messages to the company's executives.

You need to identify which Exchange technologies meet the compliance requirements. Which technologies should you identify? (Choose all that apply.)

- A. Information Rights Management (IRM)
- B. MailTips
- C. a Hub Transport rule
- D. managed folders
- E. a litigation hold

Answer: A, B, C

Explanation:

You need to have Hub Transport Rules to make A and B work Every day, information workers use e-mail to exchange sensitive information such as financial reports and data, legal contracts, confidential product information, sales reports and projections, competitive analysis, research and patent information, and customer and employee information. Because people can now access their e-mail from just about anywhere, mailboxes have transformed into repositories containing large amounts of potentially sensitive information. As a result, information leakage can be a serious threat to organizations. To help prevent information leakage, Microsoft Exchange Server 2010 includes Information Rights Management (IRM) features, which provide persistent online and offline protection of e-mail messages and attachments.

<http://technet.microsoft.com/en-us/library/dd638140.aspx>

Question: 248

Your network contains an Active Directory forest named contoso.com and two Active Directory sites named Site1 and Site2. You plan to deploy an Exchange Server 2010 Service Pack 1 (SP1) organization. An independent consultant recommends a design for the Exchange Server 2010 SP1 deployment as shown in the following table.

Server name	Server role	Database name	Site name
DC1	Domain controller Global catalog Certification authority (CA) DNS	Not applicable	Site1
DC2	Domain controller Global catalog	Not applicable	Site2
EX1	Mailbox Client Access Hub Transport	Mailbox Database 1	Site1
EX2	Mailbox	Mailbox Database 2	Site1
EX3	Mailbox Client Access Hub Transport	Mailbox Database 3	Site2
EX4	Mailbox	Mailbox Database 4	Site2

You are evaluating the implementation of Edge Transport servers in the organization. You need to identify which Exchange server configuration must be implemented to copy the list of Exchange recipients to the Edge Transport servers. What should you identify?

- A. delayed acknowledgments (ACKs)
- B. Edge Transport server cloned configuration
- C. DNS round robin on DC1 and DC2
- D. EdgeSync synchronization
- E. shadow redundancy
- F. a single copy cluster (SCC)
- G. local continuous replication (LCR) on EX1, EX2, EX3, and EX4
- H. a DNS server on DC2
- I. a database availability group (DAG)
- J. a Hosts file on EX1, EX2, EX3, and EX4
- K. Datacenter Activation Coordination (DAC) mode
- L. an activation preference for a database

Answer: D

Question: 249

Which of the following cmdlets allows you to connect a disconnected mailbox to a newly created Active Directory user account?

- A. Create-MailboxDatabase
- B. Configure-MailboxDatabase
- C. Add-MailboxDatabase
- D. New-MailboxDatabase

Answer: D

Explanation:

To create a new mailbox database from the Exchange Management Shell, you will need to use the New-MailboxDatabase cmdlet.

Question: 250

You need to add EXSRV02 to host a copy of the Sales public folder and the folders below it. Which command should you run?

- A. AddReplicaToPFRRecursive.ps1 -TopPublicFolder
- B. ReplaceReplicaOnPFRRecursive.ps1 -TopPublicFolder "\Sales" -ServerToAdd EXSRV02
- C. AddReplicaToPFRRecursive.ps1 -TopPublicFolder "\" -ServerToAdd EXSRV02
- D. ReplaceReplicaOnPFRRecursive.ps1 -TopPublicFolder "\Sales" -ServerToAdd EXSRV02

Answer: A

Explanation:

To add a copy or replica for all public folders for the Sales folder and all folders underneath it, use the included AddReplicaToPFRRecursive.ps1 script. The ReplaceReplicaOnPFRRecursive.ps1 script removes one server and adds another server.

Question: 251

You are the messaging professional for an engineering firm. The firm has considered deploying Exchange 2010 into their environment. You need to determine the Mailbox Server requirements. Which items are included in the hardware sizing process? Choose all that apply. Choose 3

- A. Create an Exchange configuration
- B. Identify Exchange public folder permissions
- C. Validate the Exchange configuration
- D. Identify Exchange usage profile

Answer: A, C, D

Explanation:

The hardware sizing process is: identify Exchange usage profile, create an Exchange configuration and validate the Exchange configuration.

Question: 252

You have created a Customer Service public folder and mail-enabled it so that it can receive emails for the customer service department. You need to give Brendan access to send email as the public folder so all of the replies are directed back to the Customer Service public folder. Which command should you run?

- A. Add-ADPermission "Customer Service" -User "Brendan" -Extendedrights "Send As"
- B. Add-PublicFolderAdministrativePermission -Identity "\Customer Service" -User "Brendan" -AccessRights AllExtendedRights
- C. Add-PublicFolderClientPermission -Identity "\Customer Service" -AccessRights Contributor -User Brendan
- D. Add-ADPermission "Customer Service" -User "Brendan" -Extendedrights "Receive As"

Answer: A

Explanation:

The Send As permission is an Active Directory right and must be assigned to the public folder object using the Add-ADPermission cmdlet. The other cmdlets will modify the administrative and client permissions but do not achieve the desired result.

Question: 253

When planning memory requirements for a Mailbox server, you have a range of RAM to add for each mailbox hosted on the server. What are the minimum and maximum values of this range of RAM that Microsoft specifies?

- A. 2 MB for light users to 5 MB for heavy users
- B. 3.5 MB for light users to 5 MB for heavy users
- C. 2 MB for light users to 7.5 MB for heavy users
- D. 3.5 MB for light users to 7.5 MB for heavy users

Answer: A

Explanation:

The Mailbox server should have a minimum of 2 GB of RAM installed plus an additional 2 MB for each light user (5 messages sent/20 messages received per day), 3.5 MB for each average user (10 messages sent/40 messages received per day), or 5 MB for each heavy user (20 messages sent/80 messages received per day).

Question: 254

What configuration do you need to make to allow the Exchange organization to accept messages for other domain namespaces?

- A. Remote domains
- B. SMTP send connector
- C. Accepted domains
- D. SMTP receive connector

Answer: C

Explanation:

Accepted domains are used to specify the SMTP domains for which the Exchange Server organization will accept and/or route messages.

Question: 255

You are the messaging professional. You need to make a business case to present to your organization's technology committee which will support your recommendation to create multiple databases on the Exchange 2010 server, instead of putting all mailboxes into a single database. What benefits of multiple databases should you present? Choose all that apply. Choose 3

- A. A single database failure will impact fewer mailboxes, because mailboxes are in multiple databases
- B. Database restores can be done faster since each database is smaller
- C. A single database failure will impact more mailboxes, because mailboxes are in multiple databases
- D. Databases can be used to define mailbox limits, rather than applying limits directly to each mailbox.

Answer: A, B, D

Explanation:

Rather than putting all mailboxes in a single database, creating multiple databases has the following benefits:

A single database failure will impact fewer mailboxes, because mailboxes are in multiple databases.

A database restore can be done faster since each database is smaller.

Databases can be used to organize mailboxes.

Databases can be used to define mailbox limits, rather than applying limits directly to each mailbox.

Question: 256

What PowerShell command can you use on a Client Access server to modify the startup properties of the IMAP4 service?

- A. Set-Service
- B. Put-Service
- C. Change-Service
- D. Get-Service

Answer: A

Explanation:

You will use the Set-Service cmdlet to change the startup properties for a service.

Question: 257

You are the messaging professional. The firm you work for has required you to provide a way to approve or reject a message before it is sent to the companies All Users distribution group. What should you do to meet this new requirement?

- A. Specify a moderation recipient for the distribution group
- B. Specify an inbox rule to forward all requests to the approve
- C. Add the approver to the domain admins AD group
- D. Add the approver to the Exchange Server Administrators role

Answer: A

Explanation:

Now Administrators have the ability to specify a moderation recipient for a mailbox recipient or distribution group. All messages sent to mailbox recipient or distribution group is sent to the moderation recipient for approval or rejection.

Question: 258

You are configuring your Internet-accessible Client Access servers to provide Outlook Web App, Outlook Anywhere, and Autodiscover services. You need to obtain the fewest number of certificates to secure the clients' connection to these servers. According to the recommended practice, which type of certificate will you need to obtain to provide trusted secure access to both domain-joined and non-domain-joined devices?

