Microsoft MCSE Certification 70-341 Exam

- **Vendor: Microsoft**
- **Exam Code: 70-341**
- **Exam Name: Microsoft Core Solutions of Microsoft Exchange Server 2013**

QUESTION 1

You have an Exchange Server 2013 organization. You create two distribution groups named Group1 and Group2. Group1 and Group2 each contain several hundred users. Group1 contains a user named User1. You need to configure moderation for Group2. The solution must meet the following requirements:

- Email sent from the members of Group1 must NOT be moderated unless the sender is User1.
- All other email must be moderated by a user named Admin1.

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

A. Create a transport rule that has a condition of the recipient is Group2.
Configure the transport rule to have an action of Forward the message for approval to Admin1.
B. Run Set-DistributionGroup Group2 -Moderated By Admin1.
BypassModerationFromSendersOrMembers Group1 -ModerationEnabled $true.
C. Create a transport rule that has the conditions of the sender is User1 and the recipient is Group2.
Configure the transport rule to have an action of Forward the message for approval to Admin1.
D. Create a transport rule that has the conditions of the sender is User1 and the recipient is Group1.
Configure the transport rule to have an action of Forward the message for approval to Admin1.

Answer: BC

Explanation:

Moderated Transport.

You can require all messages sent to specific recipients be approved by moderators by Using the moderated transport feature in Microsoft Exchange Server 2013. You can configure any type of recipient as a moderated recipient, and Exchange 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.

Transport Rules.

Using Transport rules, you can look for specific conditions in messages that pass through your organization and take action on them. Transport rules let you apply messaging policies to email messages, secure messages, protect messaging systems, and prevent information leakage. Many organizations today are required by law, regulatory requirements, or company policies to apply messaging policies that limit the interaction between recipients and senders, both inside and outside the organization. In addition to limiting interactions among individuals, departmental groups inside the organization, and entities outside the organization, some organizations are also subject to the following messaging policy requirements:

- Preventing inappropriate content from entering or leaving the organization Filtering confidential organization information
- Tracking or archiving copying messages that are sent to or received from specific individuals

Redirecting inbound and outbound messages for inspection before delivery Applying disclaimers to messages as they pass through the organization as messages go through the Transport pipeline, the Transport rules agent is invoked. The Transport rules agent is a special Transport agent that processes the Transport rules you create. The Transport rules agent scans the message, and if the message fits the conditions you specify in a Transport rule, it takes the specified action on that message.

NOT A

This means that all email sent to Group2 will be moderated.

NOT D

Unknown option.

B

When you configure a recipient for moderation, all messages sent to that recipient are subject to approval by the designated moderators. Allow the members of the distribution group named Group1 to bypass moderation. Combination of this rule and option C allows for only User1 to be affected by the moderator Admin1.

C

Need to create a transport rule that identifies User1.

QUESTION 2

You have an Exchange Server 2013 organization that contains one server named exl.contoso.com. The server has the Mailbox server role and the Client Access server role installed. You plan to configure users to work from home and to access their email by using the Outlook Anywhere feature. Upon testing the planned configuration, you discover that the users can connect and synchronize email from home, but they cannot execute the following tasks:

- Set automatic replies for Out of Office.
- Download changes to the offline address book.
- View availability data when scheduling meetings with coworkers.

The users can execute these tasks when they work from the office. You need to ensure that the users can execute the tasks when they work from home. Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

A. Install a new certificate on exl.contoso.com.
B. Modify the EWS virtual directory.
C. Create a new Autodiscover virtual directory.
D. Renew the certificate on exl.contoso.com.
E. Modify the OAB virtual directory.

Answer: BE

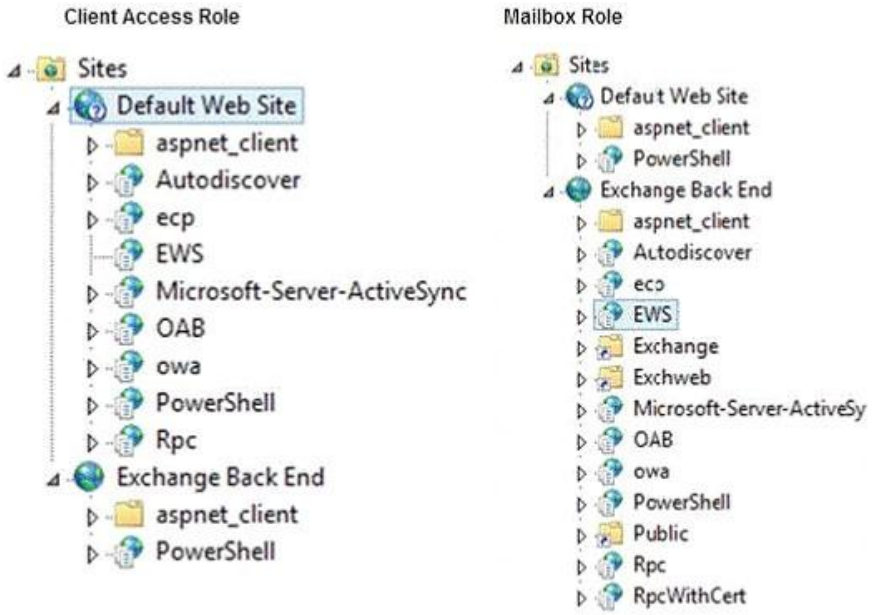
Explanation:

http://blogs.msdn.com/b/mvpawardprogram/archive/2013/03/18/virtual-directories-exchange-2013.aspx

EWS virtual directory (Exchange Web Services).

A virtual directory is used by Internet Information Services (IIS) to allow access to a web applications in Exchange 2013 Autodiscover Service, ECP, EWS, ActiveSync, OWA, OAB, Powershell are the available virtual directories through EAC. You can manage a variety of virtual directory settings on Exchange 2013 including authentication, security, and reporting settings. I am explaining here, how you can manage the Virtual Directories through Exchange Admin Center. I have also included some example PowerShell cmdltes to show how to manage those resources:

The Client Access Role naturally uses the **Default Web Site** as the home for all the Exchange Virtual Directories (EWS, OAB, RPC, Autodiscover), just as it did in Exchange 2007 & 2010. The Mailbox Role uses the Exchange Back End site as the home for the corresponding Exchange 2013 Web Applications.



Although it would appear that these sites are relatively similar, the main difference between the two is not immediately visible until you go to PowerShell to manage the Virtual Directories. Just as in Exchange 2007 & 2010, you will run the varios commands to manage your Virtual Directories:

- Get-WebServicesVirtualDirectory
- Get-OabVirtualDirectory
- Get-AutodiscoverVirtualDirectory
- Get-ActiveSyncVirtualDirectory

Default settings on Virtual Directories in Exchange Server 2013.
http://maybe-i-know-it.blogspot.com.au/2013/05/default-settings-on-virtual-directories.html
Autodiscover
[PS] C:\Windows\system32>get-autodiscovervirtualdirectory exch01\autodiscover* | fl name, internal*, external*, *authentication
Name: Autodiscover (Default Web Site)
InternalAuthenticationMethods : {Basic, Ntlm, WindowsIntegrated, WSSecurity, OAuth} InternalUrl :
ExternalAuthenticationMethods : {Basic, Ntlm, WindowsIntegrated, WSSecurity, OAuth}
ExternalUrl :
LiveIdNegotiateAuthentication : False
WSSecurityAuthentication : True
LiveIdBasicAuthentication : False
BasicAuthentication : True
DigestAuthentication : False
WindowsAuthentication : True
OAuthAuthentication : True
AdfsAuthentication : False
IIS FE: Anonymous, Basic, Windows Authentication
IIS BE: Anonymous, Windows Authentication
ECP
[PS] C:\Windows\system32>Get-ecpvirtualDirectory exch01\ecp* | fl name, internal*, external*,

*authentication
Name : ecp (Default Web Site)
InternalAuthenticationMethods : {Basic, Fba}
InternalUrl : https://exch01.contoso.com/ecp
ExternalUrl :
ExternalAuthenticationMethods : {Fba}
BasicAuthentication : True
WindowsAuthentication : False
DigestAuthentication : False
FormsAuthentication : True
LiveIdAuthentication : False
AdfsAuthentication : False
IIS FE: Anonymous, Basic
IIS BE: Anonymous, Basic
EWS
[PS] C:\Windows\system32>Get-WebServicesVirtualDirectory exch01\ews* | fl name, internal*, external*,
*authentication
Name : EWS (Default Web Site)
InternalNLBBypassUrl :
InternalAuthenticationMethods : {Ntlm, WindowsIntegrated, WSSecurity, OAuth}
InternalUrl : https://exch01.contoso.com/EWS/Exchange.asmx
ExternalAuthenticationMethods : {Ntlm, WindowsIntegrated, WSSecurity, OAuth}
ExternalUrl :
CertificateAuthentication :
LiveIdNegotiateAuthentication :
WSSecurityAuthentication : True
LiveIdBasicAuthentication : False
BasicAuthentication : False
DigestAuthentication : False
WindowsAuthentication : True
OAuthAuthentication : True
AdfsAuthentication : False
IIS FE: Anonymous, Basic
IIS BE: Anonymous, Basic
Microsoft-Server-ActiveSync
[PS] C:\Windows\system32>Get-activesyncvirtualDirectory exch01\microsoft* | fl name, internal*, external*,
*authentication
Name : Microsoft-Server-ActiveSync (Default Web Site)
InternalUrl : https://exch01.contoso.com/Microsoft-Server-ActiveSync
InternalAuthenticationMethods : {}
ExternalUrl :
ExternalAuthenticationMethods : {}
IIS FE: Basic
IIS FE: Basic
OAB
[PS] C:\Windows\system32>Get-oabVirtualDirectory exch01\oab* | fl name, internal*, external*, *authentication
Name : OAB (Default Web Site)
InternalUrl : https://exch01.contoso.com/OAB
InternalAuthenticationMethods : {WindowsIntegrated}
ExternalUrl :
ExternalAuthenticationMethods : {WindowsIntegrated}
BasicAuthentication : False

WindowsAuthentication : True
IIS FE: Windows Authentication
IIS FE: Windows Authentication
OWA
[PS] C:\Windows\system32>Get-OwaVirtualDirectory exch01\owa* | fl name, internal*, external*, *authentication Name : owa (Default Web Site)
InternalAuthenticationMethods : {Basic, Fba}
InternalUrl : https://exch01.contoso.com/owa
ExternalUrl :
ExternalAuthenticationMethods : {Fba}
BasicAuthentication : True
WindowsAuthentication : False
DigestAuthentication : False
FormsAuthentication : True
LiveIdAuthentication : False
AdfsAuthentication : False
IIS FE: Basic
IIS BE: Anonymous, Windows Authentication
PowerShell
[PS] C:\Windows\system32>Get-powershellvirtualDirectory exch01\powershell* | fl name, internal*, external*,
*authentication Name : PowerShell (Default Web Site)
InternalAuthenticationMethods : {}
InternalUrl : http://exch01.contoso.com/powershell
ExternalAuthenticationMethods : {}
ExternalUrl :
CertificateAuthentication : True
LiveIdNegotiateAuthentication : False
WSSecurityAuthentication : False
LiveIdBasicAuthentication : False
BasicAuthentication : False
DigestAuthentication : False
WindowsAuthentication : False
OAuthAuthentication : False
AdfsAuthentication : False
IIS FE: None
IIS BE: Windows Authentication
RPC
[PS] C:\>Get-outlookanywhere exch01\rpc* | fl name, internal*, external*, *authentication Name : Rpc (Default Web Site)
InternalHostname : exch01.contoso.com
InternalClientAuthenticationMethod : Ntlm
InternalClientsRequireSsl : False
ExternalHostname :
ExternalClientAuthenticationMethod : Negotiate
ExternalClientsRequireSsl : False
IIS FE: Basic, Windows Authentication
IIS FE: Windows Authentication
NOT AD
Not related to a certificate issue.
NOT C
You may create a new Autodiscover site if your organization has multiple e-mail domains and each requires its own Autodiscover site and corresponding virtual directory, use the New-AutodiscoverVirtualDirectory cmdlet to create a new Autodiscover virtual directory under a new Web site. Not required in this scenario. If you were going to create a new Autodiscover site then

you would have to delete the old one first.

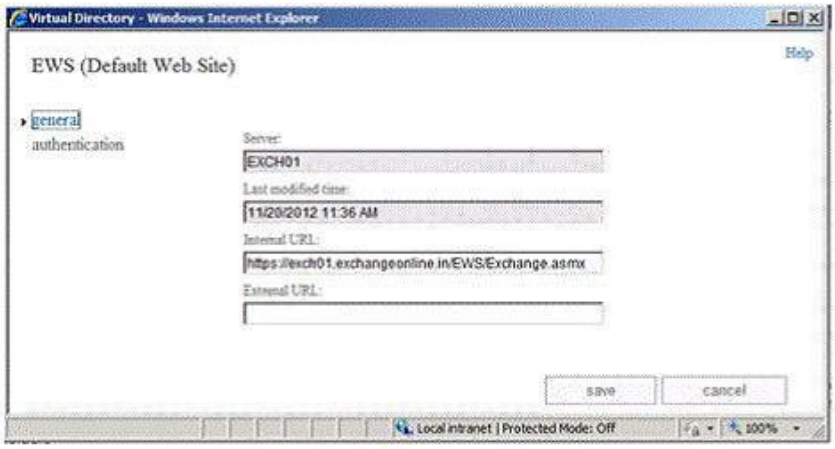
B

Need to modify the EWS virtual directory in order to create the external URL.

3. EWS (Default Website)

Select ews (Default Website) and click Edit to go through the following windows:

General Settings



You may have a chance here to edit the External/Internal url associated with EWS.

Authentication

Integrated, Digest, Basic authentications are available to set with EWS.

Use the **Set-WebServicesVirtualDirectory**cmdlet to modify an existing Exchange Web Services virtual directory on a server running Microsoft Exchange Server 2013. For example, the following cmdlet can set the EWS authentication method as *DigestAuthentication* and also it sets the external and internal EWS virtual directories of EWS

Set-WebServicesVirtualDirectory -Identity exchangeonline.in\EWS(Default Web Site)-ExternalUrl https://www.exchangeonline.in/EWS/exchange.asmx -BasicAuthentication Strue -InternalUrl https://exchangeonline.internal.in/EWS/exchange.asmx

Note: Please remember to set the corresponding changes in IIS virtual Directory for ews also.

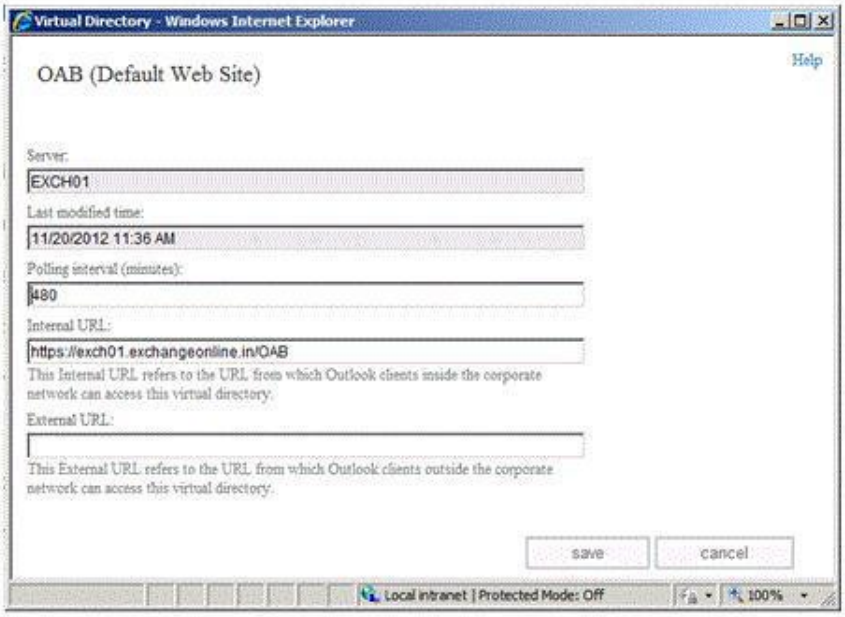
E

Need to modify the OAB virtual directory to create the External URL.

5. oab (Default WebSite)

Select oab (Default Website) and click Edit to go through the following windows:

General Settings



You may set a new value for 'Poliing interval' of Offline Address Book fetch in this window. Thus the new oab will be checked in this interval set here. You may also set the Internal, External URL values here.

http://technet.microsoft.com/en-us/library/bb123710(v=exchg.150).aspx
http://technet.microsoft.com/en-us/library/bb232155(v=exchg.150).aspx
http://technet.microsoft.com/en-us/library/bb125170(v=exchg.150).aspx

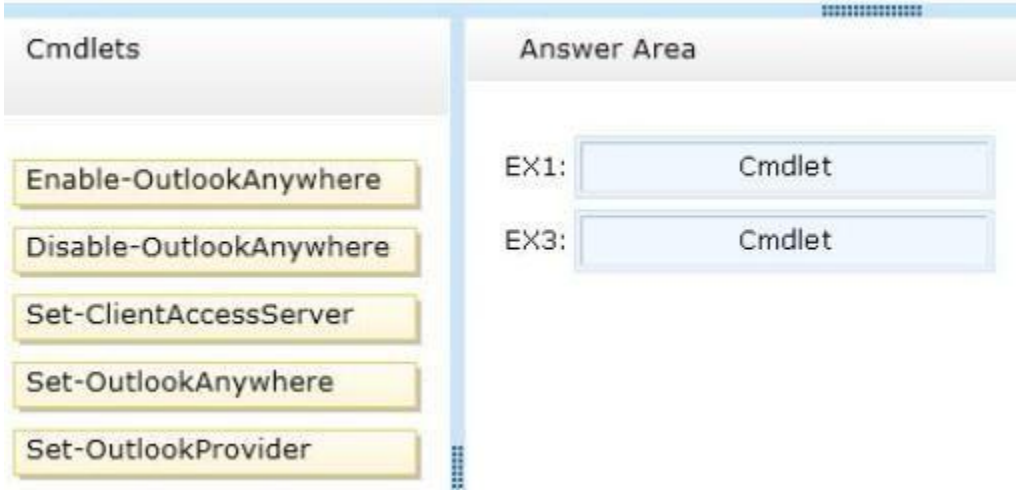
QUESTION 3

Drag and Drop Question

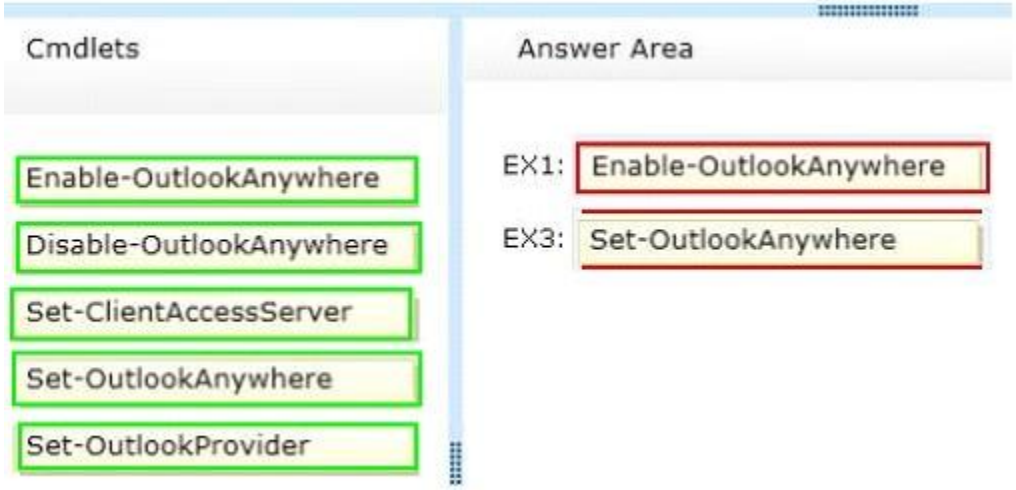
Your network contains an Active Directory forest. The forest contains a single domain named fabrikam.com. You have an Exchange Server organization that contains four servers. The servers are configured as shown in the following table.

Server name	Role	Exchange Server version
EX1	Client Access Hub Transport	Exchange Server 2010
EX2	Mailbox	Exchange Server 2010
EX3	Client Access	Exchange Server 2013
EX4	Mailbox	Exchange Server 2013

You plan to enable Outlook Anywhere for all users. You plan to configure the users to connect to the name oa.fabrikam.com. The IP address of oa.fabrikam.com points to EX3. You need to ensure that users on EX2 and EX4 can access their mailbox by using Outlook Anywhere, Which command should you run on EX1 and EX3? (To answer, drag the appropriate cmdlets to the correct servers. Each cmdlet may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.)



Answer:



QUESTION 4

You have an Exchange Server 2013 organization named adatum.com. The organization contains two servers named EX1 and EX2 that are configured as shown in the table. Both servers are members of a database availability group (DAG). EX1 has the active copy of a database named Database1. Several users who have mailboxes in Database1 discover that all of their outbound email messages remain in their Drafts folder when they use Outlook Web App. You need to ensure that the email messages are delivered. What should you do?

Server name	Role
EX1	Mailbox, Client Access
EX2	Mailbox, Client Access

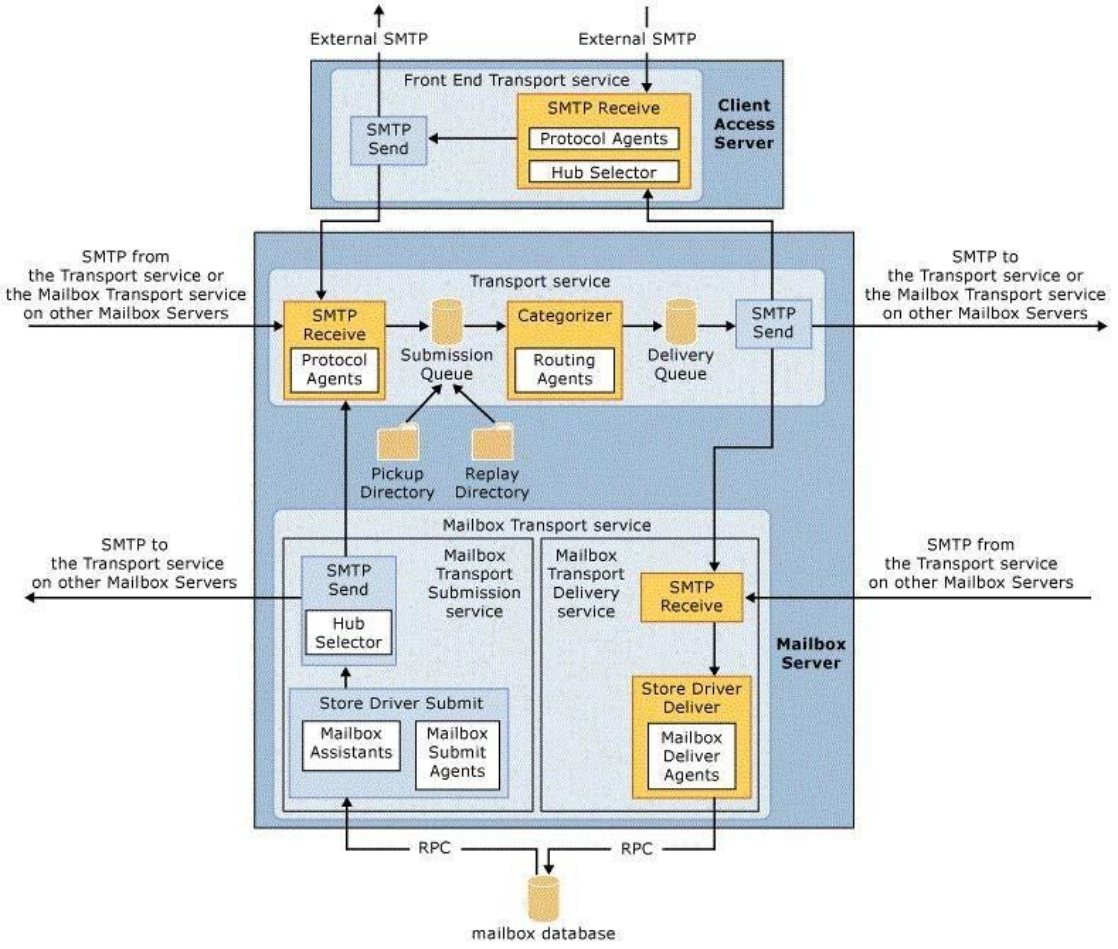
A. On EX2, retry the message queues.
B. On EX1, start the Microsoft Exchange Mailbox Transport Submission service.
C. On EX2, start the Microsoft Exchange Mailbox Transport Submission service.
D. On EX1, retry the message queues.

Answer: B

Explanation:

In Microsoft Exchange Server 2013, mail flow occurs through the transport pipeline. The transport pipeline is a collection of services, connections, components, and queues that work together to route all messages to the categorizer in the Transport service on a Mailbox server inside the organization.

The following figure shows the relationships among the components in the Exchange 2013 transport pipeline.



The Transport service on a Mailbox server.

Every message that's sent or received in an Exchange 2013 organization must be categorized in the Transport service on a Mailbox server before it can be routed and delivered. After a message has been categorized, it's put in a delivery queue for delivery to the destination mailbox database, the destination database availability group (DAG), Active Directory site, or Active Directory forest, or to the destination domain outside the organization. The Transport service on a Mailbox server consists of the following components and processes:

- SMTP Receive

When messages are received by the Transport service, message content inspection is performed, transport rules are applied, and anti-spam and anti-malware inspection is performed if they are enabled. The SMTP session has a series of events that work together in a specific order to validate the contents of a message before it's accepted. After a message has passed completely through SMTP Receive and isn't rejected by receive events, or by an anti-spam and anti-malware agent, it's put in the Submission queue.

- Submission

Submission is the process of putting messages into the Submission queue. The categorizer picks up one message at a time for categorization. Submission happens in three ways: Through an SMTP

Receive connector. Through the Pickup directory or the Replay directory. These directories exist on the Mailbox server. Correctly formatted message files that are copied into the Pickup directory or the Replay directory are put directly into the Submission queue through a transport agent.
- Categorizer
The categorizer picks up one message at a time from the Submission queue. The categorizer completes the following steps:
- Recipient resolution, which includes top-level addressing, expansion, and bifurcation.
- Routing resolution.
- Content conversion.
Additionally, mail flow rules that are defined by the organization are applied. After messages have been categorized, they're put into a delivery queue that's based on the destination of the message. Messages are queued by the destination mailbox database, DAG, Active Directory site, Active Directory forest or external domain.
- SMTP Send
How messages are routed from the Transport service depends on the location of the message recipients relative to the Mailbox server where categorization occurred. The message could be routed to the Mailbox Transport service on the same Mailbox server, the Mailbox Transport service on a different Mailbox server that's part of the same DAG, the Transport service on a Mailbox server in a different DAG, Active Directory site, or Active Directory forest, or to the Front End Transport service on a Client Access server for delivery to the Internet.
- Retry a Message Queue
When a transport server can't connect to the next hop, the delivery queue is put in a status of Retry. When you retry a delivery queue by using Queue Viewer or the Shell, you force an immediate connection attempt and override the next scheduled retry time. If the connection isn't successful, the retry interval timer is reset. The delivery queue must be in a status of Retry for this action to have any effect. Use Queue Viewer in the Exchange Toolbox to retry a queue Click Start > All Programs > Microsoft Exchange 2013 > Exchange Toolbox. In the Mail flow tools section, double-click Queue Viewer to open the tool in a new window. In Queue Viewer, click the Queues tab. A list of all queues on the server to which you're connected is displayed. Click Create Filter, and enter your filter expression as follows:
- Select Status from the queue property drop-down list.
- Select Equals from the comparison operator drop-down list.
- Select Retry from the value drop-down list.
- Click Apply Filter. All queues that currently have a Retry status are displayed.
- Select one or more queues from the list. Right-click, and then select Retry Queue. If the connection attempt is successful, the queue status changes to Active. If no connection can be made, the queue remains in a status of Retry and the next retry time is updated.
- Resubmit messages in queues
Resubmitting a queue is similar to retrying a queue, except the messages are sent back to the Submission queue for the categorizer to reprocess. You can resubmit messages that have the following status:
- Delivery queues that have the status of Retry. The messages in the queues can't be in the Suspended state.
- Messages in the Unreachable queue that aren't in the Suspended state.
- Messages in the poison message queue.
OWA DRAFTS FOLDER
http://thoughtsofanidlemind.wordpress.com/2013/03/25/exchange-2013-dns-stuck-messages/
OWA clients automatically capture copies of messages as they are being composed and store them in the Drafts folder. When the user issues a sent command, the Mailbox submit agent (running within the Store driver) takes over and processes the outbound message by giving it to either the Transport service running on the same mailbox server or to the Transport server running on another mailbox server. The connection is made via SMTP. Messages stay in the Drafts folder until they are successfully sent by being processed by the transport service. At this point, items are moved into the Sent Items folder. OWA 2013 behaves in the same way as OWA 2010 -nothing has changed in the way that messages are held in the Drafts folder until dispatch. What might account for user

descriptions of items being "stuck" is when a problem occurs somewhere in the transport pipeline that prevents outbound messages being processed. For instance, items will remain in the Drafts folder if the Store cannot pass them to the transport system. If the transport service is not running on any available server or the mailbox transport service is not running on the mailbox server that hosts the active database for the user's mailbox, items will stay in the Drafts folder until the services come online and Exchange is able to process outbound items.
NOT AC
Active copy of a database named Database1 (EX1) not on EX2.
NOT D
Messages stay in the Drafts folder until they are successfully sent by being processed by the transport service.
B
Resubmitting a queue is similar to retrying a queue, except the messages are sent back to the Submission queue for the categorizer to reprocess. Messages stay in the Drafts folder until they are successfully sent by being processed by the transport service If the transport service is not running on any available server or the mailbox transport service is not running on the mailbox server that hosts the active database for the user's mailbox, items will stay in the Drafts folder until the services come online and Exchange is able to process outbound items.

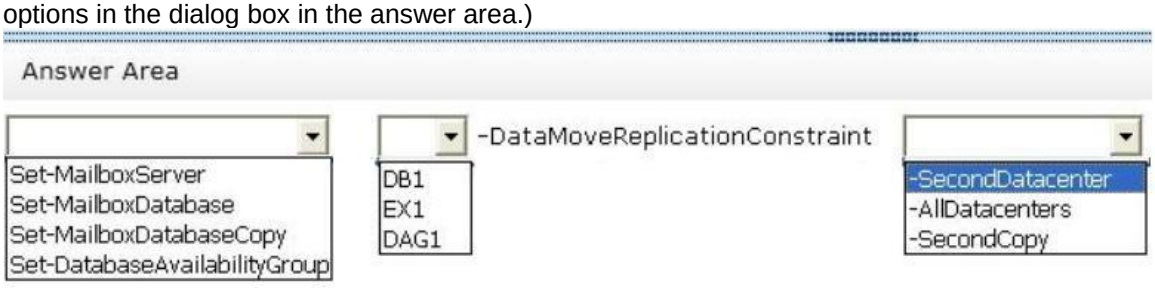
QUESTION 5
Hotspot Question
You have an Exchange Server 2013 organization that contains three servers. The servers are configured as shown in the following table.

Server name	Role	Active Directory site
EX1	Mailbox Client Access	Chicago
EX2	Mailbox Client Access	Seattle
EX3	Mailbox Client Access	Dallas

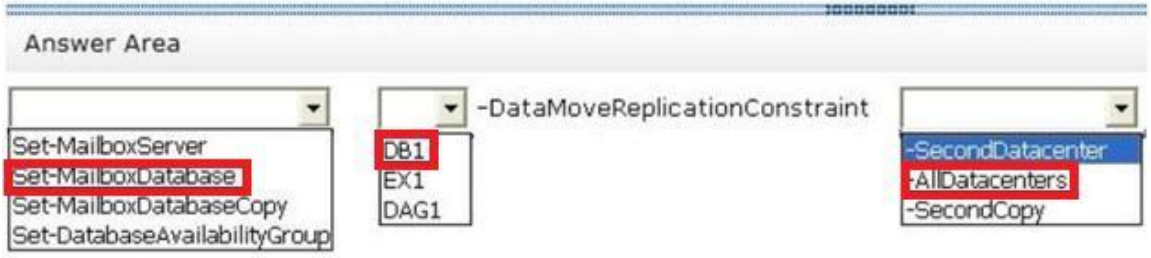
All of the servers are part of a database availability group (DAG) named DAG1. The databases are configured as shown in the following table.

Database name	Mounted on server
DB1	EX1
DB2	EX2

All of the databases replicate between all the members of DAG1. You plan to move all mailboxes from DB1 to DB2. You need to ensure that the passive copies of DB1 are in a healthy state before you move the mailboxes. Which command should you run? (To answer, select the appropriate options in the dialog box in the answer area.)



Answer:



Explanation:

SECTION1

NOT Set-MailboxServer

Use the Set-MailboxServer cmdlet to modify attributes on a computer running Microsoft Exchange with the Mailbox server role installed. Not required in this scenario.

Set-MailboxDatabase

Use the Set-MailboxDatabase cmdlet to configure a variety of properties for a mailbox database.

EXAMPLE 1

This example sets the length of time that deleted items are retained. If a specific mailbox has its own item retention set, that value is used instead of this value, which is set on the mailbox database. Set-MailboxDatabase "Mailbox Database01" -DeletedItemRetention 7.00:00:00 NOT Set-MailboxDatabaseCopy

Use the Set-MailboxDatabaseCopy cmdlet to configure the properties of a database copy.

EXAMPLE 1

This example configures the replay lag time with a value of 3 days for a copy of the database DB2 hosted on the Mailbox server MBX1. Set-MailboxDatabaseCopy -Identity DB2\MBX1 -ReplayLagTime 3.0:0:0

EXAMPLE 2

This example configures an activation preference of 3 for the copy of the database DB1 hosted on the Mailbox server MBX2.Set-MailboxDatabaseCopy -Identity DB1\MBX2 -ActivationPreference 3

NOT Set-DatabaseAvailabilityGroup

Use the Set-DatabaseAvailabilityGroup cmdlet to configure some of the properties of a database availability group (DAG). The Set-DatabaseAvailabilityGroup cmdlet enables you to manage DAG properties that can't be managed from the Exchange Management Console, such as enabling and disabling cross-site RPC client access, configuring network discovery, selecting the TCP port used for replication, and enabling datacenter activation coordination (DAC) mode.

SECTION2

Need to identify the name of the mailbox database. (DB1)

SECTION3

The DataMoveReplicationConstraint parameter specifies the throttling behavior for high availability mailbox moves. The possible values include:

None Moves shouldn't be throttled to ensure high availability. Use this setting if the database isn't part of a database availability group (DAG).

SecondCopy

At least one passive mailbox database copy must have the most recent changes synchronized. This is the default value. Use this setting to indicate that the database is replicated to one or more mailbox database copies.

SecondDatacenter

At least one passive mailbox database copy in another Active Directory site must have the most recent changes replicated. Use this setting to indicate that the database is replicated to database copies in multiple Active Directory sites. AllDatacenters At least one passive mailbox database copy in each Active Directory site must have the most recent changes replicated. Use this setting to indicate that the database is replicated to database copies in multiple Active Directory sites.

AllCopies

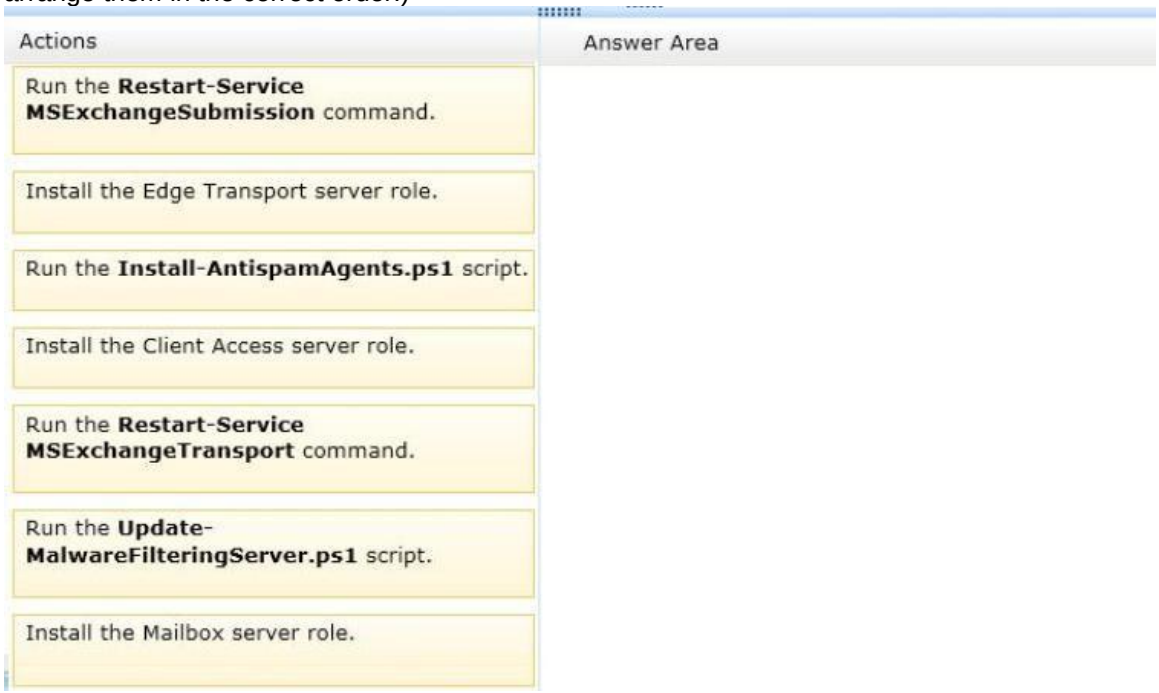
All copies of the database must have the most recent changes replicated. Use this setting to indicate that the database is replicated to one or more mailbox database copies. The database is

replicated to database copies in multiple Active Directory sites so eliminate SecondCopy. Unsure of why -AllDatacenters is the final choice but there are 3 Active Directory sites in this scenario.

QUESTION 6

Drag and Drop Question

Your network contains an internal network and a perimeter network. You have an Exchange Server 2010 organization that contains an Edge Transport server named EX3. You plan to upgrade the organization to Exchange Server 2013. You plan to replace EX3 and its functionalities with a new server named EX6 that has Exchange Server 2013 installed. EX6 will be used to send all email messages to and receive all email messages from the Internet and to filter spam. You need to recommend which steps are required to install EX6. EX6 must have the least number of Exchange Server roles installed. Which three actions should you recommend performing on EX6 in sequence? (To answer, move the appropriate three actions from the list of actions to the answer area and arrange them in the correct order.)



Answer:

Explanation:
The transport services indeed exist in MBX role in Exchange 2013.
https://technet.microsoft.com/en-us/library/bb201691%28v=exchg.150%29.aspx
In Microsoft Exchange Server 2013, the following anti-spam agents are available in the Transport service on Mailbox servers, but they are not installed by default:
- Content Filter agent
- Sender ID agent
- Sender Filter agent
- Protocol Analysis agent for sender reputation

Case Study 1: Contoso Ltd. (QUESTION 7 ~ QUESTION 14)

.....

Case Study 2: Litware, Inc. (QUESTION 15 ~ QUESTION 21)

.....

Case Study 3: A.Datum Corporation (QUESTION 22 ~ QUESTION 30)

.....

Case Study 4: Proseware, Inc. (QUESTION 31 ~ QUESTION 37)

.....

Case Study 5: Fabrikam, Inc. (QUESTION 57 ~ QUESTION 68)

Overview
Fabrikam, Inc., is a pharmaceutical company located in Europe. The company has 5,000 users. The company is finalizing plans to deploy an Exchange Server 2013 organization. The company has offices in Paris and Amsterdam.

Existing Environment

Active Directory Environment

The network contains an Active Directory domain named fabrikam.com. An Active Directory site exists for each office.

Network Infrastructure

The roles and location of each server are configured as shown in the following table.

Server name	Role	Location
DC1	Domain controller Global catalog server	Paris office
DC2	Domain controller	Paris office
DC3	Schema master Domain controller Global catalog server	Amsterdam office
FS1	File server	Paris office
FS2	File server	Paris office
FS3	File server	Amsterdam office
FS4	File server	Amsterdam office
TMG1	Microsoft Forefront Threat Management Gateway (TMG) 2010	Perimeter network in the Paris office

Client computers run either Windows 7 or Windows 8 and have Microsoft Office 2010 installed. The Paris office uses the 192.168.1.0/24 IP range. The Amsterdam office uses the 192.168.2.0/24 IP range. The offices connect to each other by using a high-speed, low-latency WAN link. Each office has a 10-Mbps connection to the Internet.

Planned Exchange Infrastructure

The company plans to deploy five servers that run Exchange Server. The servers will be configured as shown in the following table.

Server name	Server role	Location
EX1	• Exchange Server 2013 Mailbox server • Exchange Server 2013 Client Access server	Paris office
EX2	• Exchange Server 2013 Mailbox server • Exchange Server 2013 Client Access server	Paris office
EX3	• Exchange Server 2013 Mailbox server • Exchange Server 2013 Client Access server	Amsterdam office
EX4	• Exchange Server 2013 Mailbox server • Exchange Server 2013 Client Access server	Amsterdam office
EDGE1	Exchange Server 2010 Edge Transport server	Perimeter network in the Paris office

The company plans to have mailbox databases replicated in database availability groups (DAGs). The mailbox databases and DAGs will be configured as shown in the following table.

DAG name	Database name	DAG member
DAG1	OperationsDB FinanceDB SalesDB	EX1, EX3
DAG2	MarketingDB ResearchDB LabDB	EX2, EX4

DAG1 will use FS1 as a file share witness. DAG2 will use FS3 as a file share witness. You plan to create the following networks on each DAG:

- A dedicated replication network named DAGNET1
- A MAPI network named DAGNET2

All replication traffic will run on DAGNET1. All client connections will run on DAGNET2. Client connections must never occur on DAGNET1. Replication traffic must only occur on DAGNET2 if DAGNET1 is unavailable. Each Exchange Server 2013 Mailbox server will be configured to have two network adapters. The following two mailbox databases will not be replicated as part of the

DAGs:
- A mailbox database named AccountingDB that is hosted on EX1.
- A mailbox database named TempStaffDB that is hosted on EX4 EDGE1 will have an Edge Subscription configured, with both EX1 and EX2 as targets.

Requirements

Planned Changes

An external consultant reviews the Exchange Server 2013 deployment plan and identifies the following areas of concern:
- The DAGs will not be monitored.
- Multiple Edge Transport servers are required to prevent the potential for a single point of failure.

Technical Requirements

Fabrikam must meet the following technical requirements:
- Email must be evaluated for SPAM before the email enters the internal network.
- Production system patching must minimize downtime to achieve the highest possible service to users.
- Users must be able to use the Exchange Control Panel to autonomously join and disjoin their department's distribution lists.
- Users must be able to access all Internet-facing Exchange Server services by using the names of mail.fabrikam.com and autodiscover.fabrikam.com.

The company establishes a partnership with another company named A. Datum Corporation. A. Datum uses the SMTP suffix adatum.com for all email addresses. Fabrikam plans to exchange sensitive information with A. Datum and requires that the email messages sent between the two companies be encrypted. The solution must use Domain Security. Users in the research and development (R&D) department must be able to view only the mailboxes of the users in their department from Microsoft Outlook. The users in all of the other departments must be prevented from viewing the mailboxes of the R&D users from Outlook. Administrators plan to produce HTML reports that contain information about recent status changes to the mailbox databases. Fabrikam is evaluating whether to abort its plan to implement an Exchange Server 2010 Edge Transport server and to implement a Client Access server in the Paris office instead. The Client Access server will have anti-spam agents installed.

QUESTION 57

Hotspot Question

You need to recommend which configurations must be set for each network. Which configurations should you recommend? To answer, select the appropriate configurations for each network in the answer area.

Network Name	ReplicationEnabled	MapiAccessEnabled
DAGNET1	☐	☐
DAGNET2	☐	☐

Answer:

Network Name	ReplicationEnabled	MapiAccessEnabled
DAGNET1	☐	☐
DAGNET2	☐	☐

QUESTION 58
An administrator recommends removing EDGE1 from the implementation plan and adding a new Client Access server named CAS-8 instead. You need to identify which anti-spam feature will NOT be available on CAS-8. Which anti-spam feature should you identify?

A. Connection Filtering
B. Sender Filtering
C. Content Filtering
D. Recipient Filtering

Answer: A
Explanation:
EDGE1 is an exchange server 2010. CAS-8 would be an exchange server 2013. Typically, you would enable the anti-spam agents on a mailbox server if your organization doesn't have an Edge Transport server, or doesn't do any prior anti-spam filtering before accepting incoming messages. Connection Filtering agent is only available on the Edge Transport server role. Exchange 2013 does not have an Edge Transport server role yet. The Connection Filter agent and the Attachment Filter agent are only available on an Edge Transport server. Connection Filtering on Edge Transport Servers: Exchange 2013 Help.
Anti-spam agents on Legacy Edge Transport servers.
If your organization has an Exchange 2007 or Exchange 2010 Edge Transport server installed in the perimeter network, all of the anti-spam agents that are available on a Mailbox server are installed and enabled by default on the Edge Transport server. However, the following anti-spam agents are only available on an Edge Transport server. Connection Filtering agent Connection filtering inspects the IP address of the remote server that's trying to send messages to determine what action, if any, to take on an inbound message. The remote IP address is available to the Connection Filtering agent as a byproduct of the underlying TCP/IP connection that's required for the SMTP session. Connection filtering uses a variety of IP Block lists, IP Allow lists, as well as IP Block List provider services or IP Allow List provider services to determine whether the connection from the specific IP should be blocked or allowed in the organization. For more information about connection filtering in Exchange 2010:
http://technet.microsoft.com/library/bb124320(v=exchg.141).aspx
Attachment Filter agent.
Attachment filtering filters messages based on attachment file name, file name extension, or file MIME content type. You can configure attachment filtering to block a message and its attachment, to strip the attachment and allow the message to pass through, or to silently delete the message and its attachment. For more information about attachment filtering in Exchange 2010:
http://technet.microsoft.com/library/bb124399(v=exchg.141).aspx
What's Discontinued in Exchange 2013.
http://technet.microsoft.com/en-us/library/jj619283(v=exchg.150).aspx
Feature.
Anti-spam agent management in the EMC.
In Exchange 2010, when you enabled the anti-spam agents on the Hub Transport server, you could manage the anti-spam agents in the Exchange Management Console (EMC). In Exchange 2013, when you enable the anti-spam agents in the Transport service on a Mailbox server, you can't manage the agents in the Exchange admin center (EAC). You can only use the Exchange Management Shell. For information about how to enable the anti-spam agents on a Mailbox server, see Enable Anti-Spam Functionality on a Mailbox Server.
Connection Filtering agent on Hub Transport servers.
In Exchange 2010, when you enabled the anti-spam agents on a Hub Transport server, the Attachment Filter agent was the only anti-spam agent that wasn't available. In Exchange 2013, when you enable the antispam agents in the Transport service on a Mailbox server, the Attachment Filter agent and the Connection Filtering agent aren't available. The Connection Filtering agent

provides IP Allow List and IP Block List capabilities. For information about how to enable the anti-spam agents on a Mailbox server, see Enable Anti-Spam Functionality on a Mailbox Server.
Note:
You can't enable the anti-spam agents on an Exchange 2013 Client Access server. Therefore, the only way to get the Connection Filtering agent is to install an Exchange 2010 or Exchange 2007 Edge Transport server in the perimeter network. For more information, see Use an Edge Transport Server in Exchange 2013.
Sender Filter agent
Sender filtering compares the sender on the MAIL FROM: SMTP command to an administrator-defined list of senders or sender domains who are prohibited from sending messages to the organization to determine what action, if any, to take on an inbound message.
Content Filter agent
Content filtering assesses the contents of a message. Spam quarantine is a feature of the Content Filter agent that reduces the risk of losing legitimate messages that are incorrectly classified as spam. Spam quarantine provides a temporary storage location for messages that are identified as spam and that shouldn't be delivered to a user mailbox inside the organization.
Recipient Filter agent
Recipient filtering compares the message recipients on the RCPT TO: SMTP command to an administrator defined Recipient Block list. If a match is found, the message isn't permitted to enter the organization. You can't enable the anti-spam agents on an Exchange 2013 Client Access server. Therefore, the only way to get the Connection Filtering agent is to install an Exchange 2010 or Exchange 2007 Edge Transport server in the perimeter network Connection Filtering agent is only available on the Edge Transport server role. Exchange 2013 does not have an Edge Transport server role yet.
NOT BCD
Only need to identify 1 and this is connection filtering.

QUESTION 59
You need to recommend which task is required to prepare Active Directory for the planned Exchange Server 2013 implementation. What should you recommend?

A. On any domain controller in the Paris office, run setup.exe /preparead.
B. On any domain controller in the Amsterdam office, run setup.exe /preparead.
C. On any domain controller in the Paris office, run setup.exe /preparealldomains.
D. On any domain controller in the Amsterdam office, run setup.exe /preparedomain.

Answer: B
Explanation:
B
The schema master is in the Amsterdam office. Before you install the release to manufacturing (RTM) version of Microsoft Exchange Server 2013 or later cumulative updates (CU) on any servers in your organization, you must prepare Active Directory and domains. Run setup.exe /preparead on the schema master.
NOT AC
The schema master is in the Amsterdam office. Run setup.exe /preparead on the schema master.
NOT D
Fabrikam has a single domain. In order to prepare a domain, run the following command from an elevated command prompt after browsing to the Exchange 2013 DVD/ISO:
Setup.exe /PrepareDomain /IAcceptExchangeServerLicenseTerms
If you have a single domain environment, you don't have to prepare the domain as the local domain is prepared for 2013 as part of preparing the AD. But, if you have a multi-domain environment, all other domains (except the one on which the AD was prepared) has to be ready for 2013. You can prepare all the domains in one go by running the command below:
Setup.exe /PrepareAllDomains /IAcceptExchangeServerLicenseTerms (you will need Enterprise

Admin rights).

QUESTION 60

Drag and Drop Question

You need to recommend to a solution to deploy the Outlook app. Which three actions should you recommend performing in sequence?

Answer:

QUESTION 61

You have an Exchange Server 2013 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

QUESTION 62
Your company has a Exchange Server 2013 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 63
You need to recommend a design that meets the technical requirements for communication between Fabrikam and A. Datum. Which three actions should you perform in fabrikam.com? (Each correct answer presents part of the solution. Choose three.)