- A. Enterprise CA certificate
- B. User certificate
- C. Trusted third-party UCC certificate
- D. Trusted third-party certificate

Answer: C

Explanation:

A trusted third-party UCC certificate will handle multiple services and provide compatibility with non-domain-joined devices.

Question: 259

What must be, at a minimum, the domain functional level of your Active Directory domains before you can install any Exchange Server 2010 servers?

- A. Windows 2000 mixed
- B. Windows 2000 native
- C. Windows 2000 interim
- D. Windows 2003 native

Answer: D

Explanation:

In each domain that will have Exchange recipients or Exchange Server roles installed, the domain functional level must be at the Windows 2003 Server native mode or higher.

Question: 260

What PowerShell cmdlet do you use to enable or disable a role assignment?

- A. Set-ManagementRoleAssignment
- B. Configure-ExchangeAdministrator
- C. Modify-ExchangeAdministrator
- D. Set-ExchangeAdministrator

Answer: A

Explanation:

To enable or disable a role assignment using the Exchange Management Shell, you would enter the following command: Set-ManagementRoleAssignment

Question: 261

By default, two SMTP receive connectors are configured on a newly installed Exchange Server 2010 Hub Transport server. Which one accepts inbound messages on TCP port 25?

- A. SMTP connector servername
- B. Default servername
- C. Client servername
- D. Receive connector servername

Answer: B

Explanation:

The Default servername SMTP receive connector accepts mail on TCP port 25, which is the default port for receiving messages from SMTP clients. The connector accepts mail on all installed network adapters in the Hub Transport server by default, and it also accepts the inbound messages from all IP addresses on the network by default, but only from Exchange servers. Additionally, this connector will not accept anonymous submissions.

Question: 262

To configure attachment filtering to block all PDF files, which of the following commands should you issue?

- A. Add-AttachmentFilterEntry -name *.pdf -type FileName
- B. Set-AttachmentFilterEntry -type *.pdf -type FileType
- C. Add-AttachmentFilterEntry -name *.pdf -type ContentType
- D. Set-AttachmentFilterEntry -name *.pdf -type FileName

Answer: A

Explanation:

To add an attachment filtering option that blocks all PDF files, you need to define a name of a wildcard with the PDF filename extension (*.pdf) using the -FileName option, such as Add-AttachmentFilterEntry -name *.pdf -type FileName.

Question: 263

Which of the following groups could be mail-enabled? (Choose two)

- A. A global distribution group
- B. A universal security group
- C. A local computer group
- D. A universal distribution group

Answer: B, D

Explanation:

Both security and distribution groups can be mail-enabled. However, only universal groups have their membership information published to the global catalog servers in the organization.

Question: 264

What PowerShell cmdlet do you use to enable POP3 access for a mailbox?

- A. Set-CASMailbox
- B. Set-MailboxProtocols
- C. Set-Mailbox
- D. Put-MailboxProtocols

Answer: A

Explanation:

To enable POP3 access for a mailbox, you need to use the Set-CASMailbox cmdlet, such as: Set-CASMailbox-Identity robert.jones@wiley.com -POPEnabled:\$true.

Question: 265

When configuring the OWA (Default Web Site) properties for segmentation, which of the following options are available? (Choose three)

- A. Calendar
- B. Contacts
- C. Public Folders
- D. Standard Client
- E. Change Password

Answer: A, B, E

Explanation:

Calendar, Contacts, and Change Password are among the options that you can disable or enable from the Segmentation tab of the OWA (Default Web Site) Properties dialog box.

Question: 266

What PowerShell cmdlet do you use to mail-enable an existing universal security group?

- A. MailEnable-SecurityGroup
- B. Enable-DistributionGroup
- C. Enable-SecurityGroup
- D. MailEnable-DistributionGroup

Answer: B

Explanation:

You use the Enable-DistributionGroup cmdlet to mail-enable any existing security group.

Question: 267

To perform message tracking from the Exchange Management Shell, what cmdlet must you use?

- A. Get-MessageTrackingLog
- B. View-MessageTrackingLog
- C. Track-Messages
- D. Get-MessageTracking

Answer: A

Explanation:

To perform message tracking from the Exchange Management Shell, you will need to use the Get-MessageTrackingLog cmdlet.

Question: 268

A project manager at your company missed a deadline on a high-profile project because they did not know one of the people on the project's distribution list was out of the office. You need to allow these notifications to be returned to the message sender on this distribution group. Which cmdlet should you run?

- A. Set-DistributionGroup ProjectX -ReportToOriginatorEnabled:\$true
- B. Set-DistributionGroup ProjectX -ReportToManagerEnabled:\$true
- C. Set-DistributionGroup ProjectX -SendOofMessageToOriginatorEnabled:\$true
- D. Set-DistributionGroup ProjectX -CreateDTMFMap:\$true

Answer: C

Explanation:

Enabling the SendOofMessageToOriginator parameter allows out-of-office messages to be returned to the originator of a message to the distribution group.

Question: 269

You are the Nutex Corporation's Exchange 2010 administrator. The Chief Information Officer (CIO) is apprehensive about applying upgrades and service packs until they are needed. What would be reasons to apply SP1 to the Exchange 2010 servers in the organization?

- A. To preserve mailbox items that may have been deleted or edited by users
- B. To use annotations to associate a case number or another unique identifier with a message
- C. To get an estimate of search results to determine the total number and size of items returned by a discovery search
- D. To enable search results of multiple mailbox servers to copy only one instance of a unique message to the discovery mailbox on a mailbox server running Exchange 2010 or Exchange 2010 SP1
- E. To enable discovery searches of items placed on hold

Answer: B, C

Explanation:

The following are reasons to upgrade to Exchange 2010 SP1:

You can use annotations to associate a case number or another unique identifier with a message.

You can get an estimate of search results to determine the total number and size of items returned by a discovery search.

Discovery managers can perform a discovery search across the cloud or on-premise servers. With Exchange 2010 SP1, a discovery manager could get an estimate of the size of the search results before running the search, and add annotations to messages. Annotations allow a discovery manager to add annotations to the message. For example, a discovery manager can associate a unique identifier with a message such as a case number. The discovery manager could then search for all items with that number.

Exchange 2010 SP1 does not enable search results of multiple mailbox servers to copy only one instance of a unique message to the discovery mailbox on a mailbox server running Exchange 2010. Exchange 2010 SP1 contains a feature called deduplication that only works on a discovery mailbox located on an Exchange 2010 SP1 Mailbox server. Deduplication copies only one instance of a unique message to a discovery mailbox, reducing the size of the discovery mailbox size.

Exchange 2010 already includes the litigation hold feature. Litigation hold preserves mailbox contents for discovery requests until a lawsuit has been concluded. A litigation hold will do the following:

- Keep user's mailbox items in an unaltered state
- Keeps mailbox items that may have been edited or deleted
- Keeps mailbox items automatically deleted by MRM

Question: 270

You are the Exchange administrator for the Nutex Corporation's Exchange organization. Nutex has single Active Directory domain named nutex.com. All Exchange server roles are running Exchange 2010 SP1. You have each server role on a separate subnet. The routers used to create the subnets have firewall capabilities. Which ports should be open on the firewall? (Choose two.)

- A. You should consider opening TCP port 25, TCP port 135, TCP port 389, TCP port 443, TCP port 993, and TCP ports 5060 to 5062 for the Hub Transport server to communicate with other Exchange server roles and other services.
- B. You should consider opening TCP port 53, TCP port 389, TCP port 443, TCP port 993, and TCP port 995 for the Client Access server to communicate with other Exchange server roles and other services.
- C. You should consider opening TCP port 135, TCP port 389, TCP port 443, and TCP port 3268 for the Mailbox server to communicate with other Exchange server roles and other services.
- D. You should consider opening TCP port 25, TCP port 88, TCP port 389, TCP port 443, TCP port 3268, and UDP ports 1024 to 65535 for the Unified Messaging server to communicate with other Exchange server roles and other services.

Answer: B, D

Explanation:

You should consider opening TCP port 25, TCP port 88, TCP port 389, TCP port 443, TCP port 3268, and UDP ports 1024 to 65535 for the Unified Messaging server to communicate with other Exchange server roles and other services. The Unified Messaging server needs to have TCP port 25 open for SMTP communication with the Transport server. TCP port 88 is used for Kerberos communication. TCP port 389 is used for LDAP communication with Active Directory. TCP port 443 is used for SSL communication used by the Unified Messaging Web service. UDP ports 1024 to 65535 are used for Unified Messaging Phone interaction.

You should consider opening TCP port 53, TCP port 389, TCP port 443, TCP port 993, and TCP port 995 for the Client Access server to communicate with other Exchange server roles and other services. TCP port 53 is used to

communicate with the DNS server. TCP port 389 is used for LDAP communication with Active Directory. TCP port 443 is used for SSL communication used by Exchange Web services. TCP port 995 is used for secure communication with POP3. TCP port 993 is used for secure communication with IMAP4.

You should not open TCP port 993 and TCP 5060 to 5062 for the Hub Transport server to communicate with other Exchange server roles. A Hub Transport server will use the following:

- TCP port 25 for SMTP communications.
- TCP port 135 to communicate with a Mailbox server via MAPI
- TCP port 389 to allow communications with Active Directory
- TCP port 443 for HTTPS communications with an Active Directory Rights Management Services server

TCP port 993 is used for secure IMAP4 communication. IMAP4 is used for communication with Client Access server. TCP 5060 to 5062 is used for communication from a Client Access server to a Unified Messaging server. You should not consider opening TCP port 443 for the Mailbox server to communicate with other

Exchange server roles and other services. TCP port 443 is not used by the Mailbox server. TCP port 3268 is used by the Mailbox server for LDAP access to a global catalog server.

Question: 271

You have successfully migrated from an on-premise Exchange 2010 organization to Exchange Online. All clients use Microsoft Office 365. You want to capture all edits made to user Michelle Smith's mailbox for 17 days. You want to have a rolling legal hold to preserve the data in the mailbox, with the data not affected by any of Michelle Smith's actions. What should you do?

A. Run the following cmdlet:

```
Set-Mailbox -identity "Michelle Smith" -SingleItemRecoveryEnabled $true
```

B. Contact the Office 365 help desk

C. Upgrade to an Exchange Online (Plan 2) subscription and contact the Office 365 help desk

D. Upgrade to an Exchange Archiving subscription and contact the Office 365 help desk

Answer: B

Explanation:

You should contact the Office 365 help desk to enable a Single Item Recovery (SIR) for 17 days. SIR is enabled by default on all mailboxes in Exchange Online with a 14-day retention period. To extend or decrease the SIR period, you must contact the Office 365 help desk.

You should not run Set-Mailbox -identity "Michelle Smith" -SingleItemRecoveryEnabled \$true. This action will enable SIR for an on-premise account. SIR is not enabled by default on an on-premise account. In this scenario, you have upgrade Exchange 2010 to Exchange online so all accounts are in the cloudbased service.

You do not need to upgrade to an Exchange Online (Plan 2) subscription and contact the Office 365 help desk.

A SIR can be placed on account with an Exchange Online (Plan 1) subscription if you want to have a rolling legal hold of 30 days or less.

You do not need to upgrade to an Exchange Archiving subscription and contact the Office 365 help desk. An Exchange Archiving subscription provides a personal e-mail archive for users who have mailboxes on Exchange Server 2010 and is not a requirement to have a SIR.

Case Study: 1

Contoso Ltd

Company Overview

Contoso, Ltd. is a wholesale travel agency.

Physical Locations

The company has offices in New York and Seattle. Each office has a call center. All IT staff and help desk

staff are located in the New York office.

Existing Environment

Contoso has a single domain named contoso.com. An Active Directory site exists for each office. The sites connect to each other by using a high-speed WAN link. The WAN link has an average utilization rate of 90 percent during business hours. The domain contains three domain controllers. The domain controllers are configured as shown in the following table.

Server name	Server role	Server site
DC1	Global catalog Schema master Domain naming master RID master	New York
DC2	Global catalog PDC emulator	New York
DC3	Infrastructure master	Seattle

The network has an Exchange Server 2010 Service Pack 1 (SP1) organization that contains four servers. The servers are configured as shown in the following table.

Server name	Server role	Server site	Mailbox database name
EX1	Mailbox Client Access Hub Transport	New York	DB1
EX2	Mailbox Client Access Hub Transport	New York	DB2
EX3	Mailbox Client Access Hub Transport	Seattle	DB3
EX4	Mailbox Client Access Hub Transport	Seattle	DB4

Each mailbox database is 400 GB.

All of the servers have the following hardware configurations:

- 64 GB of RAM
- One dual quad-core Intel Xeon processor
- Two 1-gigabit per second Ethernet network adapters
- One RAID 10 disk array that has 12 300-GB, 15,000-RPM SAS disks for data
- one RAID 1 disk array that has two 73-GB, 10,000-RPM SAS disks for program files
- One RAID 1 disk array that has two 73-GB, 10,000-RPM SAS disks for the operating system

Requirements

Business Goals

Contoso has the following general requirements that must be considered for all technology deployments:

- Minimize costs whenever possible.
- Minimize administrative effort whenever possible.
- Minimize traffic on the WAN link between the offices.

Planned Changes

Contoso acquires a company named Margie's Travel. Margie's Travel has 3,000 employees.

Margie's Travel has the following email infrastructure:

- A call center, where 200 employees work
- UNIX-based email hosts that users access by using POP3 and SMTP
- Three departments that use the SMTP domains of margiestravel.com, east.margiestravel.com, and

blueyonderairlinesexam. Users are assigned only one email address that uses the SMTP domain of their department

You plan to deploy a new Exchange Server 2010 SP1 organization to Margie's Travel. The new email infrastructure must meet the following implementation requirements:

- All employees must have access to their mailbox if a single server fails.
- Call center employees must use windows Internet Explorer 8 to access their mailbox.
- The administration of the Margie's Travel Exchange organization must be performed by a dedicated team.
- Call center employees must be prevented from accessing the calendar or journal features of Outlook Web App.
- All employees who do not work in the call center must have access to all of the Outlook web App features.
- All email messages sent to recipients outside of Margie's Travel must have a return address in the user@margiestravel.com format.

The new email infrastructure for Margie's Travel must meet the following security requirements:

- Contoso administrators must be prevented from viewing or modifying the settings of the mailboxes of Margie's Travel users.
- All inbound and outbound Internet email to and from the Margie's Travel domains must be routed through the Hub Transport servers of Contoso.
- All email messages that contain confidential customer information must be encrypted automatically while in transit and the recipients of the messages must be prevented from forwarding them to other users.

Compliance Requirements

Contoso must meet the following compliance requirements:

- Each email message sent by an attorney from the Contoso legal department must be approved by the manager of the legal department.
- Attorneys must be able to classify email messages as "attorney-client privileged".
- All messages classified as "attorney-client privileged" must contain a legal disclaimer automatically.

User Requirements

All users who have a portable computer use Microsoft Outlook 2010 when they work online and offline. When the users work offline, they must be able to read existing email messages and create new email messages. Users who have a large mailbox must minimize the amount of hard disk space used by the mailbox on their portable computer.

Question: 1

You are designing the Exchange organization for Margies Travel. You need to ensure that all of the emails sent to the Internet by the Margie's Travel users have return email addresses in the required format. What should you include in the design?

- A. a Hub Transport server and address rewrite entries
- B. an Edge Transport server and address rewrite entries
- C. an Edge Transport server and Edge Transport rules
- D. a Hub Transport server and Hub Transport rules

Answer: B

Explanation:

The question states What should you include in the design Hub Transport cannot be used for address rewrites. see below and transport rules on either the Hub Transport or the Edge Transport will not work You use address rewriting to present a consistent appearance to external recipients of messages from your Exchange 2010 organization. Address rewriting can be valuable to organizations that use third-party vendors to provide e-mail support and services. Customers and partners expect e-mail messages to come from the organization, not a third-party vendor. Similarly,

after a merger or acquisition, an organization might want all email messages to appear to come from the single new organization. The address rewriting feature frees organizations to structure their businesses by business requirements instead of by technical requirements or limitations.

You can also use address rewriting to enable appropriate routing of inbound messages from outside your Exchange 2010 organization to internal recipients. Address rewriting enables replies to messages that were rewritten to be correctly routed to the original sender of the rewritten message.

You configure Address Rewriting agents on the Receive connector and Send connector on a computer that has the Edge Transport server role installed.