A. Create a remote domain for adatum.com.
B. Exchange certificates with the administrators of adatum.com.
C. From EDGE1, create a Send connector that has an address space for adatum.com.
D. Run the Set-TransportConfigcmdlet.
E. Run the Set-TransportServercmdlet.
F. From a Mailbox server, create a Send connector that has an address space for adatum.com.

Answer: BDF
Explanation:
NOT A
Applies to: Exchange Server 2013, Exchange Online.
Remote domains are SMTP domains that are external to your Microsoft Exchange organization. You can create remote domain entries to define the settings for message transferred between your Exchange organization and specific external domains. The settings in the remote domain entry for a specific external domain override the settings in the default remote domain that normally apply to all external recipients. The remote domain settings are global for the Exchange organization. You can create remote domain entries to define the settings for message transfers between your Exchange Online organization and external domains. When you create a remote domain entry, you control the types of messages that are sent to that domain. You can also apply message format policies and acceptable character sets for messages that are sent from users in your organization to the remote domain.
NOT C
Edge1 is in the perimeter network and the send connector needs to be created on a mailbox server.
NOT E
Set-TransportServercmdlet.
Use the Set-TransportServer cmdlet to set the transport configuration options for the Transport

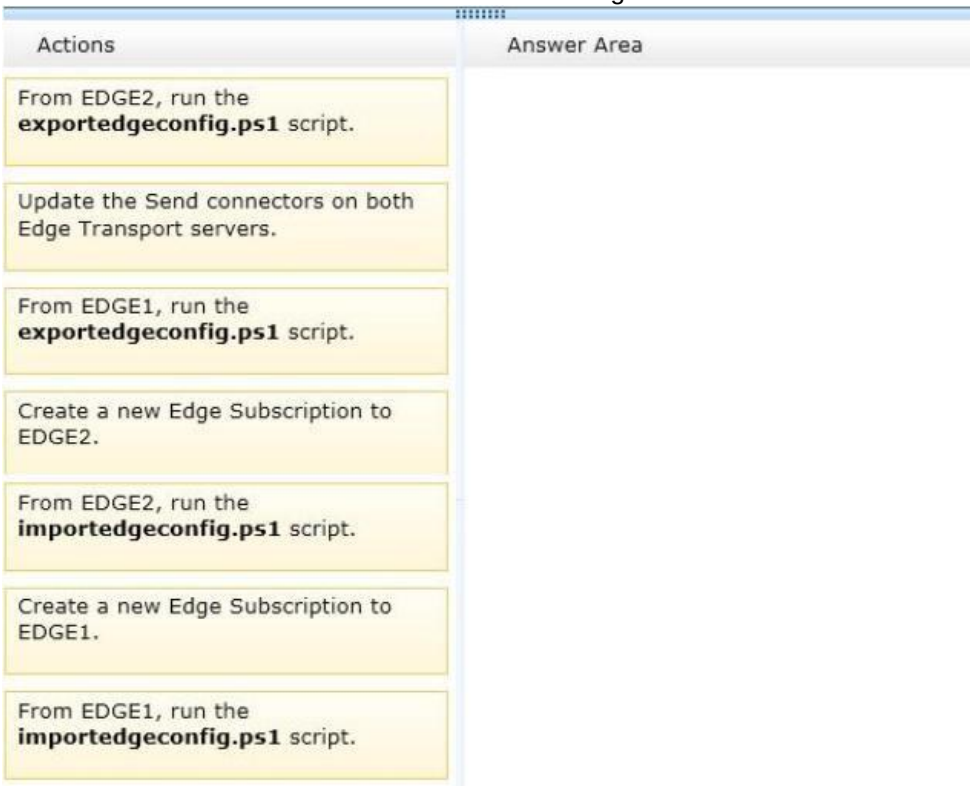
service on Mailbox servers or for Edge Transport servers. This example sets the DelayNotificationTimeout parameter to 13 hours on server named Mailbox01. Set-TransportServer Mailbox01 -DelayNotificationTimeout 13:00:00 Need Set-TransportConfig and the TLSReceiveDomainSecureList parameter to specify the domains from which you want to receive domain secured email by using mutual Transport Layer Security (TLS) authentication.
B
To activate SSL encryption on an Exchange server, you need a server certificate on the Client Access Server in each company. The client access server is the internet facing server in an organization. An SSL certificate is a digital certificate that authenticates the identity of the exchange server and encrypts information that is sent to the server using Secure Sockets Layer (SSL) technology.
Mailbox server certificates.
One key difference between Exchange 2010 and Exchange 2013 is that the certificates that are used on the Exchange 2013 Mailbox server are self-signed certificates. Because all clients connect to an Exchange 2013 Mailbox server through an Exchange 2013 Client Access server, the only certificates that you need to manage are those on the Client Access server. The Client Access server automatically trusts the self-signed certificate on the Mailbox server, so clients will not receive warnings about a self-signed certificate not being trusted, provided that the Client Access server has a non-self-signed certificate from either a Windows certification authority (CA) or a trusted third party. There are no tools or cmdlets available to manage self-signed certificates on the Mailbox server. After the server has been properly installed, you should never need to worry about the certificates on the Mailbox server.
D
Set-TransportConfig.
Use the Set-TransportConfig cmdlet to modify the transport configuration settings for the whole Exchange organization.
EXAMPLE 1
This example configures the Exchange organization to forward all DSN messages that have the DSN codes 5.7.1, 5.7.2, and 5.7.3 to the postmaster email account.
Set-TransportConfig -GenerateCopyOfDSNFor 5.7.1,5.7.2,5.7.3
The TLSReceiveDomainSecureList parameter specifies the domains from which you want to receive domain secured email by using mutual Transport Layer Security (TLS) authentication.
F
If you want to ensure secure, encrypted communication with a partner, you can create a Send connector that is configured to enforce Transport Layer Security (TLS) for messages sent to a partner domain. TLS provides secure communication over the Internet. Use the EAC to create a Send connector to send email to a partner, with TLS applied To create a Send connector for this scenario, log in to the EAC and perform the following steps:
- In the EAC, navigate to Mail flow > Send connectors, and then click Add.
- In the New send connector wizard, specify a name for the send connector and then select Partner for the Type.
- When you select Partner, the connector is configured to allow connections only to servers that authenticate with TLS certificates. Click Next.
- Verify that MX record associated with recipient domain is selected, which specifies that the connector uses the domain name system (DNS) to route mail. Click Next.
- Under Address space, click Add . In the Add domain window, make sure SMTP is listed as the Type. For Fully Qualified Domain Name (FQDN), enter the name of your partner domain. Click Save.
- For Source server, click Add . In the Select a server window, select a Mailbox server that will be used to send mail to the Internet via the Client Access server and click Add . After you've selected the server, click Add .
- Click OK.
- Click Finish.
Once you have created the Send connector, it appears in the Send connector list.
Send Connector.

In Microsoft Exchange Server 2013, a Send connector controls the flow of outbound messages to the receiving server. They are configured on Mailbox servers running the Transport service. Most commonly, you configure a Send connector to send outbound email messages to a smart host or directly to their recipient, using DNS. Exchange 2013 Mailbox servers running the Transport service require Send connectors to deliver messages to the next hop on the way to their destination. Send connectors that are created on Mailbox servers are stored in Active Directory and are available to all Mailbox servers running the Transport service in the organization.

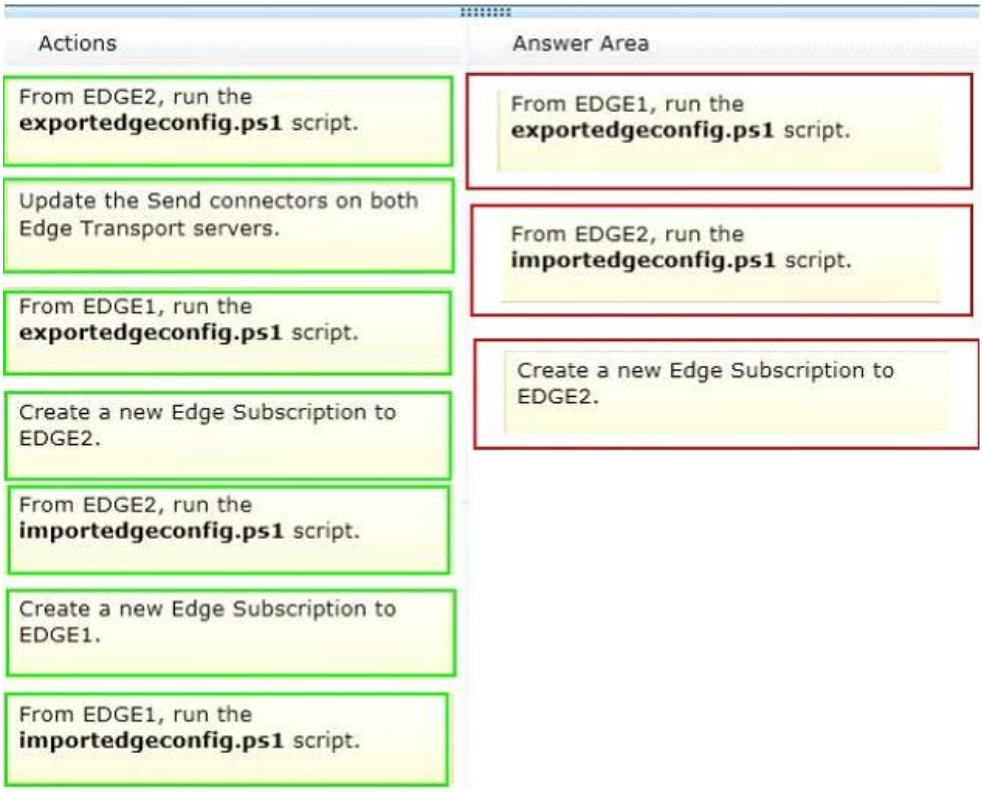
QUESTION 64

Drag and Drop Question

You are evaluating the implementation of a second Edge Transport server named EDGE2 in the Amsterdam office. You need to recommend which tasks must be performed to ensure that email messages can be sent by the organization if a single Edge Transport server fails. Which three actions should you include in the recommendation? To answer, move the three appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Answer:



QUESTION 65
You need to recommend which type of group must be used to create the planned department lists. Which type of group should you recommend?

A. Universal Distribution
B. Dynamic Distribution
C. Global Security
D. Universal Security

Answer: A
Explanation:
A
Universal Distribution.
Mail-enabled universal distribution groups (also called distribution groups) can be used only to distribute messages.
NOT B
A dynamic distribution group is a distribution group that uses recipient filters and conditions to derive its membership at the time messages are sent.
http://technet.microsoft.com/en-us/library/bb123722(v=exchg.150).aspx
Use the EAC to create a dynamic distribution group. As ExamTester from Netherlands commented below. But the Fabrikam case asks that users must be able to add and remove themselves from the distribution group. This is not possible using a dynamic group since membership is dynamically calculated based on attributes.
Use this explanation for NOT B.
http://technet.microsoft.com/en-us/library/bb201680(v=exchg.150).aspx
You can't use Exchange Server 2013 to create non-universal distribution groups. Mail-enabled non-universal groups were discontinued in Exchange Server 2007 and can exist only if they were

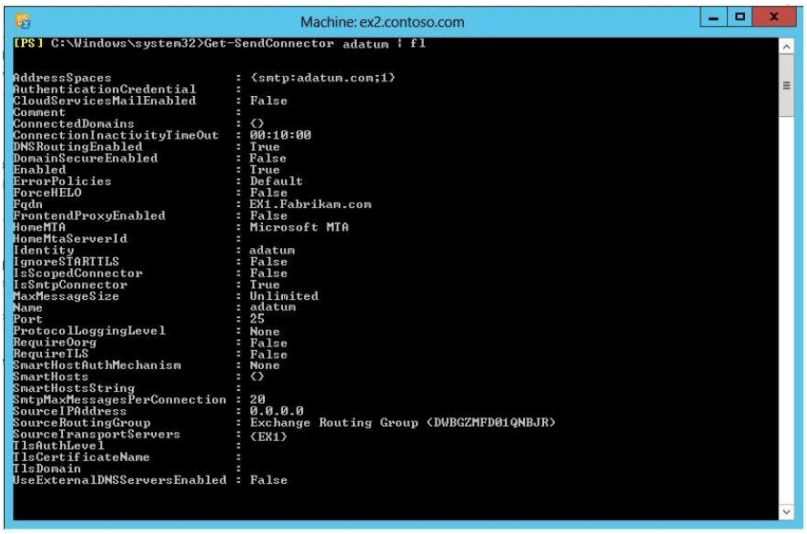
migrated from Exchange 2003 or earlier versions of Exchange. Seems to contradict the above.
NOT CD
In Exchange, all mail-enabled groups are referred to as distribution groups, whether they have a security context or not.

QUESTION 66
You need to recommend which tasks must be performed to meet the technical requirements of the research and development (R&D) department. Which two tasks should you recommend? (Each correct answer presents part of the solution. Choose two.)

A. Create a new global address list (GAL) and a new address book policy.
B. Modify the permissions of the default global address list (GAL), and then create a new GAL.
C. Run the Update AddressList cmdlet.
D. Run the Set-Mailbox cmdlet.
E. Create an OAB virtual directory.

Answer: AD
Explanation:
NOT B
Need an address book policy.
NOT C
Update AddressList cmdlet. Use the Update-AddressList cmdlet to update the recipients included in the address list that you specify.
EXAMPLE 1
This example updates the recipients of the address list building4 and under the container All Users\Sales.
Update-AddressList -Identity "All Users\Sales\building4"
NOT E
Will not resolve the issue. Need an address book policy and to assign this policy to users.
A
Address book policies (ABPs) allow you to segment users into specific groups to provide customized views of your organization's global address list (GAL). When creating an ABP, you assign a GAL, an offline address book (OAB), a room list, and one or more address lists to the policy. You can then assign the ABP to mailbox users, providing them with access to a customized GAL in Outlook and Outlook Web App. The goal is to provide a simpler mechanism to accomplish GAL segmentation for on-premises organizations that require multiple GALs.
D
After you create an address book policy (ABP), you must assign it to mailbox users. Users aren't assigned a default ABP when their user account is created. If you don't assign an ABP to a user, the global address list (GAL) for your entire organization will be accessible to the user through Outlook and Outlook Web App.
This example assigns the ABP All Fabrikam to the existing mailbox user joe@fabrikam.com.
Set-Mailbox -Identity joe@fabrikam.com -AddressBookPolicy "All Fabrikam"
Address Book Policies: Exchange Online Help.

QUESTION 67
You are testing the planned implementation of Domain Security. You discover that users fail to exchange domain-secured email messages. You open the Exchange Management Shell and discover the output shown in the exhibit. (Click the Exhibit button.) You need to ensure that users can exchange email messages by using Domain Security. Which two parameters should you modify by using the Set-SendConnector cmdlet? (Each correct answer presents part of the solution. Choose two.)



A. tlsauthlevel
B. requiretls
C. ignorestarttls
D. tlsdomain
E. domainsecureenabled
F. smarthostauthmechanism

Answer: BE
Explanation:
Domain Security.
Domain Security is a feature of Exchange Server (both 2010 and 2013) that can secure SMTP traffic between two Exchange organizations. It is implemented on server level, and it works without configuring any options on user (sender or recipient) side. Domain Security uses mutual TLS authentication to provide session-based authentication and encryption. Mutual TLS authentication is different from TLS as it's usually implemented. Usually, when you implement TLS, client will verify the server certificate, and authenticate the server, before establishing a connection. With mutual TLS authentication, each server verifies the connection with the other server by validating a certificate that's provided by that other server, so clients are not included at all. We establish secure SMTP channel between two Exchange Servers, usually over the Internet. Clients, Outlook and Outlook Web App, will be aware that Domain Security is established. Green icon with check mark will be shown on each messages exchanged between servers on which Domain Security is implemented.
Set-SendConnector.
Use the Set-SendConnector cmdlet to modify a Send connector.
EXAMPLE 1
This example makes the following configuration changes to the Send connector named Contoso.com Send Connector:
Sets the maximum message size limit to 10 MB.
Changes the connection inactivity time-out to 15 minutes.
Set-SendConnector "Contoso.com Send Connector" -MaxMessageSize 10MB -ConnectionInactivityTimeOut
00:15:00
PARAMETERS
Requiretls.
The RequireTLS parameter specifies whether all messages sent through this connector must be transmitted using TLS. The default value is $false.

Domainsecureenabled.
The DomainSecureEnabled parameter is part of the process to enable mutual Transport Layer Security (TLS) authentication for the domains serviced by this Send connector. Mutual TLS authentication functions correctly only when the following conditions are met:
- The value of the DomainSecureEnabled parameter must be $true.
- The value of the DNSRoutingEnabled parameter must be $true.
- The value of the IgnoreStartTLS parameter must be $false.
- The wildcard character (*) is not supported in domains that are configured for mutual TLS authentication.
- The same domain must also be defined on the corresponding Receive connector and in the TLSReceiveDomainSecureList attribute of the transport configuration.
The default value for the DomainSecureEnabled parameter is $false for the following types of Send connectors:
- All Send connectors defined in the Transport service on a Mailbox server.
- User-created Send connectors defined on an Edge server.
The default value for the DomainSecureEnabled parameter is $true for default Send connectors defined on an Edge server.
NOT TLSAUTHLEVEL.
The TlsAuthLevel parameter specifies the TLS authentication level that is used for outbound TLS connections established by this Send connector. Valid values are:
- EncryptionOnly: TLS is used only to encrypt the communication channel. No certificate authentication is performed.
- CertificateValidation: TLS is used to encrypt the channel and certificate chain validation and revocation lists checks are performed.
- DomainValidation: In addition to channel encryption and certificate validation, the Send connector also verifies that the FQDN of the target certificate matches the domain specified in the TlsDomain parameter. If no domain is specified in the TlsDomain parameter, the FQDN on the certificate is compared with the recipient's domain.
You can't specify a value for this parameter if the IgnoreSTARTTLS parameter is set to $true, or if the RequireTLS parameter is set to $false.
NOT IgnoreStarttls.
The IgnoreSTARTTLS parameter specifies whether to ignore the StartTLS option offered by a remote sending server. This parameter is used with remote domains. This parameter must be set to $false if the RequireTLS parameter is set to $true. Valid values for this parameter are $true or $false.
NOT TlsDomain.
The TlsDomain parameter specifies the domain name that the Send connector uses to verify the FQDN of the target certificate when establishing a TLS secured connection. This parameter is used only if the TlsAuthLevel parameter is set to DomainValidation. A value for this parameter is required if:
- The TLSAuthLevel parameter is set to DomainValidation.
- The DNSRoutingEnabled parameter is set to $false (smart host Send connector).
NOT SmartHostAuthMechanism.
The SmartHostAuthMechanism parameter specifies the smart host authentication mechanism to use for authentication with a remote server. Use this parameter only when a smart host is configured and the DNSRoutingEnabled parameter is set to $false. Valid values are None, BasicAuth, BasicAuthRequireTLS, ExchangeServer, and ExternalAuthoritative. All values are mutually exclusive. If you select BasicAuth or BasicAuthRequireTLS, you must use the AuthenticationCredential parameter to specify the authentication credential.

QUESTION 68
You need to recommend which recovery solution will restore access to all of the mailboxes in AccountingDB if EX1 fails. The solution must restore access to email messages as quickly as possible. Which recovery solution should you recommend?

A. On EX2, create a new mailbox database.
Restore the database files, and then mount the database.
Run the New-MailboxRestoreRequest cmdlet for all of the mailboxes in the database.
B. On EX2, create a new mailbox database.
Restore the database files, and then mount the database.
Run the Set-Mailbox cmdlet for all of the mailboxes in the database.
C. On replacement hardware, run setup /mode:recoverserver.
Restore the database files, and then mount the database.
Run the Set-Mailbox cmdlet.
D. On replacement hardware, run setup /mode:recoverserver.
Restore the database files, and then mount the database.
Run the New-MailboxRestoreRequest cmdlet for all of the mailboxes in the database.

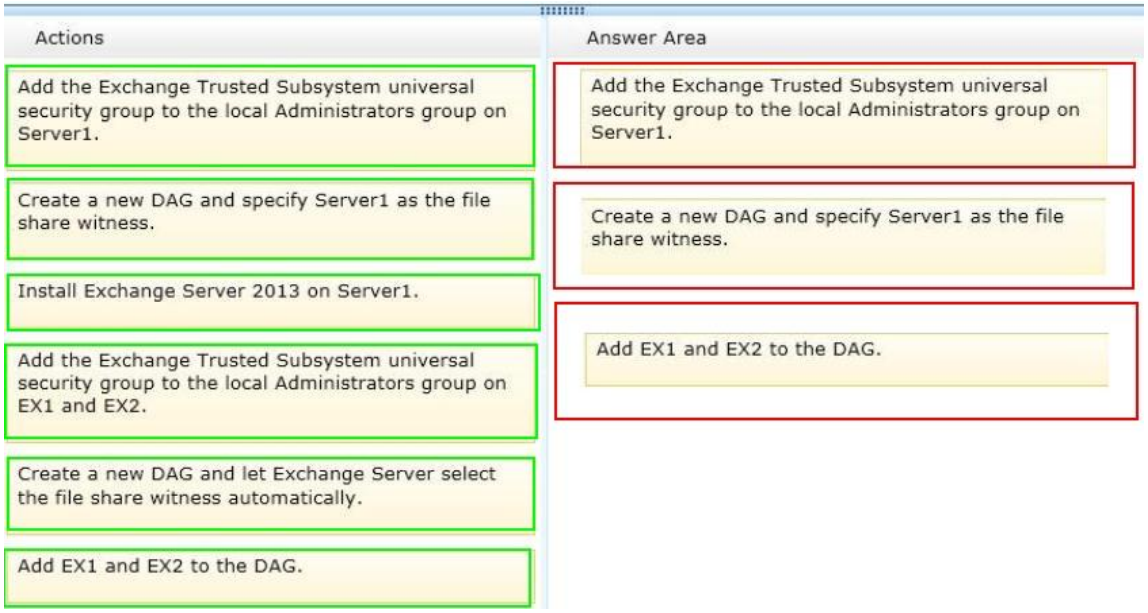
Answer: A
Explanation:
Restore Data Using a Recovery Database.
Create a Recovery Database.
http://technet.microsoft.com/en-us/library/ee332351%28v=exchg.150%29.aspx

QUESTION 69
Drag and Drop Question
You have an Exchange Server 2013 organization that contains two servers. The servers are configured as shown in the following table.

Server name	Server role
Ex1	Mailbox server Client Access server
Ex2	Mailbox server Client Access server

You need to create a new database availability group (DAG) that contains EX1 and EX2. Which three actions should you perform? To answer, move the three appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Answer:



QUESTION 70

You have an Exchange Server 2013 organization that contains one Client Access server. The Client Access server is accessible from the Internet by using a network address translation (NAT) device. You deploy an additional Client Access server. You also deploy an L4 hardware load balancer between the Client Access servers and the NAT device. After deploying the hardware load balancer, you discover that all of the Exchange Server traffic is directed to a single Client Access server. You need to ensure that the hardware load balancer distributes traffic evenly across both Client Access servers. What should you do?

A. Change the default route of the Client Access servers to point to the hardware load balancer.
B. Configure the NAT device to pass the original source IP address of all connections from the Internet.
C. Configure the Client Access servers to have a second IP address and web site.
Create the Exchange virtual directories in the new sites.
D. Configure SSL offloading on the hardware load balancer and the Client Access servers.

Answer: B

Explanation:

When using source NAT, the client IP address is not passed to the load balanced server. The insertion of the Client IP address into the header allows the exchange servers to see the IP that made the connection. Level 4 Load Balancer: A load balancer is a server computer with a very specialized operating system tuned to manage network traffic using user-created rules. Enterprises and hosting companies rely on load-balancing devices to distribute traffic to create highly available services L4 load balancing is fairly simple, two servers sharing the same IP address. You get redirected to the less-busy server. The most popular Layer 4 load balancing techniques are:

- round-robin
- weighted round-robin
- least connections
- weighted least connections

NOT A

http://pdfs.loadbalancer.org/Microsoft_Exchange_2013_Deployment_Guide.pdf

If there was no NAT device and the load balancer was completing the NAT translation then there maybe some merit in this answer option. B is a better answer given this scenario.

NOT C
No need to configure the Client Access servers to have a second IP address.
NOT D
Not required in this scenario. SSL offloading relieves a Web server of the processing burden of encrypting and/or decrypting traffic sent via SSL, the security protocol that is implemented in every Web browser. The processing is offloaded to a separate device designed specifically to perform SSL acceleration or SSL termination.
B
When using source NAT, the client IP address is not passed to the load balanced server. The insertion of the Client IP address into the header allows the exchange servers to see the IP that made the connection.
http://pdfs.loadbalancer.org/Microsoft_Exchange_2013_Deployment_Guide.pdf

QUESTION 71
You need to recommend a solution to resolve the issue for the London office users. What should you do?

A. Modify the properties of the OAB virtual directory.
B. Create a new address book policy.
C. Modify the properties of the default offline address book (OAB).
D. Create a new arbitration mailbox.

Answer: D
Explanation:
NOT A
Will not resolve the issue. Need to create a new arbirtration mailbox.
NOT B
Will not resolve the issue. Need to create a new arbirtration mailbox.
NOT C
Will not resolve the issue. Need to create a new arbirtration mailbox.
D
Exchange Server 2013 CAS role proxies the OAB download request to a "nearest" mailbox server hosting an active Organization Mailbox. Both London and New York host a mailbox server and a client access server. Therefore you need to create a new active Organization Mailbox Administrators can create additional Organization Mailboxes for fault tolerance or for serving users in a geographically disbursed Exchange deployment.
The Organization Mailbox.
The Organization Mailbox is a new type of arbitration mailbox introduced with Exchange 2013. The arbitration mailbox with persisted capability OrganizationCapabilityOABGen is referred to as Organization Mailbox. It plays a crucial role in OAB generation, storage and distribution. Each Exchange Server 2013 mailbox role hosting an Organization Mailbox will generate all Exchange 2013 OAB's defined in the environment. The OAB is generated in the Organization Mailbox first and later copied to the disk.
http://technet.microsoft.com/en-us/library/aa997663(v=exchg.150).aspx

QUESTION 72
You have an Exchange Server 2013 organization that contains five servers. All users connect to their mailbox by using a mobile device. All of the users in the finance department are in an organizational unit (OU) named OU1. You need to prevent the finance users from accessing the extended storage on their mobile device. What should you do?

A. Create a new mobile device mailbox policy, and then run the Set-CasMailbox cmdlet.
B. Create a new device access rule, and then run the Set-Mailbox cmdlet.
C. Create a new mobile device mailbox policy, and then run the Set-Mailbox cmdlet.

D. Create a new device access rule, and then run the Set-CasMailbox cmdlet.

Answer: A
Explanation:
Set-CASMailbox cmdlet.
Use the Set-CASMailbox cmdlet to set attributes related to client access for Microsoft Exchange ActiveSync, Microsoft Office Outlook Web App, POP3, and IMAP4 for a specified user. The Set-CASMailbox cmdlet operates on one mailbox at a time. You can configure properties for Outlook Web App, Exchange ActiveSync, POP3, and IMAP4 by using this cmdlet. You can configure a single property or multiple properties by using one statement.
Set-Mailbox cmdlet.
Use the Set-Mailbox cmdlet to modify the settings of an existing mailbox. You can use this cmdlet for one mailbox at a time.
Mobile device mailbox policy.
In Microsoft Exchange Server 2013, you can create mobile device mailbox policies to apply a common set of policies or security settings to a collection of users. After you deploy Exchange ActiveSync in your Exchange 2013 organization, you can create new mobile device mailbox policies or modify existing policies. When you install Exchange 2013, a default mobile device mailbox policy is created. All users are automatically assigned this default mobile device mailbox policy.
Device access rule.
Use device access rules to allow users to synchronize their mailboxes with specific mobile device families or models.
NOT BC
Use the Set-CASMailbox cmdlet to set attributes related to client access for Microsoft Exchange ActiveSync, Microsoft Office Outlook Web App, POP3, and IMAP4 for a specified user.
NOT D
In Microsoft Exchange Server 2013, you can create mobile device mailbox policies to apply a common set of policies or security settings to a collection of users.

QUESTION 73
You have an Exchange Server 2013 server that has a single mailbox database named DB1. You need to move the transaction log files of DB1. Which cmdlet should you run?

A. Move-DatabasePath
B. Move-Mailbox
C. Set-ExchangeServer
D. Set-MailboxDatabase

Answer: A

QUESTION 74
You have an Exchange Server 2013 organization named contoso.com. Your company is Investigating a user named User1. You need to prevent User1 from permanently deleting the items in his mailbox. What should you run?

A. Set-Mailbox User1 -LitigationHoldEnabled $true
B. Set-Mailbox User1 -ModerationEnabled $true
C. Set-Mailbox User1 -RetainDeletedItemsUntilBackup $true
D. Set-Mailbox User1 -RetentionHoldEnabled $true

Answer: A

QUESTION 75
You have an Exchange 2013 organization. You have an administrative user named Admin1. You need to ensure that Admin1 can move mailboxes in the organization. The solution must assign the minimum amount of permissions to Admin1. What should you do?

A. Create a local move request.
B. Create a custom Management role. Assign the role to Admin1.
C. Add Admin1 to the Organization Management role group.
D. Add Admin1 to the Recipient Management security group.

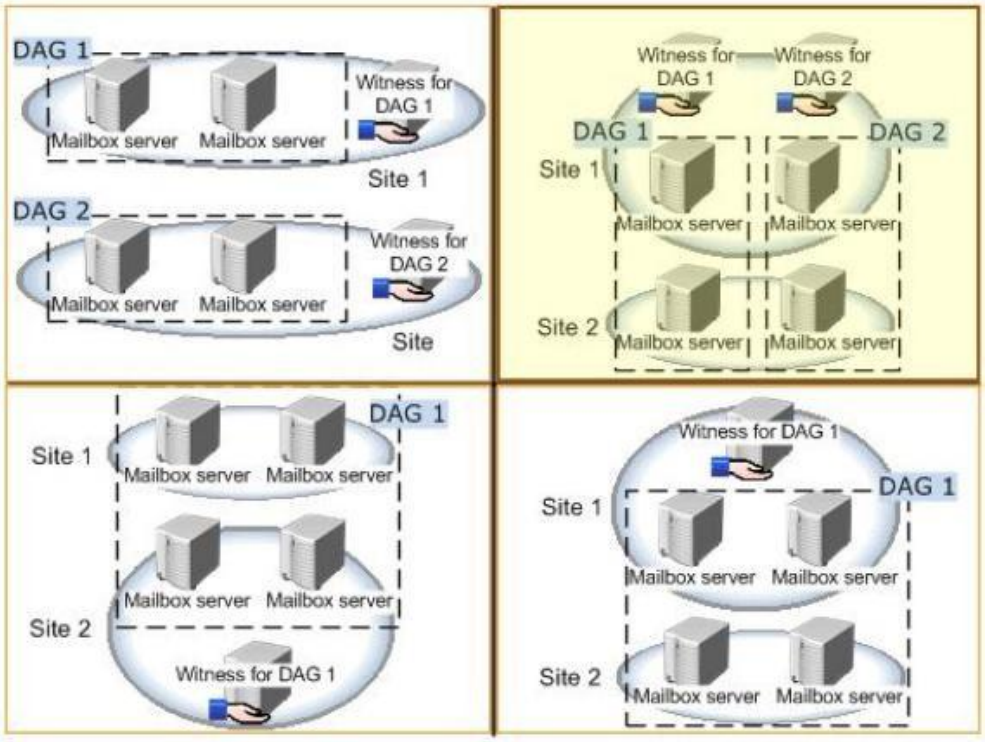
Answer: B

QUESTION 76
Hotspot Question
Your company has two offices. The offices are configured as shown in the following table.

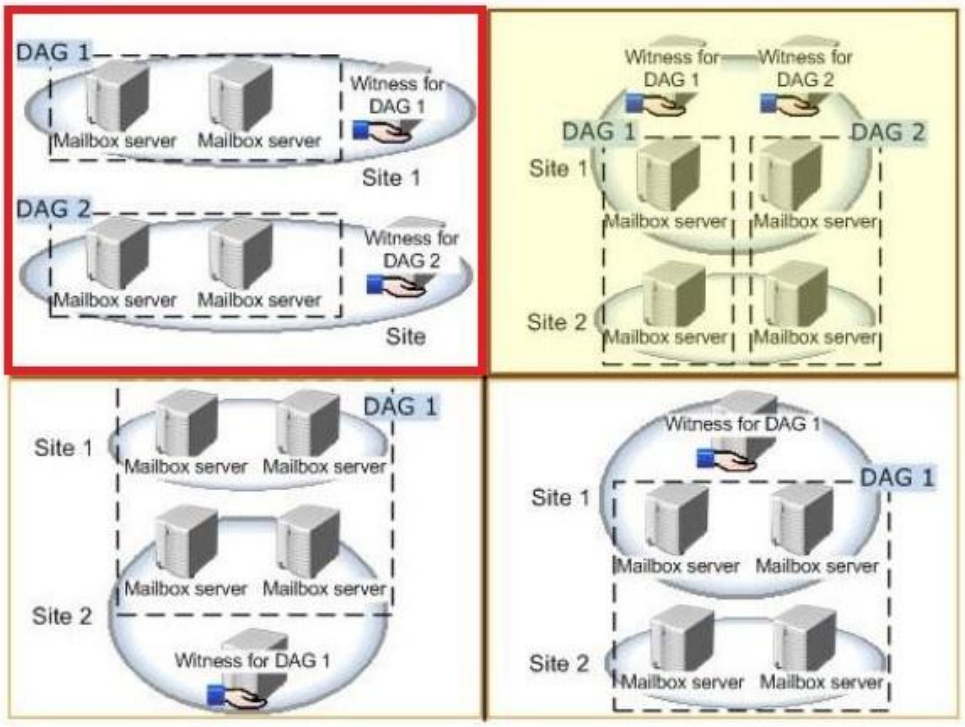
Office name	Number of users	Office site name
Office 1	2,000	Site 1
Office 2	2,000	Site 2

The offices connect to each other by using a WAN link that has a latency of more than 700 ms. You plan to deploy an Exchange Server 2013 organization to meet the following requirements:
- Ensure that users can access their mailbox if the WAN link fails.
- Ensure that users can access their mailbox if a single server fails.
- Ensure that users can access their mailbox if a single database fails.

You recommend deploying one or more database availability groups (DAGs) and mailbox database copies. You need to identify which design meets the requirements for the planned deployment. Which design should you identify? To answer, select the appropriate design in the answer area.



Answer:



Explanation:

File Share Witness.

The file share witness is used to establish a majority node set. This is done by create a share on a server that gets a little file place into it automatically. The server hosting the cluster resource (which in the DAG I think is the Primary Activation Manager server) keeps an open file lock on this file. The other servers see this open file lock and interpret this as meaning another cluster node is online, healthy, and available. A file share witness is used when the DAG contains an even number of servers within it. When you initially create the DAG you must specify the server and file location that will act as the file share witness regardless of how many servers are in the DAG (0 to start) to ensure that if you do add an even number of DAG members the FSW will be properly used.

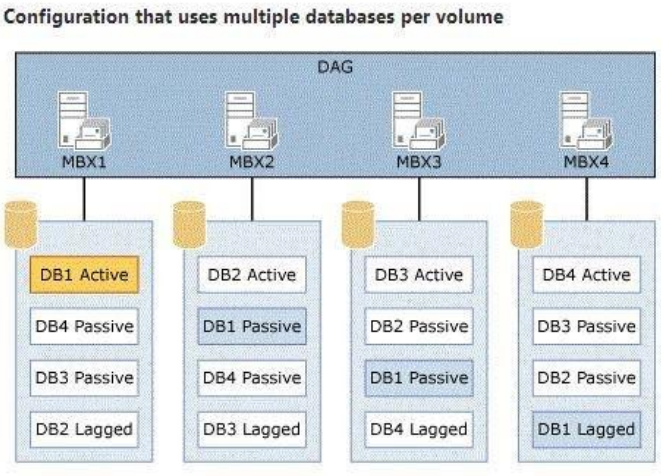
Database Availability Group.

A database availability group (DAG) is a set of up to 16 Microsoft Exchange Server 2013 Mailbox servers that provide automatic database-level recovery from a database, server, or network failure. When a Mailbox server is added to a DAG, it works with the other servers in the DAG to provide automatic, database-level recovery from database, server, and network failures. DAGs use continuous replication and a subset of Windows failover clustering technologies to provide high availability and site resilience. Mailbox servers in a DAG monitor each other for failures. When a Mailbox server is added to a DAG, it works with the other servers in the DAG to provide automatic, database-level recovery from database failures. When you create a DAG, it's initially empty, and a directory object is created in Active Directory that represents the DAG. The directory object is used to store relevant information about the DAG, such as server membership information. When you add the first server to a DAG, a failover cluster is automatically created for the DAG. In addition, the infrastructure that monitors the servers for network or server failures is initiated. The failover cluster heartbeat mechanism and cluster database are then used to track and manage information about the DAG that can change quickly, such as database mount status, replication status, and last mounted location. Witness server and witness directory The witness server is a server outside the DAG that acts as a quorum voter when the DAG contains an even number of members. The witness directory is a directory created and shared on the witness server for use by the system in maintaining a quorum.

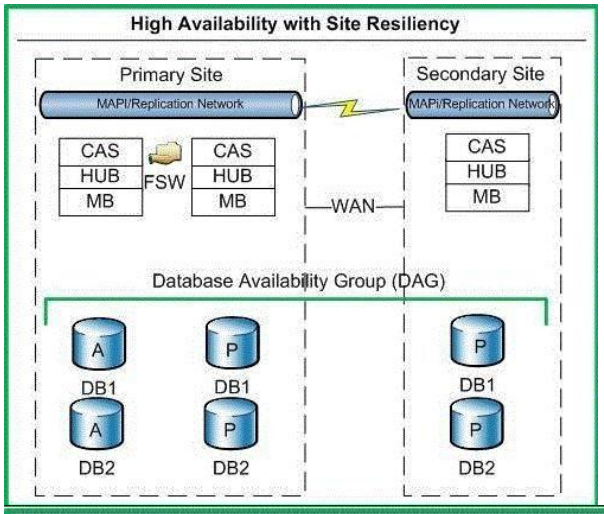
Lagged copy of a mailbox database.

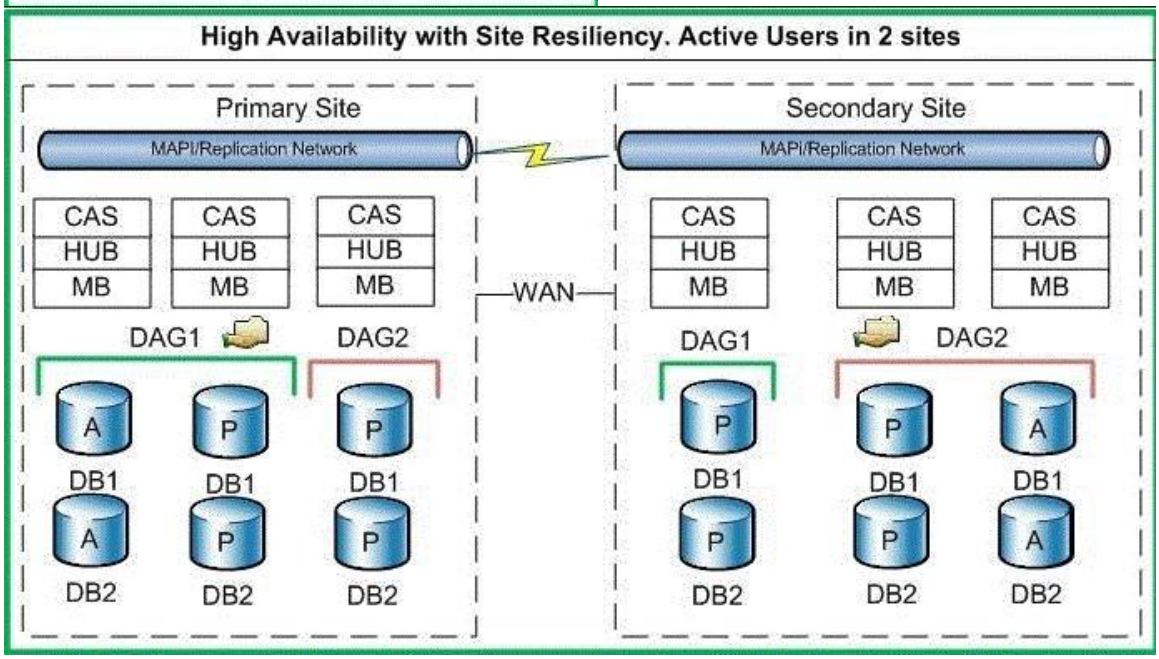
A Lagged Mailbox Database Copy is a mailbox database copy configured with a replay lag time

value greater than 0. A lagged database copy is one that is not updated by replaying transactions as they become available. Instead, the transaction logs are kept for a certain period and are then replayed. The lagged database copy is therefore maintained at a certain remove to the active database and the other non-lagged database copies. If you are planning to have more than two passive database copies of a database, think about a lagged copy also as an additional protection against unpredicted situations Lagged copies aren't considered highly available copies. Instead, they are designed for disaster recovery purposes, to protect against store logical corruption. The greater the replay lag time set, the longer the database recovery process. Depending on the number of log files that need to replayed during recovery, and the speed at which your hardware can replay them, it may take several hours or more to recover a database.



The above configuration provides a symmetrical design. All four servers have the same four databases all hosted on a single disk per server. The key is that the number of copies of each database that you have should be equal to the number of database copies per disk. In the above example, there are four copies of each database: one active copy, two passive copies, and one lagged copy. Because there are four copies of each database, the proper configuration is one that has four copies per volume. In addition, activation preference is configured so that it's balanced across the DAG and across each server. For example, the active copy will have an activation preference value of 1, the first passive copy will have an activation preference value of 2, the second passive copy will have an activation preference value of 3, and the lagged copy will have an activation preference value of 4.
Lagged mailbox database copy.
A passive mailbox database copy that has a log replay lag time greater than zero.
Crossed Lines
DAG Replication 1 and 2
Circled Areas
Site 1 and Site 2 (or DataCenter1 and DataCenter2)
WAN LINK between Site1 and Site2
High Availability with Site Resiliency Exchange 2010 Example.
http://jaworskiblog.com/2011/05/17/exchange-2010-design-principles-for-high-availability-and-site-resiliency/
FSW is the File Share Witness.





ASIDE
Windows NLB is not supported across sites. It is not recommended to use an HLB to load balance across sites.
PICTURE1 OFFERS THE BEST DESIGN IN ORDER TO MEET THE SPECIFIED CRITERIA. MORE FAULTS WITH THE OTHERS. PICTURE1 HOWEVER DOES NOT OFFER SITE RESILIENCY.
- Ensure that users can access their mailbox if the WAN link fails.
- Ensure that users can access their mailbox if a single server fails.
- Ensure that users can access their mailbox if a single database fails.

Picture1
The DAG is NOT extended across multiple data centers in a site resilience configuration. The design offers high availability within each site. However if a node fails or the wan link fails the respective file share witness for each DAG is still available unlike the other 3 configurations.
Picture2
The DAG is extended across multiple data centers in a site resilience configuration. No high availability within each site. If the wan link is unavailable the file share witness for Site2 would be unavailable This is a split brain scenario, both sites believe that they are the rightful owner of the

database, and thus would mount their respective DB's. This would cause a divergence in data. Email could be sent to either database leaving to a difference between the databases on the respective mailbox servers.
Picture3
The DAG is extended across multiple data centers in a site resilience configuration. FSW on Site2 in the event of a wan failure means that the servers cannot contact a FSW Even number of nodes on the respective site with an inability to contact the FSW. This is a split brain scenario, both sites believe that they are the rightful owner of the database, and thus would mount their respective DB's. This would cause a divergence in data. Email could be sent to either database leaving to a difference between the databases on the respective mailbox servers. A file share witness is used when the DAG contains an even number of servers within it. A Node Majority quorum model is used for DAGs with an odd number of members. A Node and File Share Majority quorum is used for DAGs with an even number of members. The DAG needs to be able to make Quorum. When 1 node fails in Site1 and the wan link is down,1 out of 2 nodes left is not a majority. Need to be able to connect to the file share witness to obtain a majority.
Picture4
DAG 1 across both sites provides site resiliency but FSW on Site1 in the event of a wan failure means that the servers cannot contact a FSW A file share witness is used when the DAG contains an even number of servers within it. Even number of nodes on the respective site with an inability to contact the FSW. This is a split brain scenario, both sites believe that they are the rightful owner of the database, and thus would mount their respective DB's. This would cause a divergence in data. Email could be sent to either database leaving to a difference between the databases on the respective mailbox servers. A file share witness is used when the DAG contains an even number of servers within it. A Node Majority quorum model is used for DAGs with an odd number of members. A Node and File Share Majority quorum is used for DAGs with an even number of members.

QUESTION 77
You deploy a server that has the Exchange Server 2013 Mailbox server role and Client Access server role installed. You need to configure anti-spam to meet the following requirements:
- Email messages sent from the Internet to a distribution list named Executives must be rejected.
- Email messages that contain the words casino and jackpot must be rejected, unless they were sent to legal@contoso.com.
Which three cmdlets should you run? (Each correct answer presents part of the solution. Choose three.)

A. Add ContentFilterPhrase
B. Set-ContentFilterConfig
C. Set-TransportConfig
D. Set-SenderReputationConfig
E. Set-RecipientFilterConfig

Answer: ABE
Explanation:
Add ContentFilterPhrase.
The Add-ContentFilterPhrase cmdlet adds phrases to the Allow or Block phrases list. Use the Add-ContentFilterPhrase cmdlet to define custom words for the Content Filter agent. A custom word is a word or phrase that the administrator sets for the Content Filter agent to evaluate the content of an e-mail message and apply appropriate filter processing.
Syntax
Examples:
EXAMPLE 1
This example adds the phrase Free credit report to the Block phrase list. Any messages that contain

this phrase will be marked as spam by the Content Filtering agent. Add-ContentFilterPhrase -Phrase "Free credit report" -Influence BadWord Set-ContentFilterConfig
Use the Set-ContentFilterConfig cmdlet to modify the content filter configuration on a Mailbox server or an Edge Transport server.
Syntax
Set-ContentFilterConfig [-BypassedRecipients <MultiValuedProperty>] [-BypassedSenderDomains <MultiValuedProperty>] [-BypassedSenders <MultiValuedProperty>] [-Confirm [<SwitchParameter>]] [-DomainController <Fqdn>] [-Enabled <$true | $false>] [-ExternalMailEnabled <$true | $false>] [-InternalMailEnabled <$true | $false>] [-OutlookEmailPostmarkValidationEnabled <$true | $false>] [-QuarantineMailbox <SmtpAddress>] [-RejectionResponse <AsciiString>] [-SCLDeleteEnabled <$true | $false>]
[-SCLDeleteThreshold <Int32>] [-SCLQuarantineEnabled <$true | $false>] [-SCLQuarantineThreshold <Int32>]
[-SCLRejectEnabled <$true | $false>] [-SCLRejectThreshold <Int32>] [-WhatIf [<SwitchParameter>]]
EXAMPLE 1
This example specifies the sender domain woodgrovebank.com as a bypassed domain. Messages received from that domain bypass the Content Filter agent.
Set-ContentFilterConfig -BypassedSenderDomains woodgrovebank.com Set-RecipientFilterConfig
Use the Set-RecipientFilterConfig cmdlet to enable and configure the Recipient Filter agent.
Syntax
Set-RecipientFilterConfig [-BlockedRecipients <MultiValuedProperty>] [-BlockListEnabled <$true | $false>] [-Confirm [<SwitchParameter>]] [-DomainController <Fqdn>] [-Enabled <$true | $false>] [-ExternalMailEnabled<$true | $false>] [-InternalMailEnabled <$true | $false>] [-RecipientValidationEnabled <$true | $false>] [-WhatIf
[<SwitchParameter>]]
EXAMPLE 1
This example modifies the Recipient Filter agent configuration so that recipient validation is enabled.
Set-RecipientFilterConfig -RecipientValidationEnabled $true
EXAMPLE 2
This example makes the following changes to the Recipient Filter agent configuration:
Enables the Blocked Recipients list.
Adds two users to the Blocked Recipients list.
Set-RecipientFilterConfig -BlockListEnabled $true lockedRecipients user1@contoso.com,user2@contoso.com
NOT C
Set-TransportConfig.
Use the Set-TransportConfig cmdlet to modify the transport configuration settings for the whole Exchange organization. This example configures the Exchange organization to redirect all journaling reports that can't be delivered to the journaling mailbox to the email account journalingndr@contoso.com.
Set-TransportConfig -JournalingReportNdrTo journalingndr@contoso.com
NOT D
Set-SenderReputationConfig.
Use the Set-SenderReputationConfig cmdlet to modify the sender reputation configuration on a Mailbox server or an Edge Transport server. Sender reputation is part of the Exchange anti-spam functionality that blocks messages according to many characteristics of the sender. Sender reputation relies on persisted data about the sender to determine what action, if any, to take on an inbound message. The Protocol Analysis agent is the underlying agent for sender reputation functionality. When you configure anti-spam agents on an Exchange server, the agents act on messages cumulatively to reduce the number of unsolicited messages that enter the organization.
Syntax
EXAMPLE 1
This example makes the following modifications to the sender reputation configuration:

It sets the sender reputation action to block all senders whose sender reputation level (SRL) rating exceeds the SRL threshold. It sets the SRL blocking threshold to 6. It sets the number of hours that senders are put on the blocked senders list to 36 hours.
Set-SenderReputationConfig -SenderBlockingEnabled $true -SrlBlockThreshold 6 -SenderBlockingPeriod 36

QUESTION 78
Your company named Contoso, Ltd., has an Exchange Server 2013 organization named contoso.com. The network contains an Active Directory domain. The domain contains an organizational unit (OU) named SalesOU. SalesOU contains two users named User1 and User2. Contoso purchases a domain name adatum.com. You need to change the primary SMTP address of all the users in SalesOU to use the SMTP suffix of adatum.com. The solution must not remove the contoso.com email address. Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

A. Create a new email address policy and apply the policy to the users in SalesOU.
B. Change the default email address policy to include adatum.com.
C. Create a new remote domain for adatum.com.
D. Create a new accepted domain for adatum.com and set the domain type to Authoritative Domain.
E. Create a new accepted domain for adatum.com and set the domain type to External RelayDomain.