<http://technet.microsoft.com/en-us/library/aa996806.aspx>

Question: 2

You need to recommend changes to the Active Directory infrastructure of Contoso. The changes must ensure that users in all of the offices can access their local mailbox if a WAN link fails. What should you recommend?

- A. Deploy a read-only global catalog server to the Seattle site.
- B. Deploy a read-only global catalog server to the New York site.
- C. Enable universal group membership caching in the Seattle site.
- D. Disable the global catalog on DC2.
- E. Enable the global catalog on DC3.
- F. Enable universal group membership caching in the New York site.

Answer: E

Question: 3

You need to recommend changes to the Exchange organization of Contoso. The changes must ensure that users can connect to their mailbox if a single Exchange server fails. The solution must meet the business requirements of Contoso. What should you recommend? (Choose all that apply.)

- A. Deploy a new hardware load balancer to each site and create a Client Access array in each site.
- B. Deploy an alternate file share witness to each Mailbox server and enable Datacenter Activation Coordination (DAC) mode.
- C. Create a database availability group (DAG) that contains all of the Mailbox servers. Create four database copies of each mailbox database.
- D. Create a Network Load Balancing cluster in each site. Create a Client Access array in each site.
- E. Create a database availability group (DAG) for each site. Add the Mailbox servers of each site to the respective DAG. Create two database copies of each mailbox database.

Answer: A, E

Explanation:

All employees must have access to their mailbox if a single server fails.

Question: 4

You need to recommend changes to the Exchange organization of Contoso. The solution must meet the compliance requirements and the business goals of Contoso. What should you include in the recommendation? (Choose all that apply.)

- A. journal rules
- B. message classification templates
- C. Hub Transport rules
- D. Edge Transport rules
- E. Secure MIME
- F. moderated recipients

Answer: B, C, F

Explanation:

Message classifications are a Microsoft Exchange Server 2010 and Microsoft Office Outlook 2007 feature intended to help organizations comply with their e-mail policies and regulatory responsibilities. When a message is classified, the message contains specific metadata that describes the intended use or audience of the message. Outlook 2007 or Microsoft Office Outlook Web App may act on this metadata by displaying a user-friendly description of the classification to senders and receivers of a classified message. In Exchange 2010, the Microsoft Exchange Transport service may act on the metadata if there's a transport rule that meets specific criteria that you have configured.

The following list provides a brief description of some of the message classification fields that you can set:

Display name:

This property specifies the display name for the message classification instance. The display name appears in the Permission menu in Outlook 2007 and Outlook Web App and is used by Outlook and Outlook Web App users to select the appropriate message classification before a message is sent. The display name is also displayed in the recipient description that appears in the InfoBar in an Outlook message. The parameter name for this property is DisplayName.

Sender description:

This property explains to the sender what the message classification is intended to achieve. The text that you enter for this field is used by Outlook and Outlook Web App users to select the appropriate message classification before a message is sent. The parameter name for this property is SenderDescription.

Recipient description:

This property explains to the recipient what the message classification was intended to achieve. The text that you enter for this field is viewed by Outlook and Outlook Web App users when they receive a message that has this message classification. The parameter name for this property is RecipientDescription.

Locale:

This field specifies a culture code to create a locale-specific version of the message classification. For more information about the locale field, see "Localizing Message Classification Instances for Different Languages and Locales" later in this topic. The parameter name for this property is Locale.

After Outlook 2007 is enabled to accept the default message classifications, users can apply message classification to messages that they send. Senders see the sender description in the InfoBar in Outlook 2007.

By using the Exchange Management Shell, you can customize the sender description for each message classification and locale.

Note:

Outlook Web App requires no special configuration to display or use message classifications.

Three message classifications are enabled in Exchange 2010 by default:

Attachment Removed This classification notifies recipients when attachments have been removed from the message.

Originator Requested Alternate Recipient Mail This classification notifies recipients that the message has been redirected from delivery to the original addressed recipient.

Partner Mail This classification notifies recipients that the message was encrypted and delivered through a secure connector.

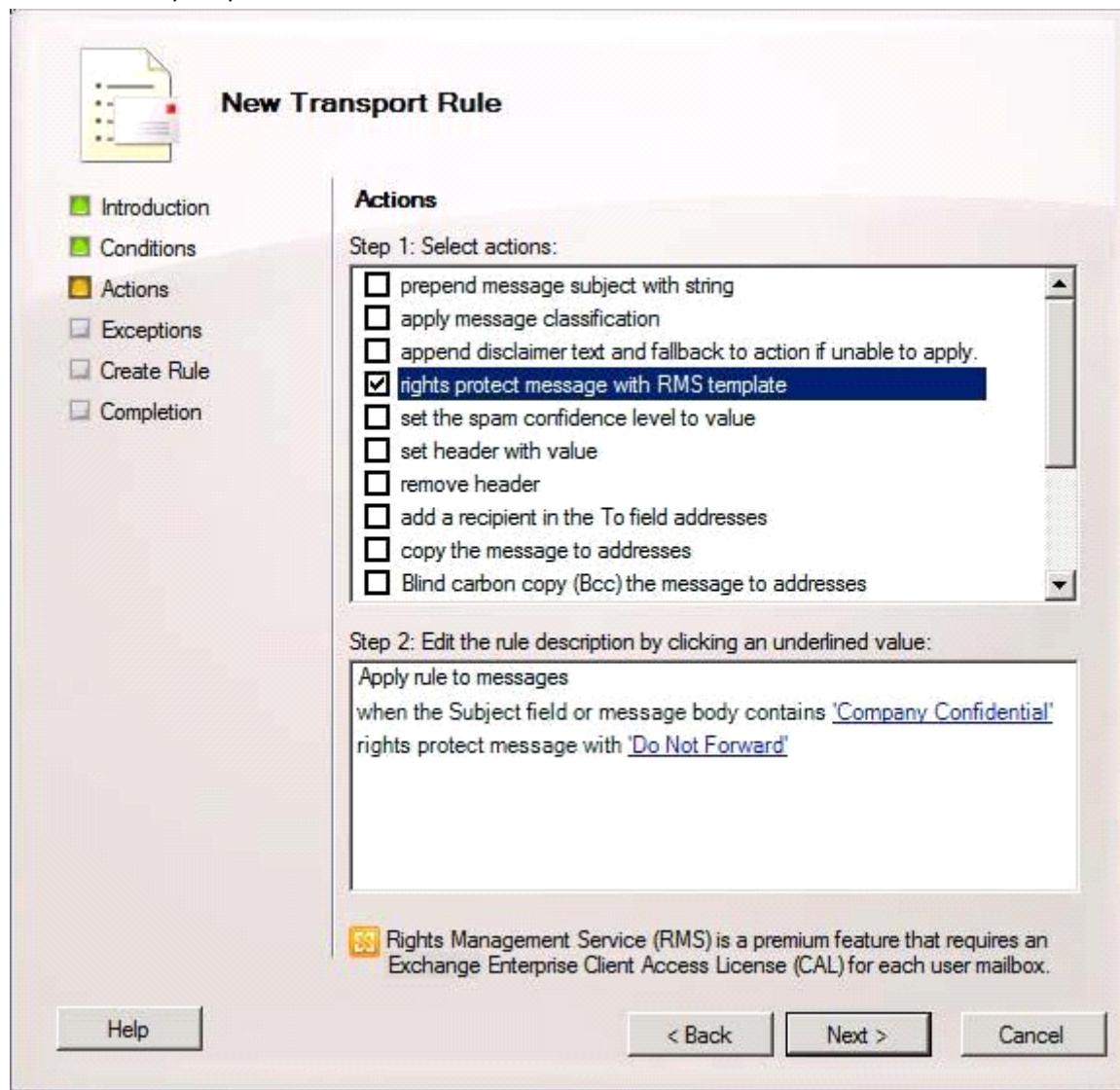
When you configure a recipient for moderation, all messages sent to that recipient are subject to approval by the designated moderators. For more information about how Exchange 2010 handles recipient moderation, see Understanding Moderated Transport.

Automatic Protection Using Transport Protection Rules

Messages containing business critical information or PII can be identified by using a combination of transport rule

conditions, including regular expressions to identify text patterns such as social security numbers. Organizations require different levels of protection for sensitive information. Some information may be restricted to employees, contractors, or partners; while other information may be restricted only to full-time employees. The desired level of protection can be applied to messages by applying an appropriate rights policy template. For example, users may mark messages or e-mail attachments as Company Confidential. As illustrated in the following figure, you can create a transport protection rule to inspect message content for the words "Company Confidential", and automatically IRM-protect the message.