Answer: AD
Explanation:
Email Address Policies.
Applies to: Exchange Server 2013.
Recipients (which include users, resources, contacts, and groups) are any mail-enabled object in Active Directory to which Microsoft Exchange can deliver or route messages. For a recipient to send or receive email messages, the recipient must have an email address. Email address policies generate the primary and secondary email addresses for your recipients so they can receive and send email. By default, Exchange contains an email address policy for every mail-enabled user. This default policy specifies the recipient's alias as the local part of the email address and uses the default accepted domain. The local part of an email address is the name that appears before the at sign (@). However, you can change how your recipients' email addresses will display. For example, you can specify that the addresses display as firstname.lastname@contoso.com. Furthermore, if you want to specify additional email addresses for all recipients or just a subset, you can modify the default policy or create additional policies. For example, the user mailbox for David Hamilton can receive email messages addressed to hdavid@mail.contoso.com and hamilton.david@mail.contoso.com. Looking for management tasks related to email address policies See Email Address Policy Procedures.
NOT B
No need to change the default email policy. Create a new email address policy.
NOT C
No need for a remote domain. You can create remote domain entries to define the settings for message transfer between the Microsoft Exchange Server 2013 organization and domains outside your Exchange organization. When you create a remote domain entry, you control the types of messages that are sent to that domain. You can also apply message format policies and acceptable character sets for messages that are sent from users in your organization to the remote domain. The settings for remote domains are global configuration settings for the Exchange organization. The remote domain settings are applied to messages during categorization in the Transport service on Mailbox servers. When recipient resolution occurs, the recipient domain is matched against the configured remote domains. If a remote domain configuration blocks a specific message type from being sent to recipients in that domain, the message is deleted. If you specify a particular message format for the remote domain, the message headers and content are modified. The settings apply to all messages that are processed by the Exchange organization.

NOT E

Do not want to use a relay server. When you configure an external relay domain, messages are relayed to an email server that's outside your Exchange organization and outside the organization's network perimeter. Typically, most Internet-facing messaging servers are configured to not allow for other domains to be relayed through them. However, there are scenarios where you may want to let partners or subsidiaries relay email through your Exchange servers. In Exchange 2013, you can configure accepted domains as relay domains. Your organization receives the email messages and then relays the messages to another email server. You can configure a relay domain as an internal relay domain or as an external relay domain. These two relay domain types are described in the following sections.

A

Need to create a new email address policy.

D

There are three types of accepted domains: authoritative, internal relay, and external relay. Configure an Accepted Domain within Your Exchange Organization as Authoritative Applies to: Exchange Server 2013 If a domain belonging to your organization hosts mailboxes for all the recipients within an SMTP namespace, that domain is considered to be authoritative. By default, one accepted domain is configured as authoritative for the Exchange organization. If your organization has more than one SMTP namespace, you can configure more than one accepted domain as authoritative.

Configure an Accepted Domain within Your Exchange Organization as Authoritative: Exchange 2013 Help.

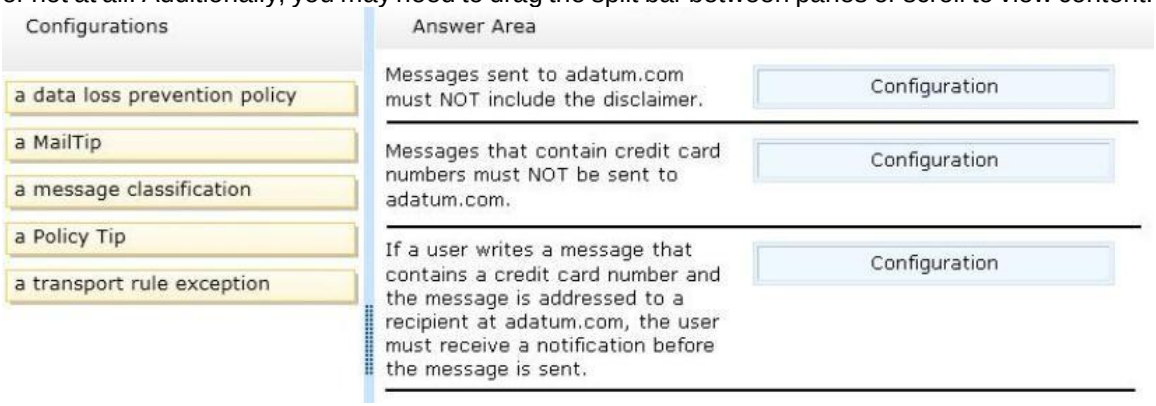
QUESTION 79

Drag and Drop Question

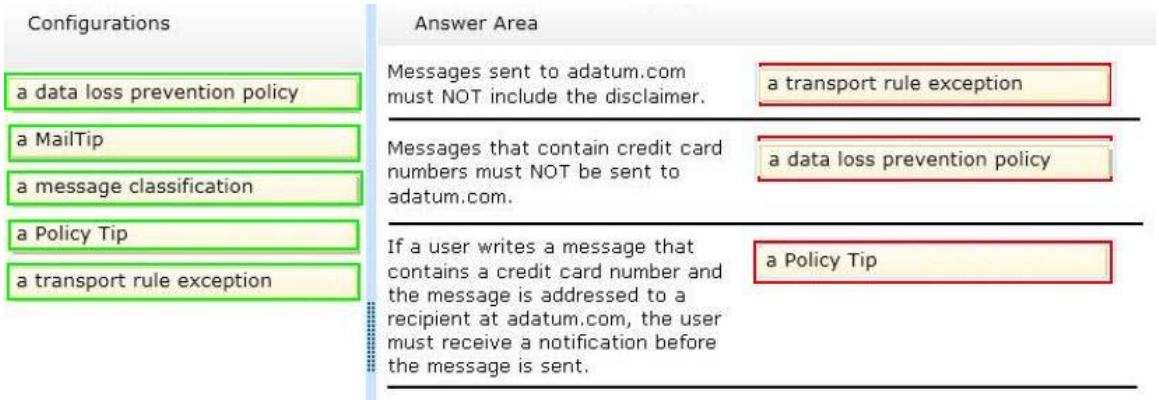
You have an Exchange Server 2013 organization named Contoso. The organization is configured to apply a disclaimer to all email messages sent to external recipients. Your company works with a partner company named A. Datum Corporation. A. Datum has an SMTP domain named adatum.com. You need to ensure that email messages sent to adatum.com meet the following compliance requirements:

- Messages sent to adatum.com must NOT include the disclaimer.
- Messages that contain credit card numbers must NOT be sent to adatum.com.
- If a user writes a message that contains a credit card number and the message is addressed to a recipient at adatum.com, the user must receive a notification before the message is sent.

What should you configure for each requirement? To answer, drag the appropriate configuration to the correct requirement in the answer area. Each configuration may be used once, more than once, or not at all. Additionally, you may need to drag the split bar between panes or scroll to view content.

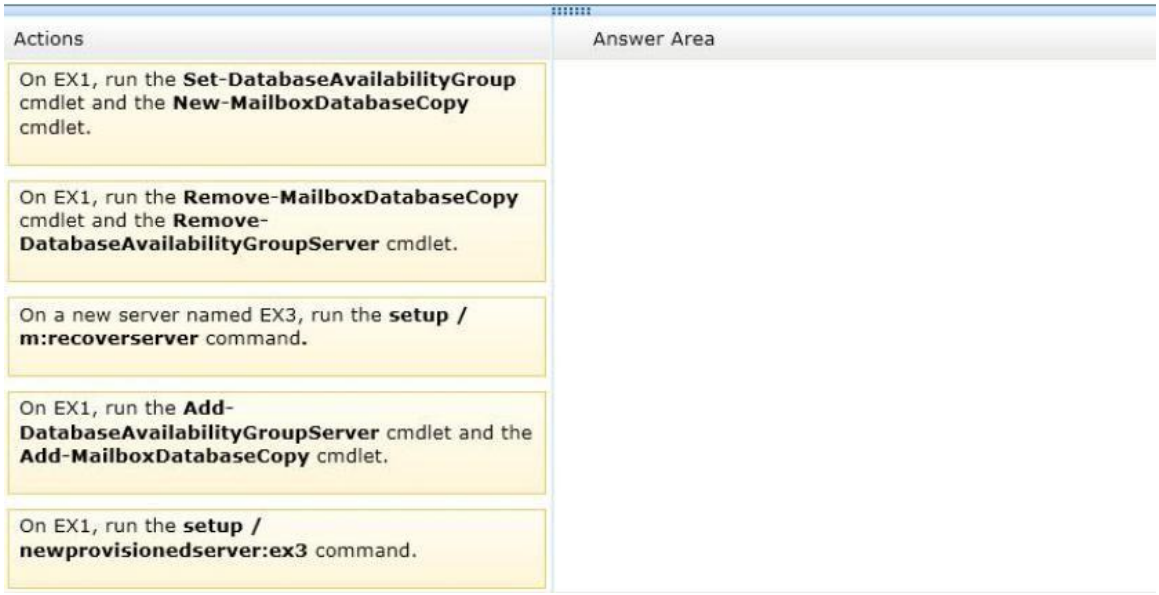


Answer:

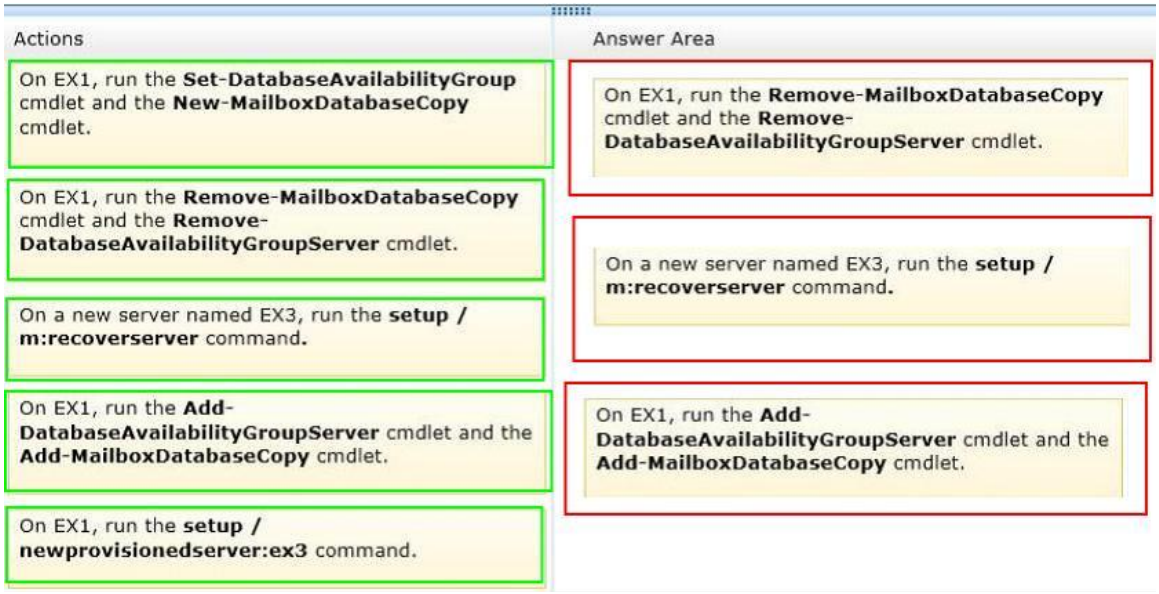


Explanation:
Box 1: A transport rule exception
Box 2: A data loss prevention policy
Box 3: a Policy Tip
Note:
- Each transport rule can have exceptions that specify what to exclude from the condition. Exceptions typically determine a subset of criteria identified in the condition. If you use transport rules, you can specify what information you don't want to enter or leave the organization, which individuals or groups shouldn't be able to communicate with one another, how messages are handled based on how they are classified by the sender, and more.
- The Data loss prevention (DLP) feature in the new Exchange will help you identify, monitor, and protect sensitive information in your organization through deep content analysis. DLP is increasingly important for enterprise message systems because business critical email includes sensitive data that needs to be protected. It's the financial information, personally identifiable information (PII) and intellectual property data that can be accidently sent to unauthorized users that keeps the CSO up all night.
- Policy Tip notification messages are displayed to users in Outlook while they are composing an email message. Policy Tip notification messages only show up if something about the sender's email message seems to violate a DLP policy that you have in place and that policy includes a rule to notify the sender when the conditions that you establish are met.
- Incorrect: MailTips are evaluated every time a sender adds a recipient to a message.
Reference: Introducing Data Loss Prevention in the New Exchange; Policy Tips

QUESTION 80
Drag and Drop Question
You have an Exchange Server 2013 organization that contains three servers named EX1, EX2, and EX3. The servers are members of a database availability group (DAG) named DAG1. A mailbox database named DB1 is replicated to all the members of DAG1. EX3 experiences a complete hardware failure. You need to restore EX3 on a new server. You reset the computer account for EX3. Which three actions should you perform next? To answer, move the three appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Answer:



Explanation:

Note: Use Setup /m:RecoverServer to recover a server.

Retrieve any replay lag or truncation lag settings for any mailbox database copies that exist on the server being recovered by using the Get-MailboxDatabase cmdlet.

(Box 1) Remove any mailbox database copies that exist on the server being recovered by using theRemove-MailboxDatabaseCopy cmdlet.

(Box 1) Remove the failed server's configuration from the DAG by using the Remove-DatabaseAvailabilityGroupServer cmdlet.

Reset the server's computer account in Active Directory. For detailed steps, see Reset a Computer Account.

(Box 2) Open a Command Prompt window. Using the original Setup media, run the following command:

Setup /m:RecoverServer

(Box 3) When the Setup recovery process is complete, add the recovered server to the DAG by

using the Add-DatabaseAvailabilityGroupServer cmdlet.
(Box 3) After the server has been added back to the DAG, you can reconfigure mailbox database copies by using the Add-MailboxDatabaseCopy cmdlet.
* You can recover a lost server by using the Setup /m:RecoverServer switch in Microsoft Exchange Server 2013. Most of the settings for a computer running Exchange 2013 are stored in Active Directory. The /m:RecoverServer switch rebuilds an Exchange server with the same name by using the settings and other information stored in Active Directory.
Reference: Recover a Database Availability Group Member Server

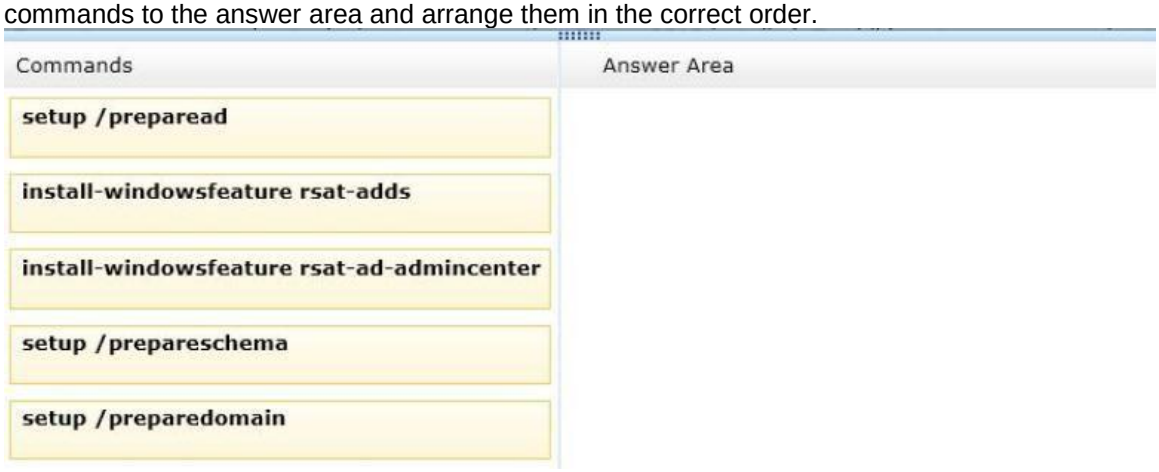
QUESTION 81
Your company has offices in Miami, Singapore and Montreal. An Active Directory site exists for each office. You have an Exchange Server 2013 organization that contains a server in each site. Each server has the Mailbox server role and the Client Access Server role installed. All users connect to the Miami servers to retrieve the public folder hierarchy. You need to create several public folders on the server in the Singapore office to meet the following requirements:
- Ensure that the public folders are available if a single Mailbox server fails.
- Ensure that the users in the Singapore office connect to their local server to retrieve the public folder hierarchy.
Which actions should you perform? (Each correct answer presents part of the solution. Choose all that apply.)

A. Create a new public folder mailbox.
B. Create a new public folder database.
C. Run the Add-MailboxDatabaseCopy cmdlet.
D. For each mailbox in the Singapore office, run the Set-Mailbox cmdlet and specify the-defaultpublicfoldermailbox parameter.
E. Run the Set-PublicFolderDatabase cmdlet.
F. For each public folder mailbox, run the Set-Mailbox cmdlet and specify the-defaultpublicfoldermailbox parameter.

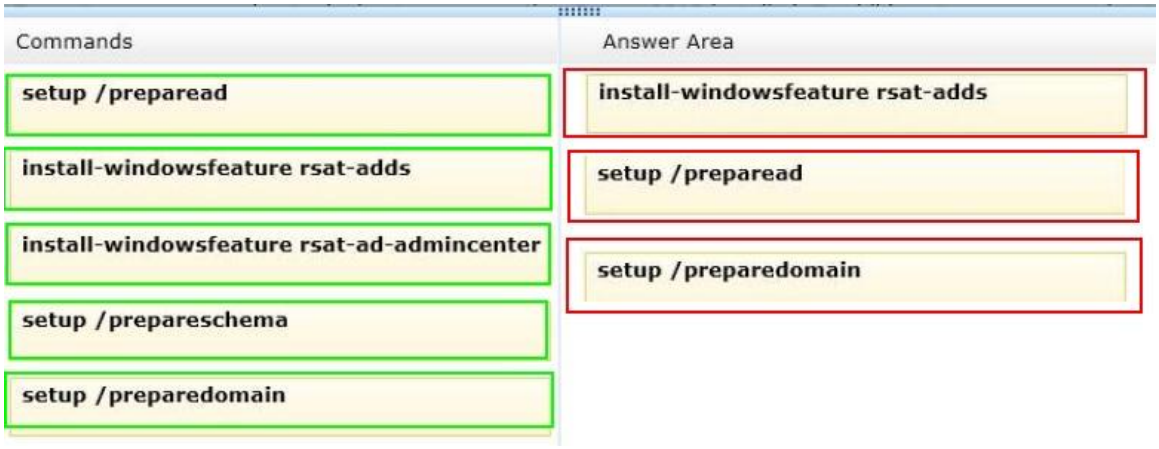
Answer: ACD
Explanation:
Public Folders.
Public folders can also be used as an archiving method for distribution groups. When you mail-enable a public folder and add it as a member of the distribution group, email sent to the group is automatically added to the public folder for later reference. Public folders are designed for shared access and provide an easy and effective way to collect, organize, and share information with other people in your workgroup or organization. Public folders help organize content in a deep hierarchy that's easy to browse. Users will see the full hierarchy in Outlook, which makes it easy for them to browse for the content they're interested in.
Public folder architecture.
In Exchange 2013, public folders were re-engineered using mailbox infrastructure to take advantage of the existing high availability and storage technologies of the mailbox database. Public folder architecture uses specially designed mailboxes to store both the public folder hierarchy and the content. This also means that there's no longer a public folder database. High availability for the public folder mailboxes is provided by a database availability group (DAG).
NOT B
In Exchange 2013, public folders were re-engineered using mailbox infrastructure to take advantage of the existing high availability and storage technologies of the mailbox database. Public folder architecture uses specially designed mailboxes to store both the public folder hierarchy and the content. This also means that there's no longer a public folder database. There is no database-level setting in Exchange 2013. Exchange 2013 has a mailbox-level ability to specify the public folder mailbox, but by default Exchange auto-calculates the per-user hierarchy mailbox.
NOT E

http://technet.microsoft.com/en-us/library/aa997225(v=exchg.141).aspx
Use the Set-PublicFolderDatabase cmdlet to set attributes of public folder databases (Exchange Server 2010). There's no longer a public folder database in Exchange Server 2013. There is no database-level setting in Exchange 2013. Exchange 2013 has a mailbox-level ability to specify the public folder mailbox, but by default Exchange auto-calculates the per-user hierarchy mailbox.
NOT F
Need to set it in the Singapore Office. Miami users still use the Miami servers to connect to the public folder hiearchy.
A
Need to create a public folder mailbox in the Singapore office. Public folder architecture uses specially designed mailboxes to store both the public folder hierarchy and the content. This also means that there's no longer a public folder database.
C
Use the Add-MailboxDatabaseCopy cmdlet to create a passive copy of an existing active mailbox database. The specified Mailbox server must be in the same database availability group (DAG), and the DAG must have quorum and be healthy.
D
Use the Set-MailboxServer cmdlet to modify attributes on a computer running Microsoft Exchange Server 2013 with the Mailbox server role installed. In Exchange 2007 and Exchange 2010, you could specify which users had access to specific public folders. In Exchange 2013, you can set the default public folder mailbox per user. To do so, run the Set-Mailbox cmdlet with the DefaultPublicFolderMailbox parameter. This ensures that the users in the Singapore office connect to their local server to retrieve the public folder hierarchy.

QUESTION 82
Drag and Drop Question
Your company plans to deploy an Exchange Server 2013 organization. The network contains an Active Directory forest. The forest contains two domains named contoso.com and child.contoso.com. The forest contains one Active Directory site. To contoso.com, you plan to deploy two servers that have Exchange Server 2013 installed. To child.contoso.com, you plan to deploy two servers that have Exchange Server 2013 installed. To the contoso.com domain, you deploy a new member server named Server1 that runs Windows Server 2012. You need to prepare the forest for the planned deployment of Exchange Server 2013. Which three commands should you run from Server1? To answer, move the three appropriate commands from the list of commands to the answer area and arrange them in the correct order.



Answer:



QUESTION 83
You have an Exchange Server 2013 organization. You need to ensure that an administrator named Admin1 receives a daily email message that contains a log of all the Exchange Server administrative actions. Which cmdlet should you use in a scheduled task?

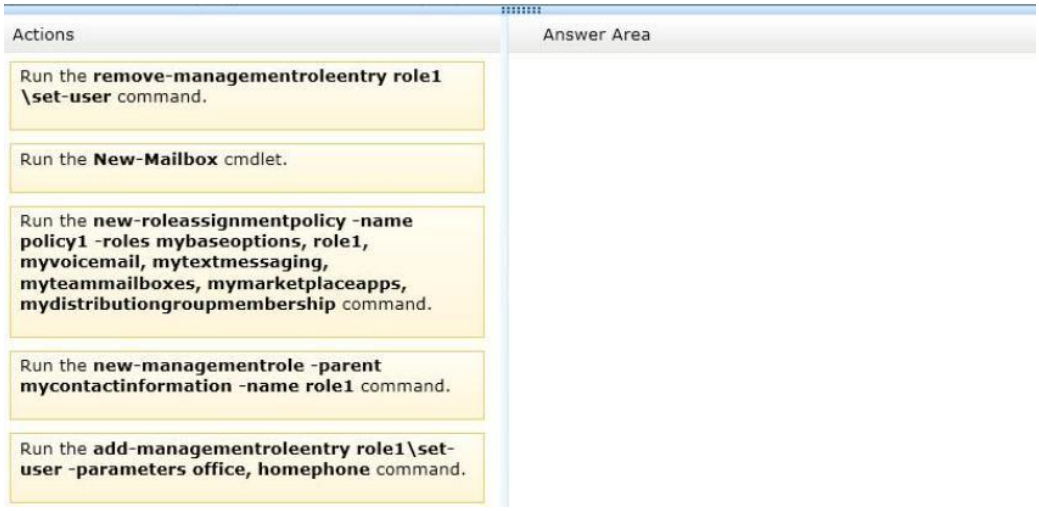
A. Set-AdminAuditLogConfig
B. Write-AdminAuditLog
C. New-AdminAuditLogSearch
D. Search-AdminAuditLog

Answer: C
Explanation:
New-AdminAuditLogSearch: Exchange 2013 Help

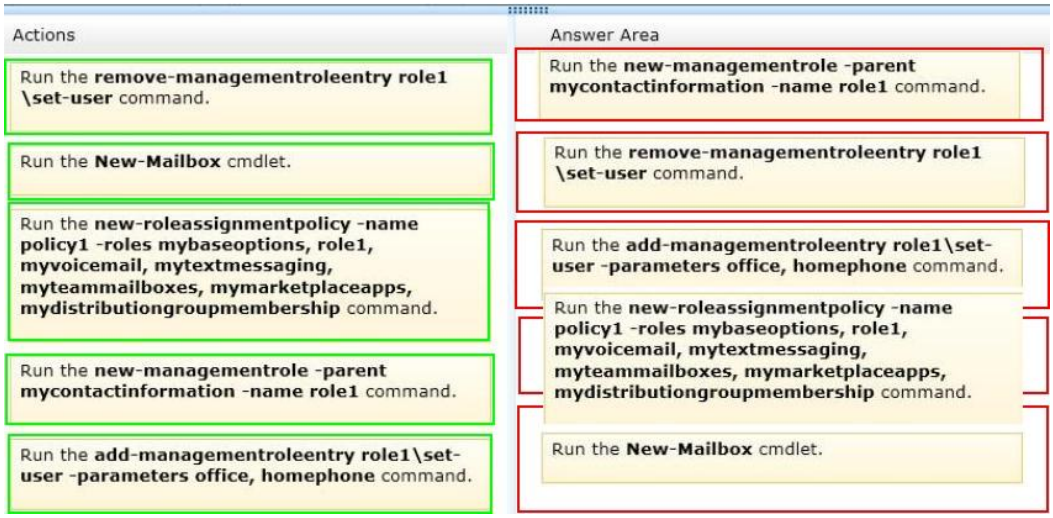
QUESTION 84
Drag and Drop Question
Your network contains four servers. The servers are configured as shown in the following table.

Server name	Server role	Exchange Server version
EX1	Mailbox server Client Access server	Exchange Server 2013
EX2	Mailbox server Client Access server	Exchange Server 2013
EX3	Mailbox server Client Access server	Exchange Server 2013
EX4	Mailbox server Client Access server Hub Transport server	Exchange Server 2010

You create a new user account for a temporary user named User1. You plan to create a new mailbox for User1. You need to recommend which actions must be performed to ensure that User1 can modify only the values of his home phone number attribute and his office location attribute. In which order should you perform the actions? To answer, move all actions from the list of actions to the answer area and arrange them in the correct order.



Answer:



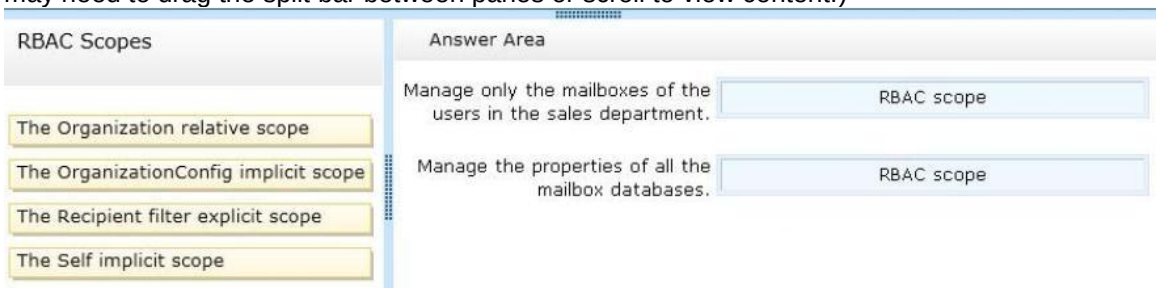
QUESTION 85

Drag and Drop Question

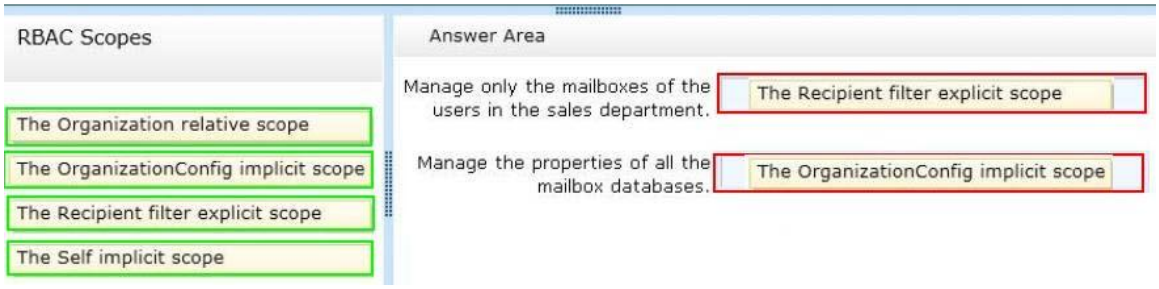
You have an Exchange Server 2013 organization that contains several custom RBAC management roles. You need to identify which RBAC scopes must be used to meet the following requirements:

- Manage only the mailboxes of the users in the sales department.
- Manage the properties of all the mailbox databases.

Which RBAC scopes should you identify? (To answer, drag the appropriate RBAC scopes to the correct requirements. Each RBAC scope may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.)



Answer:



Explanation:

http://technet.microsoft.com/en-us/library/dd335146(v=exchg.150).aspx

Management role scopes enable you to define the specific scope of impact or influence of a management role when a management role assignment is created. When you apply a scope, the role assignee assigned to the role can only modify the objects contained within that scope. A role assignee can be a management role group, management role, management role assignment policy, user, or universal security group (USG). Every management role, whether it's a built-in role or a custom role, has management scopes. Management scopes can be either of the following:

- Regular

A regular scope isn't exclusive. It determines where, in Active Directory, objects can be viewed or modified by users assigned the management role. In general, a management role indicates what you can create or modify, and a management role scope indicates where you can create or modify. Regular scopes can be either implicit or explicit scopes, both of which are discussed later in this topic.

- Exclusive

An exclusive scope behaves almost the same as a regular scope. The key difference is that it enables you to deny users access to objects contained within the exclusive scope if those users aren't assigned a role associated with the exclusive scope. All exclusive scopes are explicit scopes, which are discussed later in this topic.

Scopes can be inherited from the management role, specified as a predefined relative scope on a management role assignment, or created using custom filters and added to a management role assignment. Scopes inherited from management roles are called implicit scopes while predefined and custom scopes are called explicit scopes. Implicit scopes are the default scopes that apply to a management role type. Because implicit scopes are associated with a management role type, all of the parent and child management roles with the same role type also have the same implicit scopes. Implicit scopes apply to both built-in management roles and also to custom management roles. Implicit scopes defined on management roles.

Implicit scopes Description.

Organization If Organization is present in the role's recipient write scope, the role can create or modify recipient objects across the Exchange organization. If Organization is present in the role's recipient read scope, roles can view any recipient object across the Exchange organization. This scope is used only with recipient read and write scopes. MyGAL If MyGAL is present in the role's recipient write scope, the role can view the properties of any recipient within the current user's global address list (GAL). If MyGAL is present in the role's recipient read scope, the role can view the properties of any recipient within the current GAL. This scope is used only with recipient read scopes. Self If Self is present in the role's recipient write scope, the role can modify only the properties of the current user's mailbox. If Self is present in the role's recipient read scope, the role can view only the properties of the current user's mailbox. This scope is used only with recipient read and write scopes.

MyDistributionGroups.

If MyDistributionGroups is present in the role's recipient write scope, the role can create or modify distribution list objects owned by the current user. If MyDistributionGroups is present in the role's recipient read scope, the role can view distribution list objects owned by the current user. This scope is used only with recipient read and write scopes.

OrganizationConfig.

If OrganizationConfig is present in the role's configuration write scope, the role can create or modify any server or database configuration object across the Exchange organization. If OrganizationConfig is present in the role's configuration read scope, the role can view any server or database configuration object across the Exchange organization. This scope is used only with configuration read and write scopes. None If None is in a scope, that scope isn't available to the role. For example, a role that has None in the recipient write scope can't modify recipient objects in the Exchange organization. Explicit scopes are scopes that you set yourself to control which objects a management role can modify. Although implicit scopes are defined on a management role, explicit scopes are defined on a management role assignment. This enables the implicit scopes to be applied consistently across all management roles unless you choose to use an overriding explicit scope. For more information about management role assignments, see Understanding Management Role Assignments. Explicit scopes override the implicit write and configuration scopes of a management role. They don't override the implicit read scope of a management role. The implicit read scope continues to define what objects the management role can read.

Explicit scopes are useful when the implicit write scope of a management role doesn't meet the needs of your business. You can add an explicit scope to include nearly anything you want as long as the new scope doesn't exceed the bounds of the implicit read scope. The cmdlets that are part of a management role must be able to read information about the objects or containers that contain objects for the cmdlets to create or modify objects. For example, if the implicit read scope on a management role is set to Self, you can't add an explicit write scope of Organization because the explicit write scope exceeds the bounds of the implicit read scope.

The OrganizationConfig implicit scope.

If OrganizationConfig is present in the role's configuration write scope, the role can create or modify any server or database configuration object across the Exchange organization. If OrganizationConfig is present in the role's configuration read scope, the role can view any server or database configuration object across the Exchange organization.

CAN MANAGE THE PROPERTIES OF ALL OF THE MAILBOX DATABASES

The Self Implicit Scope If Self is present in the role's recipient write scope, the role can modify only the properties of the current user's mailbox. If Self is present in the role's recipient read scope, the role can view only the properties of the current user's mailbox.

CANNOT BE SELF AS IT PERTAINS TO ONLY THE PARTICULAR USER'S MAILBOX

The Organization relative scope.

If Organization is present in the role's recipient write scope, the role can create or modify recipient objects across the Exchange organization. If Organization is present in the role's recipient read scope, roles can view any recipient object across the Exchange organization. This scope is used only with recipient read and write scopes.

NOT MEANT FOR MANAGING MAILBOX DATABASES

A recipient is any mail-enabled object in the Active Directory directory service to which Exchange can deliver or route messages. In Microsoft Exchange recipients are comprised of mailbox users, mail-enabled users, mail contacts, distribution groups, security groups, dynamic distribution groups, and mail-enabled public folders.

The Recipient filter explicit scope.

Recipient filter scopes use filters to target specific recipients based on recipient type or other recipient properties such as department, manager, location, and more.

CAN TARGET THE USERS IN THE SALES DEPARTMENT

QUESTION 86

Drag and Drop Question

You have an Exchange Server 2007 organization. You are migrating the organization to Exchange Server 2013. The migration will last eight weeks. All servers are in a site named Site1. The servers in the organization are configured as shown in the following table. Users who have mailboxes on all of the servers will access Outlook Anywhere by using the mail.adatum.com name. You need to recommend which servers must be associated to the autodiscover.adatum.com and mail.adatum.com names. Which servers should you identify for each name? (To answer, drag the

appropriate servers to the correct names. Each server may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.)

Answer:

Explanation:

INCOMPLETE INFORMATION.

MAKES IT TOO DIFFICULT TO EVEN GUESS HOW TO ARRIVE AT THE CORRECT ANSWER MAY DEPEND ON THE TYPE OF SERVER (MAILBOX OR CLIENT ACCESS SERVER THAT IS IN USE OR THE VERSION OF OUTLOOK BEING USED. TO DETERMINE IF AUTODISCOVER CAN BE UTILISED ON THAT PARTICULAR SERVER. WHEN CAN YOU USE AUTODISCOVER WHEN CAN YOU NOT USE AUTODISCOVER.

Autodiscover.

Exchange Autodiscover is a service which is run on Exchange Client Access Servers. It is one of the new features it included in exchange 2007+ The Autodiscover service makes it easier to configure Outlook 2007 ,Outlook 2010 + and some mobile phones. Autodiscover Service cannot be used with earlier versions of Outlook, including Outlook 2003. In earlier versions of Microsoft Exchange (Exchange 2003 SP2 or earlier) and Outlook (Outlook 2003 or earlier), you had to configure all user profiles manually to access Exchange. The Autodiscover service uses a user's e-mail address and password to automatically configure a user's profile. Using the e-mail address, the Autodiscover service provides the following information to the client:

- The user's display name.
- Separate connection settings for internal and external connectivity.

- The location of the user's Mailbox server.
- The URLs for various Outlook features that manage functionality such as OOF, free/busy information, Unified Messaging, and the offline address book.
- Outlook Anywhere server settings.

Additionally, a new Active Directory object named the service connection point (SCP) is created on the server where you install the Client Access server role. And Autodiscover information is stored in it. Exchange 2013 requires its Outlook clients support auto-discovery of the server; this is in part to help streamline cloud deployments of Exchange. Clients also have to support "Outlook Anywhere" access--remote procedure calls via HTTP--to connect to Exchange 2013 instead of using TCP-based RPCs as in older versions of Exchange. What actually happens after you have entered your details is that the client looks for autodiscover.yourdomain.com and attempts to retrieve the rest of the server configuration details from there.

QUESTION 87
You have an Exchange Server 2013 organization. All user mailboxes have an In-Place Archive enabled. You need to identify which email message types can be archived by using a retention policy. Which message type or types should you identify? (Each correct answer presents part of the solution. Choose all that apply.)

A. calendar items
B. mail items
C. note items
D. task items
E. contact items

Answer: BCE

QUESTION 88
Your company, Fabrikam Inc., has an Exchange Server 2013 organization. The organization that contains three servers named Server1, Server2, and Server3. Server1 and Server2 are members of a database availability group (DAG) named DAG1. DAG1 contains two mailbox databases. All databases are active on Server1 and replicate to Server2. You start an unplanned maintenance on Server1 and shut down Server1. You discover that the databases do not mount on Server2. You restart Server1 and the databases mount automatically on Server1. You need to identify what prevents the databases from switching over successfully to Server2. Which cmdlet should you run?

A. Test-ReplicationHealth
B. Test-OutlookConnectivity
C. Test-ServiceHealth
D. Get-AvailabilityReportOutage

Answer: A
Explanation:
The cmdlet is designed for the proactive monitoring of continuous replication and the continuous replication pipeline, the availability of Active Manager, and the health and status of the underlying cluster service, quorum, and network components. The Test-ReplicationHealth cmdlet can be run locally or remotely against any Mailbox server in a DAG.
NOT B
Test-OutlookConnectivity.
Use the Test-OutlookConnectivity cmdlet to test end-to-end Microsoft Outlook client connectivity in the Microsoft Exchange Server 2013 organization. This includes testing for Outlook Anywhere (RPC/HTTP) connections.
EXAMPLE 1

This example runs a protocol test from the Mailbox server.
Test-OutlookConnectivity -ProbeIdentity "OutlookSelfTestProbe"
NOT C
Use the Test-ServiceHealth cmdlet to test whether all the Microsoft Windows services that Exchange requires on a server have started. The Test-ServiceHealth cmdlet returns an error for any service required by a configured role when the service is set to start automatically and isn't currently running.
EXAMPLE 1
This example uses the Test-ServiceHealth command without parameters to test the services on the local server.
Test-ServiceHealth
NOT D
Use the Get-AvailabilityReportOutage cmdlet to return the daily downtime (if any) for each service entity and its overridden value (if set) to the overall reported availability for the day. For information about the parameter sets in the Syntax section below, see Syntax. This example returns all outages that occurred the previous day. This cmdlet always returns outages for one day.
Get-AvailabilityReportOutage

QUESTION 89
You have an Exchange Server 2010 organization named adatum.com. You deploy a server that has Exchange Server 2013 installed. You plan to install eight additional servers that have Exchange Server 2013 installed. You are a member of the Organization Management management role group. You hire a temporary Exchange administrator named Temp1. The company's security policy states that all external consultants must have the minimum number of required permissions on the network. You need to ensure that Temp1 can install a server named Server5. The solution must meet the requirements of the security policy. Which two tasks should you perform? (Each correct answer presents part of the solution. Choose two.)

A. Run setup and specify the /newprovisionedserver:Server5 parameter.
B. Add Temp1 to the Delegated Setup management role group.
C. Add Temp1 to the Exchange Server role group.
D. Create a new management role and a new role assignment policy.
E. Run setup and specify the /roles:temp1 parameter.

Answer: AB
Explanation:
NOT C
Unable to install a server given this management role. The Exchange Servers management role enables administrators to do the following on individual servers:
- Add and remove database availability groups and configure database copies
- Enable, disable and configure Unified Messaging services
- Modify transport configuration on Mailbox and Client Access servers
- Enable and disable Microsoft Outlook Anywhere on Client Access servers
- Modify Mailbox and Client Access server configuration
- Modify Outlook Anywhere configuration on Client Access servers
- Modify content filtering configuration on Mailbox servers
- Modify general Exchange server configuration
- Modify server monitoring configuration
- View the configuration for each server role
This management role is one of several built-in roles in the Role Based Access Control (RBAC) permissions model in Microsoft Exchange Server 2013. 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 2013 components, such as mailbox

databases, 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.
NOT D
No need to create a new management role.
NOT E
Need to use the /NewProvisionedServer parameter setup /roles command is OK for exchange 2007. With temp1 appears to be an invalid command and not applicable to exchange 2013.
A
To delegate setup, you must first run Setup.com from a Command Prompt window with the /NewProvisionedServer parameter. This will not install Exchange on the server, but instead will create a placeholder object for the server in Active Directory and will add the machine account for this server to the Exchange Servers group.
B
Need to Add Temp1 to the Delegated Setup management role group.
Delegated Setup management role group.
The Delegated Setup 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 2013. 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 Delegated Setup role group can deploy servers running Exchange 2013 that have been previously provisioned by a member of the Organization Management role group. Members of the Delegated Setup role group can only deploy Exchange 2013 servers. They can't manage the server after it's been deployed. To manage a server after it's been deployed, a user must be a member of the Server Management role group. For more information about RBAC, see Understanding Role Based Access Control.

QUESTION 90
You have an Exchange Server 2013 organization that contains two Client Access servers named EX1 and EX2 and two Mailbox servers named EX3 and EX4. You have a firewall that controls all of the traffic between the internal network and the Internet. EX3 and EX4 are prevented from communicating with Internet hosts. EX1 and EX3 are in a site named Site1. EX2 and EX4 are in a site named Site2. All outbound email is sent through EX1. Site1 fails. You discover that email messages for the Internet are queued on EX4. You create a new send connector in Site2. You discover that all of the outbound email is queued on EX4 and is not delivered to the Internet. You verify that the client computers on the network can receive email messages from the Internet successfully. You need to ensure that the email messages are delivered successfully to the Internet. Which cmdlet should you run?

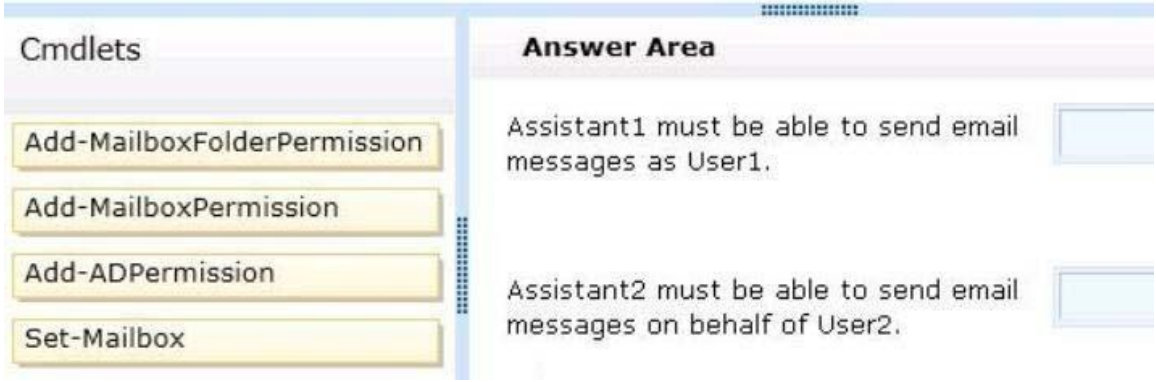
A. Set-SendConnector
B. Set-MailboxTransportService
C. Set-TransportService
D. Set-TransportServer

Answer: A

QUESTION 91
Drag and Drop Question
You have an Exchange Server 2013 organization that contains a server named Server1. A user named User1 has an administrative assistant named Assistant1. A user named User2 has an administrative assistant named Assistant2. You need to configure access to Outlook to meet the following requirements:

- Assistant1 must be able to send email messages as a User1.
- Assistant2 must be able to send email messages on behalf of User2.

Which cmdlets should you use? (To answer, drag the appropriate cmdlets to the correct requirements. Each cmdlet may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.)



Answer:

Explanation:

Add-MailboxFolderPermission.

Use the Add-MailboxFolderPermission cmdlet to manage folder-level permissions for all folders within a user's mailbox. For information about the parameter sets in the Syntax section below, see Syntax. This example assigns permissions for Ed to access Ayla's Marketing mailbox folder and applies the Owner role to his access of that folder.

Add-MailboxFolderPermission -Identity ayla@contoso.com:\Marketing -User Ed@contoso.com ?AccessRights Owner

Add-MailboxPermission

Use the Add-MailboxPermission cmdlet to add permissions to a mailbox. This example grants Kevin Kelly full access to Terry Adams's mailbox.

Note:

The Identity parameter requires the full name of the user to be enclosed in quotation marks (").

Add-MailboxPermission -Identity "Terry Adams" -User KevinKelly -AccessRights FullAccess ?InheritanceType All

Add-ADPermission.

Use the Add-ADPermission cmdlet to add permissions to an Active Directory object. This example grants Send As permissions for Aaron Painter to Terry Adams's mailbox.

Add-ADPermission -Identity "Terry Adams" -User AaronPainter -AccessRights ExtendedRight -ExtendedRights "Send As"

Send As rights is applied to Active directory object.

Set-Mailbox.

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. For information about the parameter sets in the Syntax section below, see Syntax. This example delivers John Woods's email messages to John's mailbox and also forwards them to Manuel Oliveira's (manuel@contoso.com) mailbox.

Set-Mailbox -Identity John -DeliverToMailboxAndForward $true -ForwardingSMTPAddress manuel@contoso.com

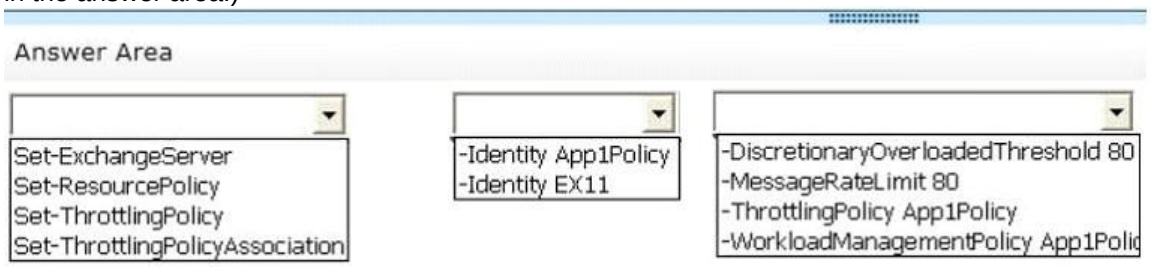
Send on Behalf.

The Send on Behalf permission allows a user to send email on behalf of the shared mailbox. For example, if John logs into the shared mailbox Reception Building 32 and sends an email, it will appear to recipients as being sent by "John on behalf of Reception Building 32". To grant Send on Behalf permissions, you must use the Exchange Management Shell. Use the Set-Mailbox cmdlet with the GrantSendonBehalf parameter.

QUESTION 92

Hotspot Question

You have an Exchange Server 2013 organization that contains 10 mailbox servers. You have a custom workload management policy named App1Policy. App1Policy is applied to three Mailbox servers. You deploy a new Mailbox server named EX11. You need to ensure that App1Policy is applied to EX11. Which command should you run? (To answer, configure the appropriate options in the answer area.)



Answer:

Explanation:

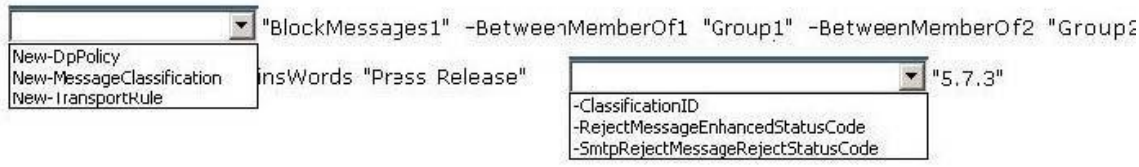
An Exchange workload is an Exchange Server feature, protocol, or service that's been explicitly defined for the purposes of Exchange system resource management. Each Exchange workload consumes system resources such as CPU, mailbox database operations, or Active Directory requests to run user requests or background work. Examples of Exchange workloads include Outlook Web App, Exchange ActiveSync, mailbox migration, and mailbox assistants. There are two ways to manage Exchange workloads: by monitoring the health of system resources or by controlling how resources are consumed by individual users (sometimes called user throttling in Exchange 2010). Managing workloads based on the health of system resources is new in Microsoft Exchange Server 2013. Controlling how resources are consumed by individual users was possible in Exchange Server 2010, and this capability has been expanded for Exchange Server 2013. You can customize the workload management settings if you want to change the default behavior of the feature for the needs of your environment.

SECTION1

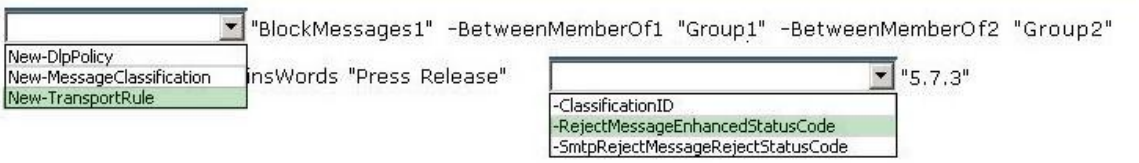
Use the Set-ExchangeServer cmdlet to set Exchange attributes in Active Directory for a specified

server.
(EX11)
Not a throttling policy. Scenario details a workload management policy. Use the Set-ResourcePolicy cmdlet to set the properties of a custom resource policy.
SECTION2
The Identity parameter specifies the GUID, distinguished name (DN), or name of the server. Need EX11 as it is the name of the server.
SECTION3
The WorkloadManagementPolicy parameter specifies the name of a workload management policy to apply in Active Directory. (App1Policy) Not a throttling policy.

QUESTION 93
Hotspot Question
You have an Exchange Server 2013 organization that contains two distribution groups named Groupl and Group2. You need to prevent the members of Groupl and Group2 from communicating with each other by using email, unless the email messages contain the string Press Release in the subject. Users whose email messages are rejected must receive a non-delivery report (NDR) that contains a status code of 5.7.3. Which command should you run? (To answer, configure the appropriate options in the answer area.)