Create a transport protection rule



For more information about creating transport rules to enforce rights protection, see Create a Transport Protection Rule.

Question: 5

You need to recommend changes to the mailboxes to meet the user requirements for the portable computers. What should you include in the recommendation?

- A. message classifications
- B. message size limits
- C. Personal Archives
- D. disabled Cached Exchange Mode

E. folder redirection

Answer: C

Question: 6

You need to recommend a Client Access solution for Margie's Travel. The solution must meet the business goals of Contoso. The solution must also meet the implementation requirements of Margie's Travel. What should you recommend?

- A. One Client Access server and one Outlook Web App policy
- B. Two Client Access servers and one Outlook Web App policy
- C. Two Client Access servers and two Outlook Web App policies
- D. One Client Access server and two Outlook Web App policies

Answer: C

Explanation:

You plan to deploy a new Exchange Server 2010 SP1 organization to Margie's Travel. The new email infrastructure must meet the following implementation requirements:

- All employees must have access to their mailbox if a single server fails.
- Call center employees must use windows Internet Explorer 8 to access their mailbox.
- The administration of the Margie's Travel Exchange organization must be performed by a dedicated team.
- Call center employees must be prevented from accessing the calendar or journal features of Outlook Web App.
- All employees who do not work in the call center must have access to all of the Outlook web App features.
- All email messages sent to recipients outside of Margie's Travel must have a return address in the user@margiestravel.com format.

Question: 7

You need to recommend changes to the Exchange organization of Contoso. The changes must support the SMTP domains of Margie's Travel. The solution must meet the security requirements of Margie's Travel. What should you recommend?

- A. Create an accepted domain for each Margie's Travel domain and configure the new domains as authoritative domains.
- B. Create an accepted domain for each Margie's Travel domain and configure the new domains as external relay domains.
- C. Create an accepted domain for each Margie's Travel domain and configure the new domains as internal relay domains.
- D. Create a remote domain named margiestravel.com and configure support for all child domains.

Answer: C

Explanation:

All inbound and outbound Internet email to and from the Margie's Travel domains must be routed through the Hub Transport servers of Contoso.

Question: 8

You need to recommend changes to the Exchange organization of Litware. The solution must meet the compliance requirements and the business goals of Litware. What should you include in the recommendation?

- A. Edge Transport rules, Secure MIME, and moderated recipients
- B. journal rules, message classification templates, and moderated recipients
- C. journal rules, Secure MIME, and moderated recipients
- D. Hub Transport rules, message classification templates, and moderated recipients

Answer: D

Question: 9

You need to recommend changes to the Active Directory infrastructure of Litware. The changes must ensure that users in all of the offices can access their local mailbox if a WAN link fails. What should you recommend?

- A. Enable the global catalog on Server3.
- B. Deploy a read-only global catalog server to the Tokyo site.
- C. Disable the global catalog on Server2.
- D. Enable universal group membership caching in the Bangkok site.
- E. Deploy a read-only global catalog server to the Bangkok site.
- F. Enable universal group membership caching in the Tokyo site.

Answer: A

Question: 10

You are designing the Exchange Server 2010 SP1 organization for A . Datum. You need to ensure that all of the email sent to the Internet by the A. Datum users has a return email address in the required format. What should you include in the design?

- A. an Edge Transport server, three Edge Transport rules, and an email address policy
- B. an Edge Transport server and address rewrite entries
- C. a Hub Transport server, three Hub Transport rules, and an email address policy
- D. a Hub Transport server and address rewrite entries

Answer: B

Question: 11

You need to recommend a solution to minimize the number of remote SMTP hosts that identify email messages sent by A . Datum users as spam. What should you include in the recommendation?

- A. a service location (SRV) record in the public DNS zone of the liware.com domain
- B. a sender policy framework (SPF) record in the internal DNS zone of the litwareinc.com domain
- C. a sender policy framework (SPF) record in the public DNS zone of the litwareinc.com domain
- D. a sender policy framework (SPF) record in the public DNS zone of the adatum.com domain
- E. a sender policy framework (SPF) record in the internal DNS zone of the adatum.com domain
- F. a service location (SRV) record in the public DNS zone of the adatum.com domain

Answer: D

Question: 12

You need to recommend changes to the mailboxes to meet the user requirements of the portable computers. What should you include in the recommendation?

- A. disabled Cached Exchange Mode
- B. disabled Outlook Anywhere
- C. Personal Archives
- D. deleted Mailbox retention
- E. message size limits

Answer: C

Question: 13

You need to recommend changes to the Exchange organization of Litware. The changes must support the SMTP domains of A . Datum. The solution must meet the security requirements of A. Datum. What should you recommend?

- A. Create an accepted domain for each A. Datum SMTP domain and configure the new domains as external relay domains.
- B. Create an accepted domain for each A. Datum SMTP domain and configure the new domains as internal relay domains.
- C. Create a remote domain for each A. Datum SMTP domain.
- D. Create an accepted domain for each A. Datum SMTP domain and configure the new domains as authoritative domains.

Answer: B

Question: 14

You need to recommend changes to the network infrastructure to support the planned changes for Margie's Travel.What should you recommend creating?

- A. A new Active Directory forest named margiestravel.com
- B. A new domain named margiestravel.contoso.com in the contoso.com forest
- C. Three organization units (OUs) named margiestravel.com, east.margiestravel.com, and blueyonderairlines.com
- D. A new domain named margiestravel.com in the contoso.com forest

Answer: A

Case Study: 2

Fabrikam Inc

Company Overview

Fabrikam Inc. is a leading manufacturer of children's toys.

Physical Locations

Fabrikam has a main office in Seattle and a manufacturing plant in Los Angeles. The offices connect to each

other by using a heavily congested high-speed WAN link. Each office has a dedicated connection to the Internet.

Research and development personnel are located in both the Seattle office and the Los Angeles office.

Existing Environment

Active Directory Environment

Fabrikam has an Active Directory forest that contains one domain name fabrikam.com. The Active Directory forest has the following configurations:

- An Active Directory site exists for each office.
- All domain controllers run Windows Server 2003 x86 Service Pack 2 (SP2).
- The functional level of the forest and the domain is Windows Server 2003 interim.
- All of the user accounts for the users in the Seattle office are located in an organizational unit (OU) named Users\Seattle.
- All of the user accounts for the users in the Los Angeles offices are located in an organizational unit (OU) named Users\Los Angeles.
- Both offices have a help desk staff. The help desk staff in each office is responsible for managing all of the users in its respective office.

Messaging Environment

Fabrikam has an Exchange Server 2003 Service Pack 2 (SP2) organization that has the following configurations:

- A 500-MB mailbox quota for all users
- An SMTP connector that has the following configurations:
 - Address space: *
 - Delivery: DNS
 - Local bridgehead: SEA-BE-1

Fabrikam has a partner company named Tailspin Toys; The Fabrikam Exchange servers are configured as ETRN servers for tailspintoys.com. The Exchange organization contains four servers. The servers are configured as shown in the following table.

Server name	Server role	Server routing group	Server site
SEA-BE-1	Back-end	RG1	Seattle
SEA-FE-1	Front-end	RG1	Seattle
LA-BE-1	Back-end	RG1	Los Angeles
LA-FE-1	Front-end	RG1	Los Angeles

Requirements

Business Goals

Fabrikam has the following business goals:

- Minimize hardware costs.
- Minimize administrative

Minimize WAN link utilization between the two offices.

Planned Changes

Fabrikam plans to migrate to Exchange Server 2010 Service Pack 1 (SP1).

You plan to deploy a Hub Transport server named SEA-HUB-1 in the Seattle site.

You plan to deploy a Hub Transport server named LA-HUB-1 in the Los Angeles site.

Archiving Requirements

Email messages that are older than 180 days must be moved automatically to a distinct mailbox database.

Security Requirements

Fabrikam must meet the following security requirements:

- Anti-spam filtering must be performed on all email messages before the messages enter the network.
- The help desk staff must be prevented from modifying user accounts for users located in remote offices.

- The number of permissions assigned to the members of a group named Exchange Server Troubleshooters must be minimized.

Security Requirements

Fabrikam must meet the following security requirements:

- Anti-spam filtering must be performed on all email messages before the messages enter the network.
- The help desk staff must be prevented from modifying user accounts for users located in remote offices.
- The number of permissions assigned to the members of a group named Exchange Server Troubleshooters must be minimized.

Redundancy Requirements

Fabrikam must meet the following redundancy requirements:

- A copy of all the mailbox databases must exist in both sites.
- The impact on users must be minimized if a single server fails.
- Users must be able to send and receive messages if a single server fails.
- All of the mailbox databases must be available if the WAN link fails between the offices.

Problem Statements

The WAN link between the Seattle office and the Los Angeles office is heavily congested. During normal business hours, the average round-trip time for packets to travel across the WAN link is 200 ms. The portable computer of the manager of the accounting department recently experienced a hard disk failure. The hard disk failure resulted in the loss of more than two years of email and other personal data.

Question: 1

You plan to deploy Microsoft Forefront Online Protection for Exchange (FOPE). You need to recommend changes to the environment to ensure that inbound email messages from the Internet are scanned by FOPE. What should you include in the recommendation?

- A. Modify the sender policy framework (SPF) record of Fabrikam to point to FOPE.
- B. Implement Microsoft Forefront Threat Management Gateway (TMG), and then create a federation trust.
- C. Modify the mail exchange (MX) records of Fabrikam to point to FOPE.
- D. Implement Forefront Protection 2010 for Exchange Server, and then create a sharing policy.

Answer: C

Question: 2

You are evaluating the implementation of database availability groups (DAGs). You need to recommend a DAG implementation that meets the redundancy requirements of Fabrikam. What should you recommend?

- A. Add one Mailbox server to each site. Create two DAGs. Add one Mailbox server to each DAG.
- B. Add one Mailbox server to each site. Create one DAG that contains both Mailbox servers.
- C. Add two Mailbox servers to each site. Create one DAG for each site. Add the Mailbox servers for each site to their respective DAG.
- D. Add two Mailbox servers to each site. Create two DAGs. Add one Mailbox server from each site to each DAG.

Answer: D

Question: 3

The members of the Exchange Servers Troubleshooters group plan to run the Test-MailFlow cmdlet regularly. You

need to identify which Role Based Access Control (RBAC) management role must be assigned to the Exchange Server Troubleshooters group. The solution must meet the security requirements of Fabrikam. Which role should you identify?

- A. Organization Management
- B. Help Desk
- C. Server Management
- D. View-Only Organization Management
- E. Recipient Management

Answer: D

Question: 4

You need to recommend a message routing design for the period during which Fabrikam transitions from Exchange Server 2003 to Exchange Server 2010 SP1. The solution must meet the business goals of Fabrikam. What should you include in the recommendation? (Choose all that apply.)

- A. a scoped Send connector that uses SEA-HUB-1 as the source server
- B. a scoped Send connector that uses LA-BE-1 as the source server
- C. a linked connector for each Send connector
- D. a scoped Send connector that uses LA-HUB-1 as the source server
- E. a scoped Send connector that uses SEA-BE-1 as the source server
- F. an Exchange hub site for each site

Answer: A, D

Question: 5

You need to recommend changes to the existing Active Directory infrastructure to support the planned Exchange Server 2010 SP1 deployment. The solution must meet the business goals of Fabrikam. What should you include in the recommendation? (Choose all that apply.)

- A. Upgrade one global catalog server in each site to Windows Server 2008 R2.
- B. Raise the functional level of the forest.
- C. Raise the functional level of the domain.
- D. Upgrade all of the global catalog servers to Windows Server 2008 R2.
- E. Upgrade all of the domain controllers to Windows Server 2008 R2.

Answer: B, C

Question: 6

You need to recommend a solution that meets the archiving requirements of Fabrikam. What should you include in the recommendation?

- A. recovery databases and Personal Archives
- B. single item recovery and retention policies
- C. single item recovery and litigation holds

- D. Personal Archives and litigation holds
- E. Personal Archives and retention policies

Answer: E

Question: 7

You need to recommend a routing group configuration that meets the business requirements of Fabrikam. What should you include in the recommendation?

- A. One routing group for each office that contains all of the Exchange servers in that office
- B. One routing group that contains all of the Exchange Server 2003 servers and all of the Exchange Server 2010 SP1 servers
- C. One routing group for each office that contains only the Exchange Server 2003 servers in that office and one routing group that contains all of the Exchange Server 2010 SP1 servers
- D. One routing group for each office that contains only the Exchange Server 2003 servers in that office and one routing group for each office that contains only the Exchange Server 2010 SP1 servers in that office

Answer: C

Question: 8

You are evaluating the implementation of SEA-HUB1 and LA-HUB1. You need to recommend a Hub Transport server topology that meets the redundancy requirements of Fabrikam. The solution must also support the business goals of Fabrikam. What should you include in the recommendation?

- A. Deploy SEA-HUB1 and an additional Hub Transport server named SEA-HUB2 to the Seattle site. Deploy LA-HUB1 and an additional Hub Transport server named LA-HUB2 to the Los Angeles site. Deploy a hardware load balancer to each site. Configure the virtual IP address of the load balancer to point to the Hub Transport servers.
- B. Deploy SEA-HUB1 to the Seattle site. Deploy LA-HUB1 to the Los Angeles site. Create one Send connector in each site.
- C. Deploy SEA-HUB1 to the Seattle site. Deploy LA-HUB1 to the Los Angeles site. Deploy a hardware load balancer to each site. Configure the virtual IP address of the load balancer to point to the Hub Transport servers.
- D. Deploy SEA-HUB1 and an additional Hub Transport server named SEA-HUB2 to the Seattle site. Deploy LA-HUB1 and an additional Hub Transport server named LA-HUB2 to the Los Angeles site. Create one Send connector in each site.

Answer: D

Question: 9

You need to recommend a Client Access server design that meets the redundancy requirements of Fabrikam. What should you include in the recommendation?

- A. Two Client Access arrays
Four Client Access servers
DNS round robin
- B. Two Client Access arrays
Four Client Access servers

- Two hardware load balancers
- C. Four Client Access servers
- One hardware load balancer
- DNS round robin
- D. One Client Access array
- Two Client Access servers
- One hardware load balancer

Answer: B

Question: 10

You are evaluating the implementation of Exchange Server 2010 SP1 Edge Transport servers and Hub Transport servers. You need to recommend a solution to ensure that the Exchange Server 2010 SP1 servers can queue email messages for tailspintoys.com. What should you include in the recommendation?

- A. an external relay domain
- B. an authoritative domain
- C. a remote domain
- D. an email address policy

Answer: A

Question: 11

You need to recommend an administrative solution for the help desk staff. The solution must meet the security requirements of Fabrikam. What should you include in the recommendation?

- A. a split permissions model
- B. built-in security groups
- C. direct role assignments
- D. management role groups

Answer: D

Case Study: 3

Litware, Inc

Company Overview

Litware, Inc. is a manufacturing company.

Physical Locations

The company has offices in Bangkok and Tokyo. Each office has a sales department. All network support staff is located in the Bangkok office.

Existing Environment

Litware has a forest that contains a single domain named litwareinc.com. An Active Directory site exists for each office. The sites connect to each other by using a high-speed WAN link. The WAN link has an average net available bandwidth of 15 percent during business hours. The domain contains three domain controllers. The domain controllers are configured as shown in the following table.

Server name	Server role	Server site
Server1	Global catalog Schema master Domain naming master RID master	Bangkok
Server2	Global catalog PDC emulator	Bangkok
Server3	Infrastructure master	Tokyo

The network has an Exchange Server 2010 Service Pack 1 (SP1) organization that contains four servers. The servers are configured as shown in the following table.