Answer:

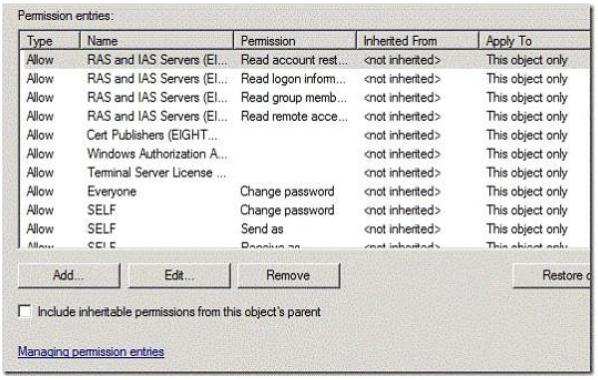


QUESTION 94
You have an Exchange Server 2013 organization named for A.Datum Inc. A user named User1 is a member of the Domain Admins group. User1 fails to synchronize a new Windows Phone device by using Exchange ActiveSync and receives an HTTP 500 error message. User1 successfully logs on to Outlook Web App and Outlook Anywhere. You need to ensure that User1 can synchronize the new Windows Phone device by using Exchange ActiveSync. Which two tasks should you perform? (Each correct answer presents a complete solution. Choose two.)

A. Disable permission inheritance on the User1 user account.
B. Enable permission inheritance on the User1 user account.
C. Install a trusted root certificate on the Windows Phone device.
D. Create a new mobile device mailbox policy.
E. Modify the Exchange ActiveSync policy that applies to User1's mailbox.

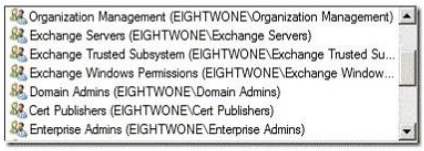
Answer: BE
Explanation:
HTTP 500 ERROR MESSAGE.
The Web server (running the Web Site) encountered an unexpected condition that prevented it from fulfilling the request by the client (e.g. your Web browser or our CheckUpDown robot) for

access to the requested URL.
B
Simply check include inheritable permissions from this object's parent.
INHERITABLE PERMISSIONS



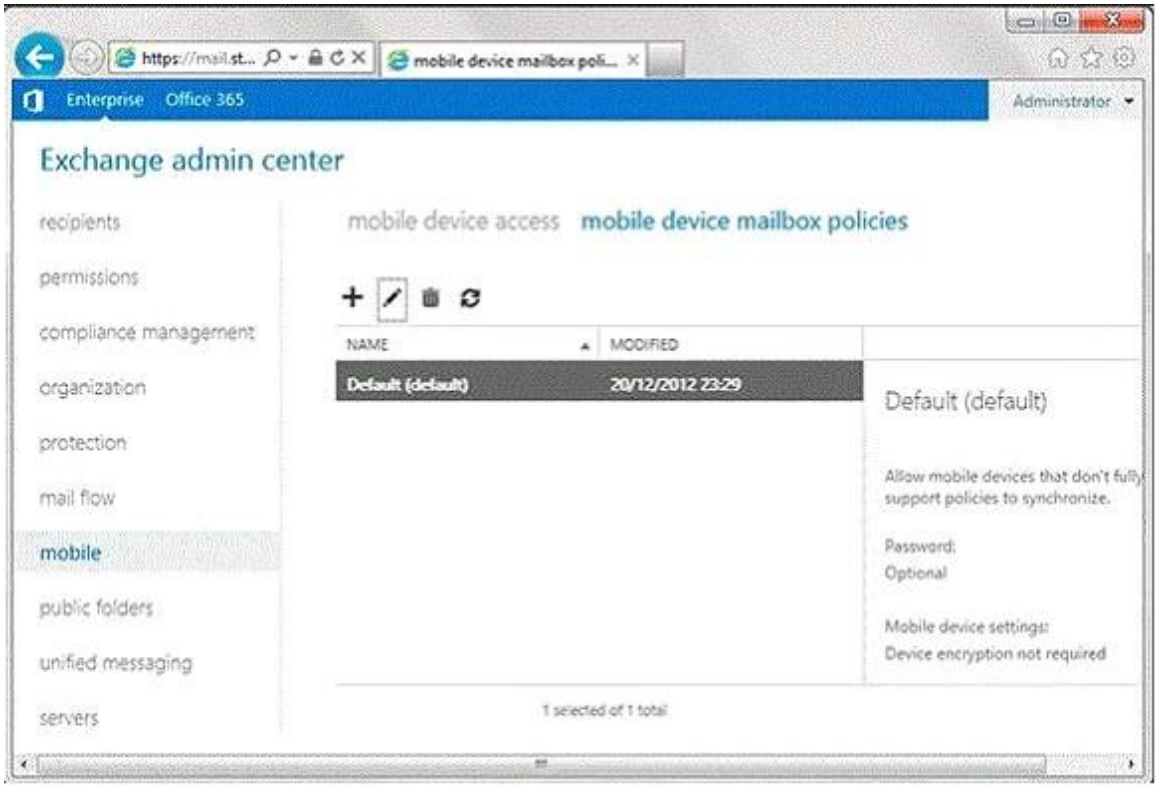
Notice the Include inheritable permissions from this object's parent is not set, the reason for Exchange not having any permissions on the object.

To fix the issue, simply check **Include inheritable permissions from this object's parent** and click **OK**. You'll return to the previous window where you'll notice the Exchange Server account is now granted permissions on the object:



At this point, ActiveSync will work and Exchange will be able to create MsExchActiveSync objects in the ExchangeActiveSyncDevices container:

NOT A
Need to enable permission inheritance on the User1 user account not disable it.
NOT C
This solution will fix a different error. (Error 80072F0D) error. This error can occur when the root certificate authority that generated the SSL certificate being used by the Exchange server is not trusted by the Windows Phone device. This will commonly occur with Exchange servers that are still configured to use a self-signed certificate, or that have a certificate issued from a private CA.
NOT D
No need to create a new policy but need to modify the existing policy.



E

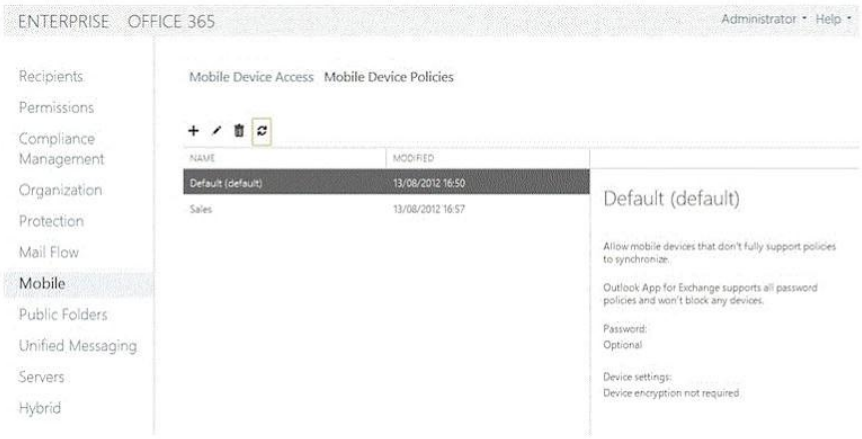
It appears that Exchange ActiveSync for User 1's mailbox may not be enabled. Use the EAC to enable or disable Exchange ActiveSync:

- In the EAC, navigate to Recipients > Mailboxes.
- In the list of user mailboxes, click the mailbox that you want to enable or disable Exchange ActiveSync for, and then click Edit.
- On the mailbox properties page, click Mailbox Features.
- Under Mobile Devices, do one of the following:

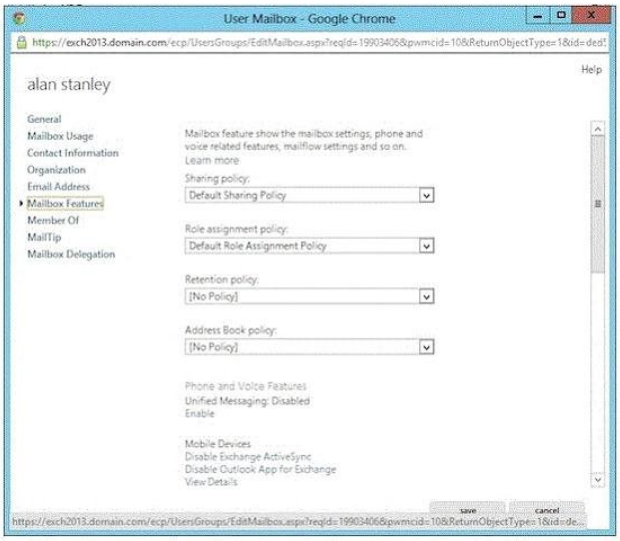
* To disable Exchange ActiveSync click Disable Exchange ActiveSync. A warning appears asking if you're sure you want to disable Exchange ActiveSync. Click Yes.
* To enable Exchange ActiveSync, click Enable Exchange ActiveSync. Click Save to save your change.

Exchange ActiveSync mailbox policies control how users use and synchronize their mobile devices in your organization. When you change an Exchange ActiveSync device policy, it affects all users whose mailbox is associated with that policy. The policy you set as the default automatically affects all users in the organization except those you have explicitly assigned different device policies to. Not all mobile devices support all the Exchange ActiveSync policy settings. If a policy setting isn't supported on a particular device, the device may not apply the setting. You can control whether devices that don't support specific policies are allowed to connect in the General settings for the policy.

Once you have created your ActiveSync policy, it will now be listed within the Exchange management interface:



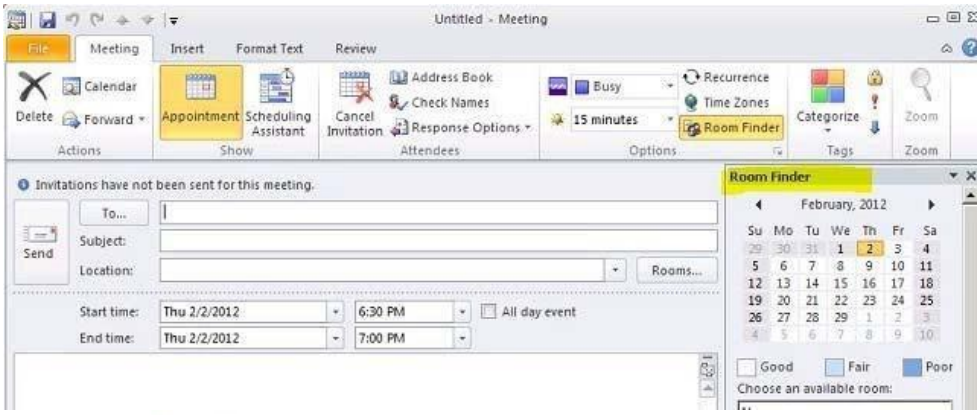
Meaning that you can assign it to users. Edit the properties of a "Recipient" and select Mailbox Features. Click on the link for View Details in the Mobile Devices section:



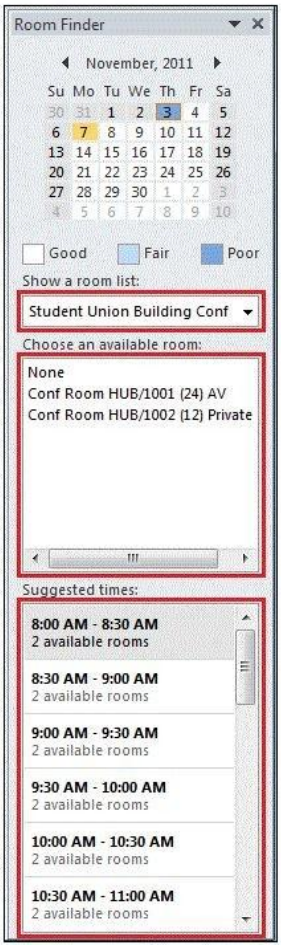
QUESTION 95
Your company has a main office and a branch office. You have an Exchange Server 2013 organization. The company recently built a new meeting room in the branch office. You need to ensure that the meeting room is available by using the Room Finder feature in Microsoft Outlook. Which cmdlet should you run?

A. Set-MailboxCalendarConfiguration
B. New-Mailbox
C. Set-CalendarProcessing
D. New RemoteMailbox

Answer: B
Explanation:
New-Mailbox.
Create a new Room Mailbox to schedule meetings in conference rooms, auditoriums, labs or other facilities: New-Mailbox -Name <Room Name> -Room

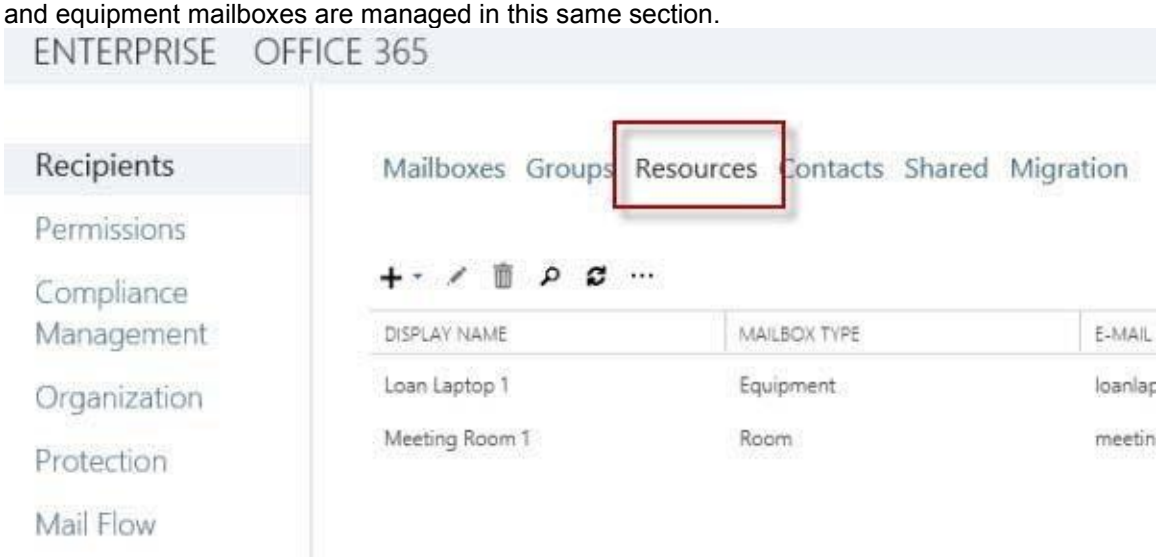


Room Finder in Outlook 2010
with Room Lists

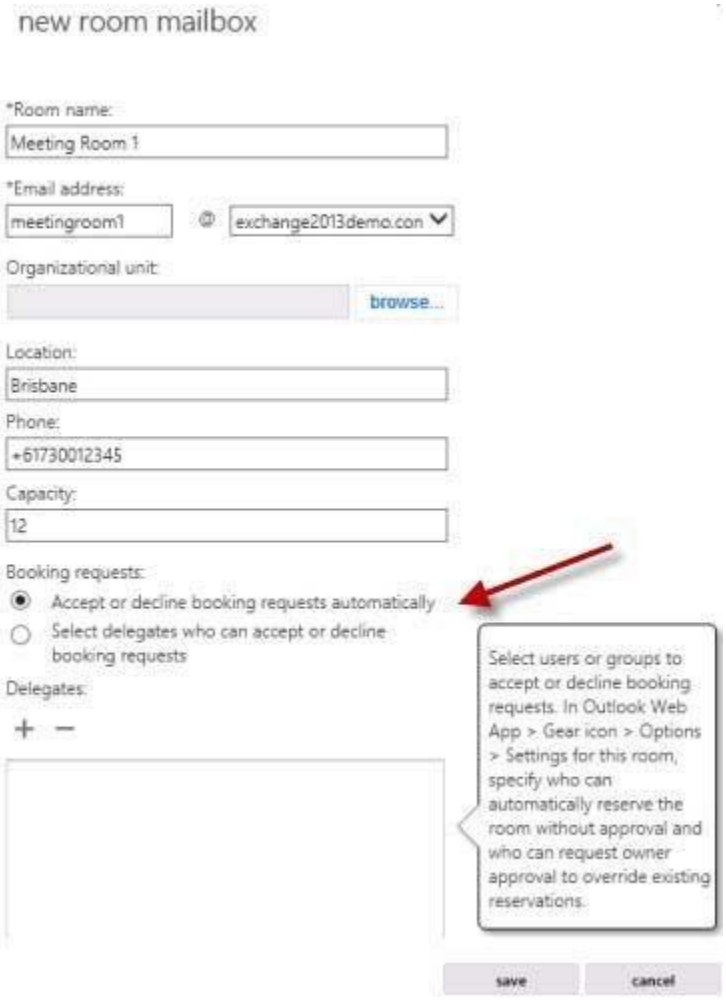


NOT A
Use the New-RemoteMailbox cmdlet to create a mail-enabled user in the on-premises Active Directory and also create an associated mailbox in the cloud-based service. Not designed for room mailboxes.
NOT C
Use the Set-MailboxCalendarConfiguration cmdlet to apply calendar settings for users using Microsoft Office Outlook Web App calendars.
NOT D
Use the Set-CalendarProcessing cmdlet to modify calendar-related processing configuration

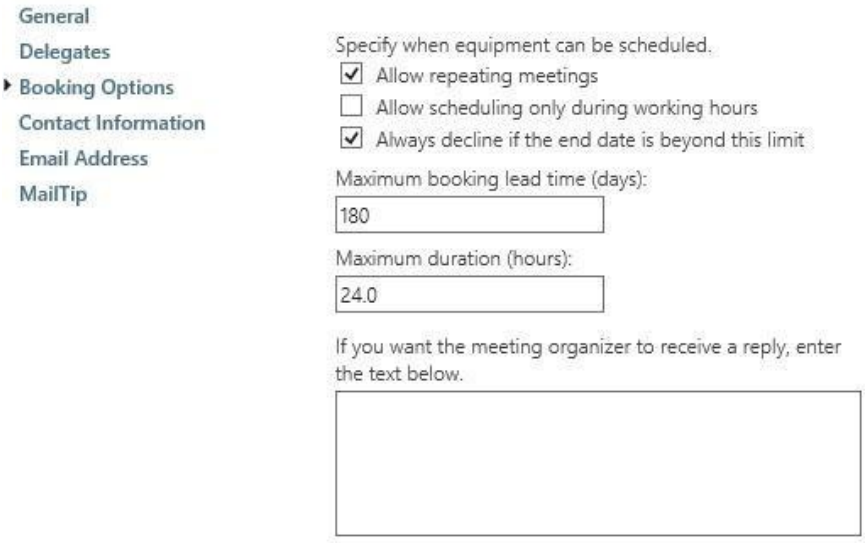
properties for the target mailbox, which include Calendar Attendant, resource booking assistant, and calendar configuration.
B
New-Mailbox.
Create a new Room Mailbox to schedule meetings in conference rooms, auditoriums, labs or other facilities Create new Room Mailbox PowerShell command syntax:
`New-Mailbox -Name <Room Name> -Room`
Example:
New-MailBox -Name FL-ROOM1 -Room
A Look at Exchange Server 2013 Resource Mailboxes.
http://exchangeserverpro.com/exchange-server-2013-room-equipment-mailboxes/
Resource mailboxes have been around for a few versions of Exchange Server, and Exchange Server 2013 brings us a few improvements in how they are managed. There are two types of resource mailboxes:
Room mailboxes are for fixed locations such as meeting rooms or conference facilities Equipment mailboxes are for items that are not fixed to a location, such as laptops or vehicles Exchange 2013 puts resource mailboxes under their own section of the Exchange Administration Center. Both room and equipment mailboxes are managed in this same section.



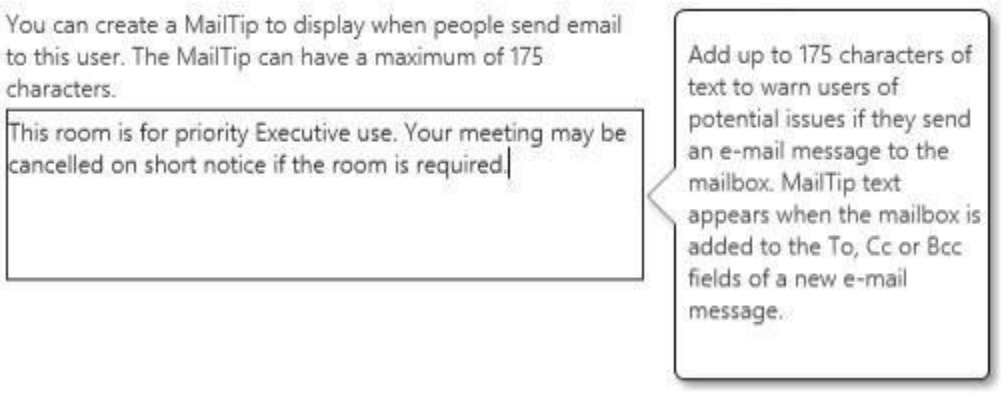
One of the immediate improvements is that you are able to set the booking policy or assign delegates during the creation of the resource mailbox, rather than as a secondary task after the mailbox is created.



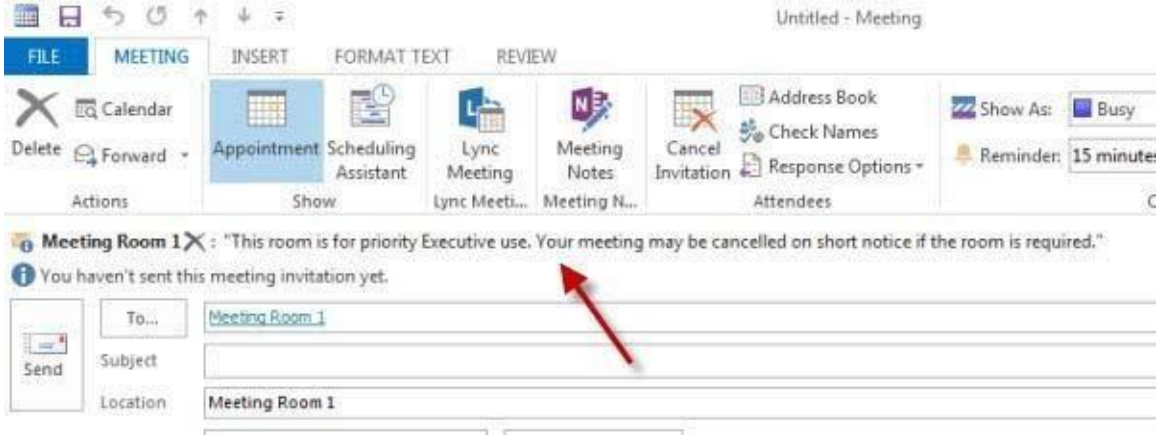
After the mailbox has been created there are a few additional properties you can customize. The booking options can be further tuned with regards to recurring meetings, booking horizon, and custom replies.



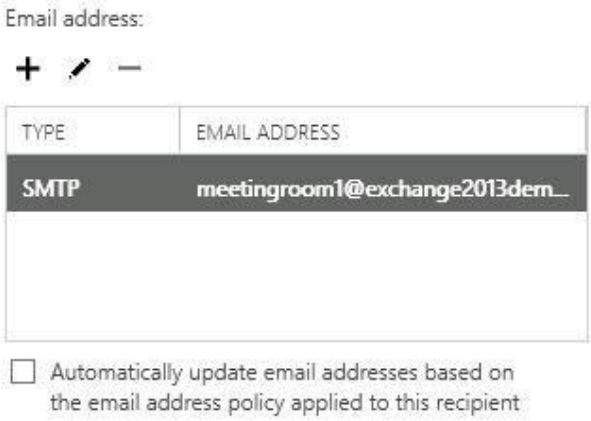
You can also easily configure a MailTip for the resource mailbox.



The text that you place in the MailTip will appear automatically when people add the room or resource mailbox to a meeting request in Outlook. Although in my opinion the MailTip needs some color to draw the person's attention to it.



Finally, an interesting default setting is the disabling of email address policies. This does make sense as most resource mailboxes are for internal use only, so having email address policies assigning multiple SMTP addresses to resource mailboxes is usually not necessary.



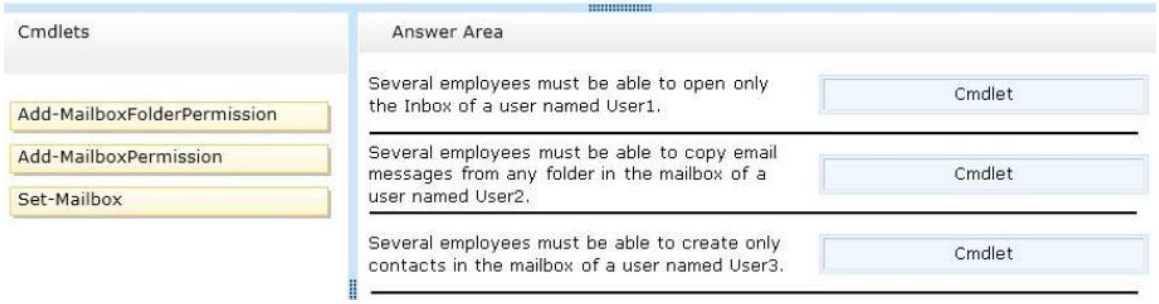
Overall it appears that room and resource mailboxes are a feature that has matured over the previous versions of Exchange Server and now receive just a few minor improvements to make them simpler to manage.