Server name	Server role	Server site	Mailbox database name	Mailbox database size
BANEXC01	Mailbox, Client Access, Hub Transport	Bangkok	MBX1	400 GB
BANEXC02	Mailbox, Client Access, Hub Transport	Bangkok	MBX2	400 GB
TOKEXC01	Mailbox, Client Access, Hub Transport	Tokyo	MBX3	400 GB
TOKEXC02	Mailbox, Client Access, Hub Transport	Tokyo	MBX4	400 GB

All of the servers have the following hardware configurations:

- 32 GB of RAM
- Two dual quad-core Intel Xeon processors
- Two 1-gigabit per second network adapters
- One RAID 10 disk array that has 12 300-GB, 1S,000-RPM SAS disks for data
- One RAID 1 disk array that has two 73-GB, 10,000-RPM SAS disks for program files
- One RAID 1 disk array that has two 73-GB, 10,000-RPM SAS disks for the operating system

Requirements

Business Goals

Litware has the following general requirements that must be considered for all technology deployments:

- Minimize costs whenever possible.
- Minimize administrative effort whenever possible.
- Minimize traffic on the WAN link between the Bangkok and Tokyo offices.

Planned Changes

Litware acquires a management company named A. Datum Corporation. A. Datum has 2,500 employees.

A. Datum has the following email infrastructure:

- A sales department, in which 150 employees work
 - A third-party email infrastructure that is used for IMAP4 and SMTP
 - Three other departments that use the SMTP domains ofadatum.com, asia.adatum.com, and contoso.com.
- Users are assigned only one email address that uses the SMTP domain of their department

You plan to deploy a new Exchange Server 2010 SP1 organization for A. Datum. The new email infrastructure must meet the following implementation requirements:

- All employees must have access to their mailbox if a single server fails.
- Sales department employees must use Windows Internet Explorer 8 to access their mailbox,
- Sales department employees must be prevented from accessing the calendar or journal features of Outlook Web App.
- All employees who do not work in the sales department must have access to all of the Outlook Web App features.
- All email messages sent to recipients outside of A. Datum must have a return address in the user@adatum.com format.
- The administration of the A. Datum Exchange organization must be performed by a dedicated team of administrators.
- The Exchange administration team for A. Datum must be distinct from the Exchange administration team of Litware.

The new email infrastructure for A. Datum must meet the following security requirements:

- Litware administrators must be prevented from viewing or modifying the settings of the mailboxes of A. Datum users.
- All inbound and outbound Internet email to and from the A. Datum domains must be routed through the Hub Transport servers of Litware.
- All email messages that contain financial information must be encrypted automatically while in transit and the recipients of the messages must be prevented from forwarding them to users outside of the company's financial department.

Compliance Requirements

Litware must meet the following compliance requirements:

- Each email message sent by an attorney from the Litware legal department must be approved by the manager of the legal department.
- Attorneys must be able to classify email messages as "attorney-client privileged".
- All email messages classified as "attorney-client privileged" must contain a legal disclaimer automatically.

User Requirements

All users who have a portable computer use Microsoft Outlook 2010 when they work online and offline. When the users work offline, they must be able to read existing email messages and create new email messages.

Users who have a large mailbox must minimize the amount of hard disk space used by the mailbox on their portable computer.

Question: 1

You need to recommend changes to the network infrastructure to meet the security requirements of A. Datum. What should you recommend creating?

- A. A new domain named adatum.com in the litwareinc.com forest
- B. A new Active Directory forest named adatum.com
- C. A new domain named adatum.litwareinc.com in the litwareinc.com forest
- D. Three organization units (OUs) named adatum.com, asia.adatum.com, and contoso.com

Answer: B

Question: 2

You need to recommend changes to the Exchange organization of Litware. The changes must support the SMTP domains of A . Datum. The solution must meet the security requirements of A . Datum. What should you recommend?

- A. Create an accepted domain for each A. Datum SMTP domain and configure the new domains as internal relay domains.
- B. Create an accepted domain for each A. Datum SMTP domain and configure the new domains as external relay domains.
- C. Create a remote domain for each A. Datum SMTP domain.
- D. Create an accepted domain for each A. Datum SMTP domain and configure the new domains as authoritative domains.

Answer: A

Question: 3

You need to recommend a Hub Transport server solution that meets the security requirements of A . Datum. The solution must meet the business goals of Litware. What should you include in the recommendation? (Choose all that apply.)

- A. NTFS permissions
- B. Secure MIME
- C. Hub Transport rules
- D. Authorization Manager
- E. Active Directory Rights Management Services (AD RMS)

Answer: C, E

Question: 4

You need to recommend a Client Access solution for A . Datum. The solution must meet the business goals of Litware. The solution must also meet the implementation requirements of A . Datum. What should you recommend?

- A. Two Client Access servers and two Outlook Web App policies
- B. Two Client Access servers and one Outlook Web App policy
- C. One Client Access server and one Outlook Web App policy
- D. One Client Access server and two Outlook Web App policies

Answer: A

Question: 5

You need to recommend changes to the Active Directory infrastructure of Litware. The changes must ensure that users in all of the offices can access their local mailbox if a WAN link fails. What should you recommend?

- A. Enable universal group membership caching in the Tokyo site.
- B. Deploy a read-only global catalog server to the Bangkok site.
- C. Enable the global catalog on Server3.
- D. Disable the global catalog on Server2.
- E. Enable universal group membership caching in the Bangkok site.

F. Deploy a read-only global catalog server to the Tokyo site.

Answer: C

Question: 6

You are designing the Exchange Server 2010 SP1 organization for A . Datum. You need to ensure that all of the email sent to the Internet by the A . Datum users has a return email address in the required format. What should you include in the design?

- A. an Edge Transport server, three Edge Transport rules, and an email address policy.
- B. an Edge Transport server and address rewrite entries.
- C. a Hub Transport server and address rewrite entries.
- D. a Hub Transport server, three Hub Transport rules, and an email address policy.

Answer: B

Question: 7

You need to recommend a solution to minimize the number of remote SMTP hosts that identify email messages sent by A . Datum users as spam. What should you include in the recommendation?

- A. a service location (SRV) record in the public DNS zone of the liware.com domain
- B. a sender policy framework (SPF) record in the internal DNS zone of the litwareinc.com domain
- C. a sender policy framework (SPF) record in the public DNS zone of the adatum.com domain
- D. a sender policy framework (SPF) record in the internal DNS zone of the adatum.com domain
- E. a sender policy framework (SPF) record in the public DNS zone of the litwareinc.com domain
- F. a service location (SRV) record in the public DNS zone of the adatum.com domain

Answer: C

Question: 8

You need to recommend changes to the mailboxes to meet the user requirements of the portable computers. What should you include in the recommendation?

- A. disabled Cached Exchange Mode
- B. disabled Outlook Anywhere
- C. Personal Archives
- D. deleted Mailbox retention
- E. message size limits

Answer: C

Question: 9

All users who have a portable computer use Microsoft Outlook 2010 when they work online and offline. When the users work offline, they must be able to read existing email messages and create new email messages. Users who have a large mailbox must minimize the amount of hard disk space used by the mailbox on their portable computer

- A. Edge Transport rules, Secure MIME, and moderated recipients
- B. journal rules, message classification templates, and moderated recipients
- C. journal rules, Secure MIME, and moderated recipients
- D. Hub Transport rules, message classification templates, and moderated recipients

Answer: D

Case Study: 4

A. Datum Corporation

Company Overview

A. Datum Corporation is a leading insurance company.

Physical Locations

A. Datum has a main office in Tokyo and a manufacturing plant in Bangkok. The offices connect to each other by using a heavily congested high-speed WAN link. Each office has a dedicated connection to the Internet. Research and development personnel are located in both the Tokyo office and the Bangkok office.
Existing Environment.

Active Directory Environment

A. Datum has an Active Directory forest that contains one domain named adatum.com. The Active Directory forest has the following configurations:

- An Active Directory site exists for each office.
- All domain controllers run Windows Server 2003 x86 Service Pack 2 (SP2).
- The functional level of the forest and the domain is Windows Server 2003 interim.
- All of the user accounts for the users in the Tokyo office are located in an organizational unit (OU) named Users\Tokyo.
- All of the user accounts for the users in the Bangkok office are located in an organizational unit (OU) named Users\Bangkok.
- Each office has a human resources team. The human resources team in each office is responsible for managing all of the users in its respective office.

Messaging Environment

A. Datum has an Exchange Server 2003 Service Pack 2 (SP2) organization that has the following configurations:

- A 375-MB mailbox quota for all users
- An SMTP connector that has the following configurations:
 - Address space: *
 - Delivery: DNS
 - Local bridgehead: TOK-BE-1

A. Datum has a partner company named Humongous Insurance. The A. Datum Exchange servers are configured as ETRN servers for humongousinsurance.com.

The Exchange organization contains six servers. The servers are configured as shown in the following table.

Server name	Server role	Server routing group	Server site
TOK -BE-1	Back-end	ASIA	Tokyo
TOK -FE-1	Front-end	ASIA	Tokyo
TOK-FE-2	Front-end	ASIA	Tokyo
BAN -BE-1	Back-end	ASIA	Bangkok
BAN -FE-1	Front-end	ASIA	Bangkok
BAN-FE2	Front-end	ASIA	Bangkok

Requirements

Business Goals

A. Datum has the following business goals:

- Minimize hardware costs.
- Minimize administrative effort.
- Minimize WAN

Planned Changes

A. Datum plans to migrate to Exchange Server 2010 Service Pack 1 (SP1). Each office will contain Exchange servers.

You plan to deploy a Hub Transport server named TOK-HUB-1 in the Tokyo site.

You plan to deploy a Hub Transport server named BAN-HUB-1 in the Bangkok site.

Archiving Requirements

Email messages that are older than 200 days must be moved automatically to a distinct mailbox database.

Security Requirements

A. Datum must meet the following security requirements:

- Anti-spam filtering must be performed on all email messages before the messages enter the network.
- The human resources teams must be allowed to modify only the user accounts of the users in their respective office.
- The number of permissions assigned to the members of a group named Exchange Secondary Support Staff must be minimized.

Redundancy Requirements

A. Datum must meet the following redundancy requirements:

- A copy of all the mailbox databases must exist in both sites.
- The impact on users must be minimized if a single server fails.
- Users must be able to send and receive email messages if a single server fails.
- All of the mailbox

Problem Statements

The WAN link between the Tokyo office and the Bangkok office is heavily congested. During normal business hours, the average round-trip time for packets to travel across the WAN link is 185 ms.

The portable computer of the manager of the finance department recently experienced a hard disk failure. The hard disk failure resulted in the loss of more than three years of email.

Question: 1

You are evaluating the implementation of Exchange Server 2010 SP1 Edge Transport servers and Hub Transport servers in adatum.com. You need to recommend a solution to ensure that the Exchange Server 2010 SP1 servers can queue email messages for humongousinsurance.com. What should you include in the recommendation?

- A. an authoritative domain
- B. a retention policy
- C. a remote domain
- D. an external relay domain

Answer: D

Question: 2

You are evaluating the implementation of database availability groups (DAGs). You need to recommend a DAG implementation that meets the redundancy requirements of A . Datum. What should you recommend?

- A. Add two Mailbox servers to each site. Create one DAG for each site. Add the Mailbox servers for each site to their respective DAG.

- B. Add one Mailbox server to each site. Create one DAG that contains both Mailbox servers.
- C. Add one Mailbox server to each site. Create two DAGs. Add one Mailbox server to each DAG.
- D. Add two Mailbox servers to each site. Create two DAGs. Add one Mailbox server from each site to each DAG.

Answer: A

Question: 3

You need to recommend changes to the existing Active Directory infrastructure to support the planned Exchange Server 2010 SP1 deployment. The solution must meet the business goals of A . Datum. What should you include in the recommendation? (Choose all that apply.)

- A. Upgrade one global catalog server in each site to Windows Server 2008 R2.
- B. Raise the functional level of the domain.
- C. Raise the functional level of the forest.
- D. Upgrade all of the global catalog servers to Windows Server 2003 x64 Edition.
- E. Upgrade all of the domain controllers to Windows Server 2003 x64 Edition.

Answer: B, C

Question: 4

You need to recommend a message routing design for the period during which A . Datum transitions from Exchange Server 2003 to Exchange Server 2010 SP1. The solution must meet the business goals of A. Datum. What should you include in the recommendation?

- A. an Exchange hub site for each site and a Send connector that uses TOK-HUB1 and BAN-HUB1 as the source servers
- B. a scoped Send connector that uses TOK-BE-1 as the source server and a scoped Send connector that uses BAN-BE-1 as the source server
- C. an Exchange hub site for each site and Exchange-specific site link costs
- D. a scoped Send connector that uses TOK-HUB-1 as the source server and a scoped Send connector that uses BAN-HUB-1 as the source server

Answer: B

Question: 5

You need to recommend an administrative solution for the human resources teams. The solution must meet the security requirements of A . Datum. What should you include in the recommendation?

- A. a split permissions model
- B. built-in security groups and distribution groups
- C. management role groups
- D. direct role assignments

Answer: C

Question: 6

You are evaluating the implementation of TOK-HUB1 and BAN-HUB1. You need to recommend a Hub Transport server topology that meets the redundancy requirements of A . Datum. The solution must also support the business goals of A . Datum. What should you include in the recommendation?

- A. Deploy TOK-HUB1 to the Tokyo site. Deploy BAN-HUB1 to the Bangkok site. Create one Send connector in each site.
- B. Deploy TOK-HUB1 to the Tokyo site. Deploy BAN-HUB1 to the Bangkok site. Deploy a hardware load balancer to each site. Configure the virtual IP address of the load balancer to point to the Hub Transport servers.
- C. Deploy TOK-HUB1 and an additional Hub Transport server named TOK-HUB2 to the Tokyo site. Deploy BAN-HUB1 and an additional Hub Transport server named BAN-HUB2 to the Bangkok site. Deploy a hardware load balancer to each site. Configure the virtual IP address of the load balancer to point to the Hub Transport servers.
- D. Deploy TOK-HUB1 and an additional Hub Transport server named TOK-HUB2 to the Tokyo site. Deploy BAN-HUB1 and an additional Hub Transport server named BAN-HUB2 to the Bangkok site. Create one Send connector in each site.

Answer: D

Question: 7

You need to recommend a routing group configuration that meets the business requirements of A . Datum. What should you include in the recommendation?

- A. one routing group for each office that contains all of the Exchange servers in that office
- B. one routing group that contains all of the Exchange Server 2003 servers and all of the Exchange Server 2010 SP1 servers
- C. one routing group for each office that contains only the Exchange Server 2003 servers in that office and one routing group for each office that contains only the Exchange Server 2010 SP1 servers in that office
- D. one routing group for each office that contains only the Exchange Server 2003 servers in that office and one routing group that contains all of the Exchange Server 2010 SP1 servers

Answer: D

Question: 8

You need to recommend a solution that meets the archiving requirements of A . Datum. What should you include in the recommendation?

- A. recovery databases and Personal Archives
- B. single item recovery and recovery databases
- C. single item recovery and litigation holds
- D. Personal Archives and retention policies

Answer: D

Question: 9

You plan to deploy Microsoft Forefront Online Protection for Exchange (FOPE). You need to recommend changes to the environment to ensure that inbound email messages from the Internet are scanned by FOPE. What should you include in the recommendation?

- A. Implement Microsoft Forefront Threat Management Gateway (TMG), and then create a sharing policy.
- B. Implement Microsoft Forefront Threat Management Gateway (TMG), and then create a federation trust.
- C. Modify the mail exchange (MX) records of A. Datum to point to FOPE.
- D. Modify the sender policy framework (SPF) record of A. Datum to point to FOPE.
- E. Implement Forefront Protection 2010 for Exchange Server, and then create an organization relationship.

Answer: C

Question: 10

You need to recommend a Client Access server design that meets the redundancy requirements of A . Datum. What should you include in the recommendation?

- A.
 - Four Client Access servers
 - One hardware load balancer
 - DNS round robin and subnet prioritization
- B.
 - Two Client Access arrays
 - Four Client Access servers
 - DNS round robin and subnet prioritization
- C.
 - Two Client Access arrays
 - Four Client Access servers
 - Two hardware load balancers
- D.
 - One Client Access array
 - Two Client Access servers
 - One hardware load balancer

Answer: D

Question: 11

The WAN link between the Tokyo office and the Bangkok office is heavily congested. During normal business hours, the average round-trip time for packets to travel across the WAN link is 185 ms. The portable computer of the manager of the finance department recently experienced a hard disk failure. The hard disk failure resulted in the loss of more than three years of email.

- A. an Edge Transport server, three Edge Transport rules, and an email address policy.
- B. an Edge Transport server and address rewrite entries.
- C. a Hub Transport server and address rewrite entries.
- D. a Hub Transport server, three Hub Transport rules, and an email address policy.

Answer: B