QUESTION 96
Drag and Drop Question

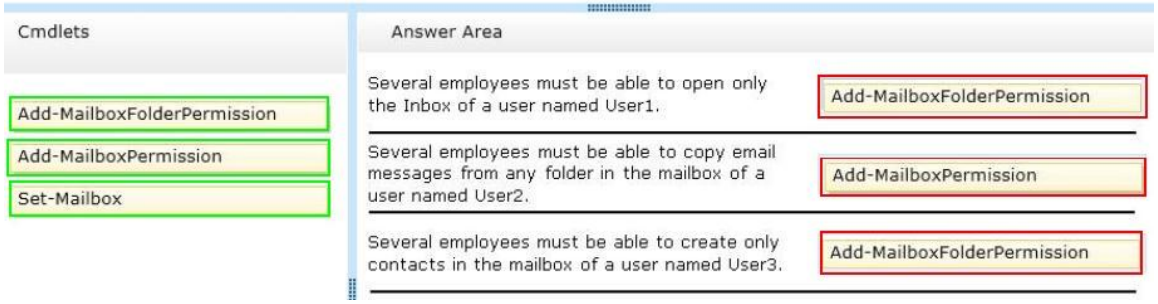
You have an Exchange Server 2013 organization that contains five servers. Several employees plan to use Microsoft Outlook to collaborate on some projects. You need to configure access to Outlook to meet the following requirements:

- Several employees must be able to open only the Inbox of a user named User1.
- Several employees must be able to copy email messages from any folder in the mailbox of a user named User2.
- Several employees must be able to create only contacts in the mailbox of a user named User3.

Which cmdlets should you use? To answer, drag the appropriate cmdlet to the correct requirement in the answer area. Each cmdlet may be used once, more than once, or not at all. Additionally, you may need to drag the split bar between panes or scroll to view content.



Answer:



Explanation:

Add-MailboxFolderPermission.

Use the Add-MailboxFolderPermission cmdlet to manage folder-level permissions for all folders within a user's mailbox.

EXAMPLE 1

This example assigns permissions for Ed to access Ayla's Marketing mailbox folder and applies the Owner role to his access of that folder.

Add-MailboxFolderPermission -Identity ayla@contoso.com:\Marketing -User Ed@contoso.com ?AccessRights Owner

Add-MailboxPermission

Use the Add-MailboxPermission cmdlet to add permissions to a mailbox.

EXAMPLE 1

This example grants Kevin Kelly full access to Terry Adams's mailbox.

Note:

The Identity parameter requires the full name of the user to be enclosed in quotation marks (").

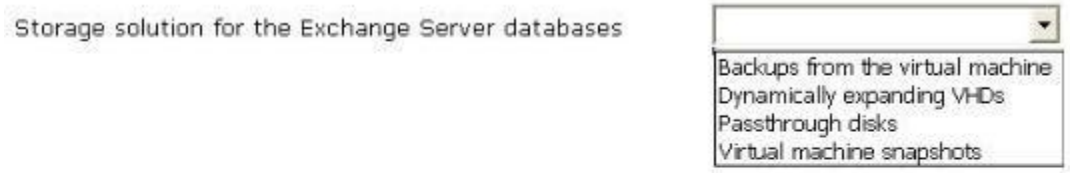
Add-MailboxPermission -Identity "Terry Adams" -User KevinKelly -AccessRights FullAccess ?InheritanceType All

Set-Mailbox.

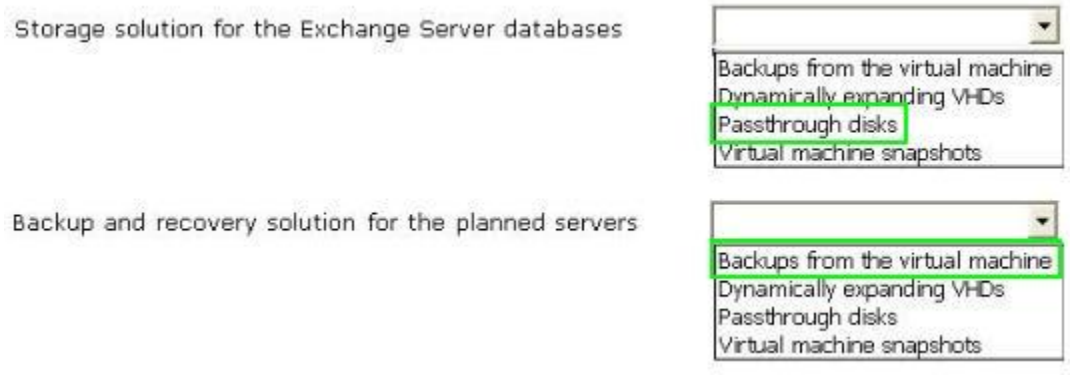
Use the Set-Mailbox cmdlet to modify the settings of an existing mailbox. You can use this cmdlet for one mailbox at a time. To perform bulk management, you can pipeline the output of various Get-

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.
EXAMPLE 1
This example delivers John Woods's email messages to John's mailbox and also forwards them to Manuel Oliveira's (manuel@contoso.com) mailbox.
Set-Mailbox -Identity John -DeliverToMailboxAndForward $true -ForwardingSMTPAddress manuel@contoso.com
STEPS
1. Use the Add-MailboxFolderPermission cmdlet to manage folder-level permissions for all folders within a user's mailbox.
2. Use the Add-MailboxPermission cmdlet to add permissions to a mailbox.
3. Use the Add-MailboxFolderPermission cmdlet to manage folder-level permissions for all folders within a user's mailbox.

QUESTION 97
Hotspot Question
You are planning to implement several servers on virtual machines. The servers have Exchange Server 2013 installed. The planned implementation must meet the following requirements:
- Minimize the amount of overhead required for the virtualization solution.
- Minimize the risk of data corruption for the Exchange Server databases.
You need to recommend a storage solution for the Exchange databases and a backup and recovery solution for the planned servers. Which solutions should you recommend? To answer, select the appropriate solutions in the answer area.



Answer:



QUESTION 98
Your network contains an Active Directory forest. The forest contains a single domain named contoso.com. You have an Exchange Server 2013 organization named Contoso. You plan to create an additional SMTP domain named sales.contoso.com. You will use sales.contoso.com as the

primary SMTP address for the users in the sales department. You create a new email address policy and apply the policy to the sales users. New sales users report that when they attempt to access their email from the Internet for the first time by using Microsoft Outlook 2010, they fail to connect. The sales users connect to their mailbox internally successfully by using Outlook 2010. All other users can connect to their mailbox from the Internet and internally. You need to ensure that the new sales users can connect to the Exchange Server 2013 organization by using Outlook Anywhere from the Internet. Which two actions should you perform? (Each correct answer presents part of the solution. Choose two.)

A. Modify each existing Service Connection Point (5CP) object in Active Directory to point to auto discover.sales.contoso.com.
B. From DNS Manager, create a host (A) record for autodiscover.sales.contoso.com.
C. On the Client Access servers, deploy a new certificate that includes the autodiscover.sales.contoso.com name.
D. Create a new Autodiscover virtual directory on the Client Access servers and configure ExternalURL to use autodiscover.sales.contoso.com.
E. Create a new Service Connection Point (SCP) object in Active Directory that points to auto discover.sales.contoso.com.

Answer: BC
Explanation:
- Externally connected clients are different, because they can't lookup the SCP in Active Directory from outside of the network. These clients might be roaming laptop users with Outlook, or they might be ActiveSync capable smartphones such as iPhones. In either case they will attempt to connect to Autodiscover by performing a DNS lookup for "autodiscover.smtpdomainname".
- You need the "autodiscover.smtpdomainname" name in the Exchange 2013 SSL certificate. (C)
- You will only need an autodiscover name for each SMTP domain that a user is likely to enter as their email address. (B)

QUESTION 99
You have an Exchange Server 2013 organization named Contoso. The organization contains a server named Server1 that has Exchange Server 2013 installed. Server1 has the Mailbox server role and the Client Access server role installed. Server1 has a Send connector for a partner company. The Send connector is configured for Domain Security with a domain named adatum.com. The only certificate installed on Server1 expires. You discover that all email messages sent to adatum.com remain in the queue on Server1. On Server1, you install a new certificate from a trusted third-party. You need to ensure that the email messages are delivered to adatum.com. What should you do?

A. Assign the new certificate to the IIS service.
B. Send the new certificate to the administrator at adatum.com.
C. Assign the new certificate to the SMTP service.
D. Create a new send connector that contains an address space to adatum.com.

Answer: C
Explanation:
- The Enable-ExchangeCertificate cmdlet enables certificates when it updates the metadata that is stored with the certificate. To enable an existing certificate to work with different services, run the Enable-ExchangeCertificate command and specify the services that you want to enable.
- You can rerun this cmdlet if you want to add new services that use the certificate. When you enable a certificate for the Simple Mail Transfer Protocol (SMTP) service and the certificate contains a FQDN that matches the FQDN of the local computer, the certificate may be published to the Active Directory directory service.

QUESTION 100

Your network contains an Active Directory forest named contoso.com. The forest contains an enterprise root certification authority (CA) named CA1. The network contains a server named EX1 that has Exchange Server 2013 installed. A partner company named A . Datum Corporation has an Active Directory domain named adatum.com. The domain contains a server named EX5 that has Exchange Server 2010 Service Pack 2 (SP2) installed. EX5 has a Receive connector that is configured for mutual TLS. Users in contoso.com plan to send email messages that contain sensitive data to users in adatum.com. You need to ensure that all of the email messages sent from contoso.com to adatum.com are encrypted by using TLS. The solution must ensure that EX1 and EX5 validate server certificates. Which three actions should you perform? (Each correct answer presents part of the solution. Choose three.)

A. Run the set-transportconfig -tlssenddomainsecurelist contoso.com command.
B. Install a certificate, and then assign the certificate to the IIS service.
Send the root certificate for contoso.com to the administrators in adatum.com.
C. Run the New-SendConnector cmdlet and specify the domainsecureenabled parameter.
D. Run the New-SendConnector cmdlet and specify the tlsdomainparameter.
E. Run the set-transportconfig -tlssenddomainsecurelist adatum.com command.
F. Install a certificate, and then assign the certificate to the SMTP service.
Send the root certificate for contoso.com to the administrators in adatum.com.

Answer: ADF

Explanation:

A: Use the Set-TransportConfig cmdlet to modify the transport configuration settings for the whole Exchange organization. TheTLSSendDomainSecureListparameter specifies the domains from which you want to send domain secured email by using mutual TLS authentication. In this scenario we send from EX1 in the contoso.com domain.
D: Need to create a new send connector. The TlsDomain parameter specifies the domain name that the Send connector uses to verify the FQDN of the target certificate when establishing a TLS secured connection.
F: A new certificate is needed for the SMTP service.

.....

QUESTION 151

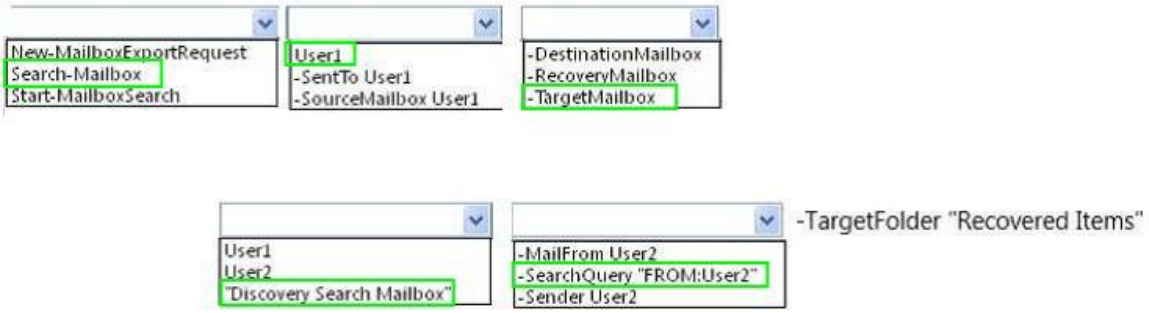
Hotspot Question

You have an Exchange Server 2013 organization. You enable single item recovery for all users. A user named User1 accidentally deletes important email messages sent from a user named User2. User1 reports that he cannot locate the email messages in his Deleted Items folder. You need to recover the items. What command should you run? (To answer, select the appropriate options in the answer area.)

Answer Area

Answer:

Answer Area



QUESTION 152

Fabrikam, Ltd. has an Exchange Server organization that contains two servers. The servers are configured as shown in the following table. Recently, the internal and external namespaces named mail.fabrikam.com and autodiscover.fabrikam.com were changed to point to EX2. You configure all of the users on EX2 to access their mailbox by using Microsoft Outlook from the Internet. You enable Outlook Anywhere on EX1. You need to ensure that users who have mailboxes on EX1 can connect to their mailbox from the Internet. What should you do on EX1?

Server name	Role	Exchange Server version	Site location
EX1	Mailbox server Client Access server Hub Transport server	Exchange Server 2010	New York
EX2	Mailbox server Client Access server	Exchange Server 2013	New York

A. Set the ExternalHostName value to NULL.
B. Set the ExternalClientAuthenticationMethod value to Basic and NTLM.
C. Set the IISAuthenticationMethods value to Basic and NTLM.
D. Set the InternalHostName value to NULL

Answer: B

QUESTION 153

Hotspot Question

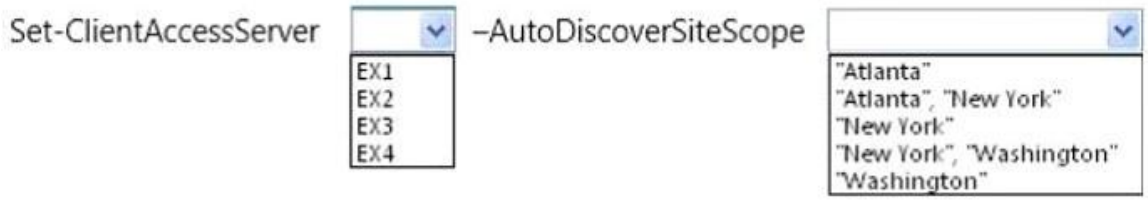
Your company has two main offices. One office is located in Atlanta and the other office is located in Washington. The offices connect to each other by using a dedicated WAN link. You have an Exchange Server 2013 organization that contains four servers. The servers are configured as shown in the following table.

Server name	Office	Role
EX1	Atlanta	Mailbox server
EX2	Atlanta	Client Access server
EX3	Washington	Mailbox server
EX4	Washington	Client Access server

The company opens a new office in New York. The New York office connects directly to the Washington office via a dedicated WAN link. You configure a separate Active Directory site for each office. You discover poor response times when scheduling meetings and configuring Microsoft Outlook profiles from the client computers in the New York office. You need to reduce the amount

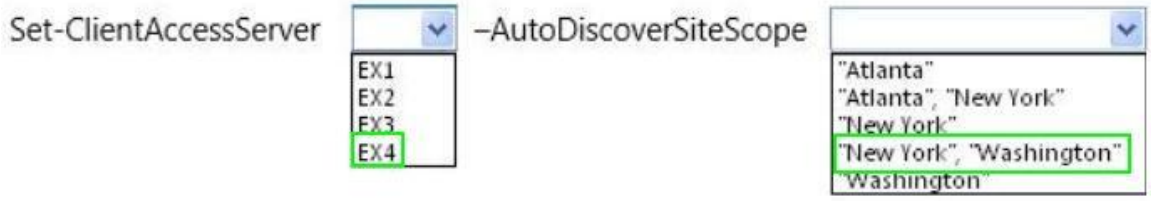
of time required to schedule meetings and to configure Outlook profiles from the computers in the New York office. What command should you run? (To answer, select the appropriate options in the answer area.)

Answer Area



Answer:

Answer Area



QUESTION 154

Your company has a main office and four branch offices. You have an Exchange Server 2013 organization that contains 2,500 mailboxes. An administrator plans to deploy Microsoft Lync Server 2013. You need to enable the unified contact store in the Exchange Server 2013 organization. What should you run?

A. The New-CsPartnerApplication cmdlet
B. The Set-ClientAccessServer cmdlet
C. The Configure-EnterprisePartnerApplication.ps1 script
D. The Set-AuthConfig cmdlet

Answer: C

Explanation:

http://memphistech.net/?p=280
http://mchahla.blogspot.co.uk/2013/01/integrating-lync-server-2013-exchange.html
http://mike-graham.co.uk/blog/2013/09/14/setting-up-lync-2013-with-exchange-2013-part-3-exchange-2013-integration

QUESTION 155

Hotspot Question

Your network contains an Active Directory forest. The forest contains a single domain. You have an Exchange Server 2013 organization named Contoso that contains a server named EX01. Split permissions are configured for the organization. You need to change the permission model to shared permissions. What command should you run? (To answer, select the appropriate options in the answer area.)

Answer Area

Answer:

Answer Area

QUESTION 156

You have an Exchange Server 2013 organization that contains a database availability group (DAG) named DAG1. DAG1 has two members. You create a mailbox database copy for each database on each DAG member. You plan to implement a service level agreement (SLA) that meets the following requirements: All deleted mailboxes must be recoverable for up to six months after they are deleted. When a mailbox is recovered, the entire contents of the mailbox must be recovered. You need to recommend a solution that meets the requirements. What should you recommend?

A. Get-Mailbox | Set-Mailbox -RetainDeletedItemsFor 180.00:00:00
B. Get-MailboxDatabase | Set-MailboxDatabase -MailboxRetention 180.00:00:00
C. Get-MailboxDatabase | Set-MailboxDatabase -DeletedItemRetention 180.00:00:00
D. Get-Mailbox | Set-Mailbox -Audit Log Age Limit 180.00:00:00

Answer: B

Explanation:

Set-MailboxDatabase.
Get-MailboxDatabase | Set-MailboxDatabase -MailboxRetention 180.00:00:00
The MailboxRetention parameter specifies the length of time to keep deleted mailboxes. To specify a value, enter it as a time span: dd.hh:mm:ss where d = days, h = hours, m = minutes, and s = seconds. For example, to specify a 15-hour interval, enter 15:00:00. The maximum length of time to retain mailboxes is 24,855 days. By default, deleted mailboxes are retained for 30 days. This attribute applies to all mailboxes in this mailbox database.
http://technet.microsoft.com/en-us/library/bb124924(v=exchg.150).aspx
http://technet.microsoft.com/en-gb/library/bb123971(v=exchg.150).aspx

QUESTION 157

You have an Exchange Server 2013 organization that contains two Client Access servers and two Mailbox servers. You configure DNS round robin on the Client Access servers. All of the host (A) and alias (CNAME) records in the DNS zone are configured to have a TTL value of 10 minutes. You need to recommend a solution to fail over client connections to a Client Access server automatically if Internet Information Services (US) fails. The solution must minimize costs. What should you recommend?

A. Deploy a Client Access server array.
B. Reduce the TTL values on all of the A and CNAME records to one minute.
C. Deploy a hardware load balancing solution.
D. Deploy Network Load Balancing (NLB) on each Client Access server.

Answer: D

QUESTION 158

Hotspot Question

Your network contains an Active Directory forest named contoso.com. The forest contains one domain and two sites named Site1 and Site2. Site1 connects directly to the Internet. You have an Exchange Server 2010 organization. Users access their email remotely by using Outlook Web App and Outlook Anywhere by connecting to the name mail.contoso.com. You plan to migrate to Exchange Server 2013. Exchange Server 2010 and Exchange Server 2013 will co-exist for several months during the migration. During the co-existence phase, the organization will contain seven servers. The servers will be configured as shown in the following table.

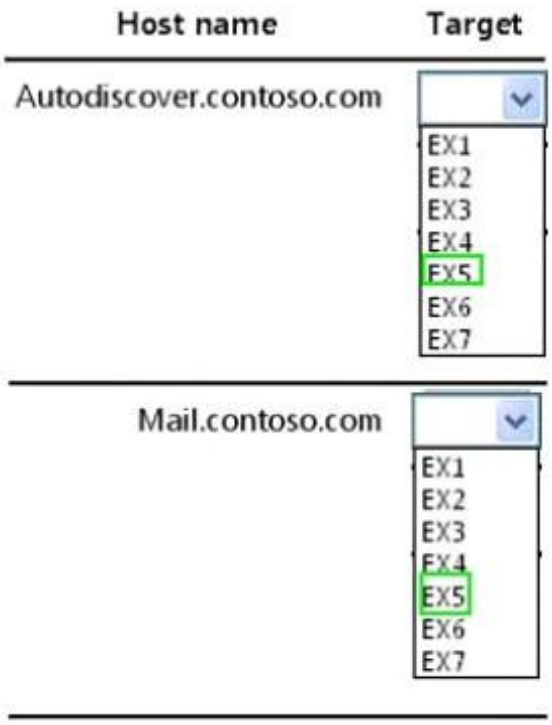
Server name	Active Directory site	Role	Exchange Server version
EX1	Site1	Client Access	Exchange Server 2010
EX2	Site1	Mailbox Hub Transport	Exchange Server 2010
EX3	Site2	Client Access Hub Transport	Exchange Server 2010
EX4	Site2	Mailbox	Exchange Server 2010
EX5	Site1	Client Access	Exchange Server 2013
EX6	Site1	Mailbox	Exchange Server 2013
EX7	Site2	Mailbox	Exchange Server 2013

You need to identify which host names must be associated to which servers. The solution must ensure that the users can access mailboxes on EX2, EX4, EX6, and EX7. What should you do? (To answer, select the appropriate target for each host name in the dialog box in the answer area.)

Answer Area

Answer:

Answer Area



QUESTION 159

A company named Fabrikam, Ltd. has an Exchange Server 2013 organization that contains two servers. The servers are configured as shown in the following table.

Server name	Role	Exchange Server version
EX1	Mailbox server Client Access server Hub Transport server	Exchange Server 2007 Service Pack 3 (SP3)
EX2	Mailbox server Client Access server	Exchange Server 2013 Cumulative Update 1 (CU1)

You configure the internal and external namespaces named mail.fabrikam.com and autodiscover.fabrikam.com to point to EX2. You configure Outlook Anywhere on EX1 as shown in the following table.

Setting	Value
ClientAuthenticationMethod	Basic
IISAuthenticationMethods	NTLM

You configure Outlook Anywhere on EX2 as shown in the following table.

Setting	Value
ExternalClientAuthenticationMethod	Basic
InternalClientAuthenticationMethod	NTLM
IISAuthenticationMethods	Basic NTLM Negotiate

You need to ensure that all of the users on EX1 can connect to their mailbox by using Microsoft Outlook from the Internet. What should you do?

A. Change the authentication settings of EX1.
B. Disable IPv6 on EX1.
C. Change the authentication settings of EX2.
D. Disable Outlook Anywhere on EX1.

Answer: A

QUESTION 160
You have an Exchange Server 2013 organization. You need to ensure that an administrator named Adminl receives a daily email message that contains a log of all the Exchange Server administrative actions. Which cmdlet should you use in a scheduled task?

A. Search-AdminAuditLog
B. Set-AdminAuditLogConfig
C. New-AdminAuditLogSearch
D. Write-AdminAuditLog

Answer: C
Explanation:
New-AdminAuditLogSearch.
http://technet.microsoft.com/en-us/library/ff459243(v=exchg.150).aspx
After the New-AdminAuditLogSearch cmdlet is run, the report is delivered to the mailboxes you specify within 15 minutes. The log is included as an XML attachment on the report email message. The maximum size of the log that can be generated is 10 megabytes (MB). You need to be assigned permissions before you can run this cmdlet. Although all parameters for this cmdlet are listed in this topic, you may not have access to some parameters if they're not included in the permissions assigned to you. To see what permissions you need, see the "View-only administrator audit logging" entry in the Exchange and Shell infrastructure permissions topic.
New-AdminAuditLogSearch -ExternalAccess $true -StartDate 07/25/2013 -EndDate 10/24/2013 -StatusMailRecipients admin@contoso.com,pilarp@contoso.com -Name "Datacenter admin audit log"

QUESTION 161
You have an Exchange Server 2013 organization. You plan to assign the default workload management policy to all of the servers in the organization. You need to remove the Calendar Synchronization Assistant workload from the workload management policy before you assign the policy to the servers. Which cmdlet should you run?

A. Remove-ResourcePolicy
B. Set-ResourcePolicy
C. Set-WorkloadPolicy

D. Remove-WorkloadPolicy

Answer: D
Explanation:
New-WorkloadManagementPolicy.
EXAMPLE 1
This example creates a custom workload management policy that will be used to control Exchange workloads at the Dublin, Ireland location of Contoso.com. The name of the server in the Dublin, Ireland location of Contoso.com is Dublin01.
New-WorkloadManagementPolicy -Name DublinWorkloadManagementPolicy -DomainController Dublin02.contoso.com
Set-ExchangeServer -WorkloadManagementPolicy DublinWorkloadManagementPolicy -Identity Dublin01
EXAMPLE 2
This example uses the Template parameter to create a policy object DallasWorkloadManagementPolicy based on the Default Workload Management Policy. It is then customized to remove the ELC Assistant workload from the Workload Management Policy. The Workload Management Policy is then assigned to server Dallas01.
New-WorkloadManagementPolicy -Name DallasWorkloadManagementPolicy -Template DefaultWorkloadManagementPolicy_15.0.505.0 Remove-WorkloadPolicy DallasWorkloadManagementPolicy\ELCAssistant Set-ExchangeServer -WorkloadManagementPolicy DallasWorkloadManagementPolicy -Server Dallas01
http://technet.microsoft.com/en-us/library/jj150485(v=exchg.150).aspx
http://technet.microsoft.com/en-us/library/jj215703(v=exchg.150).aspx

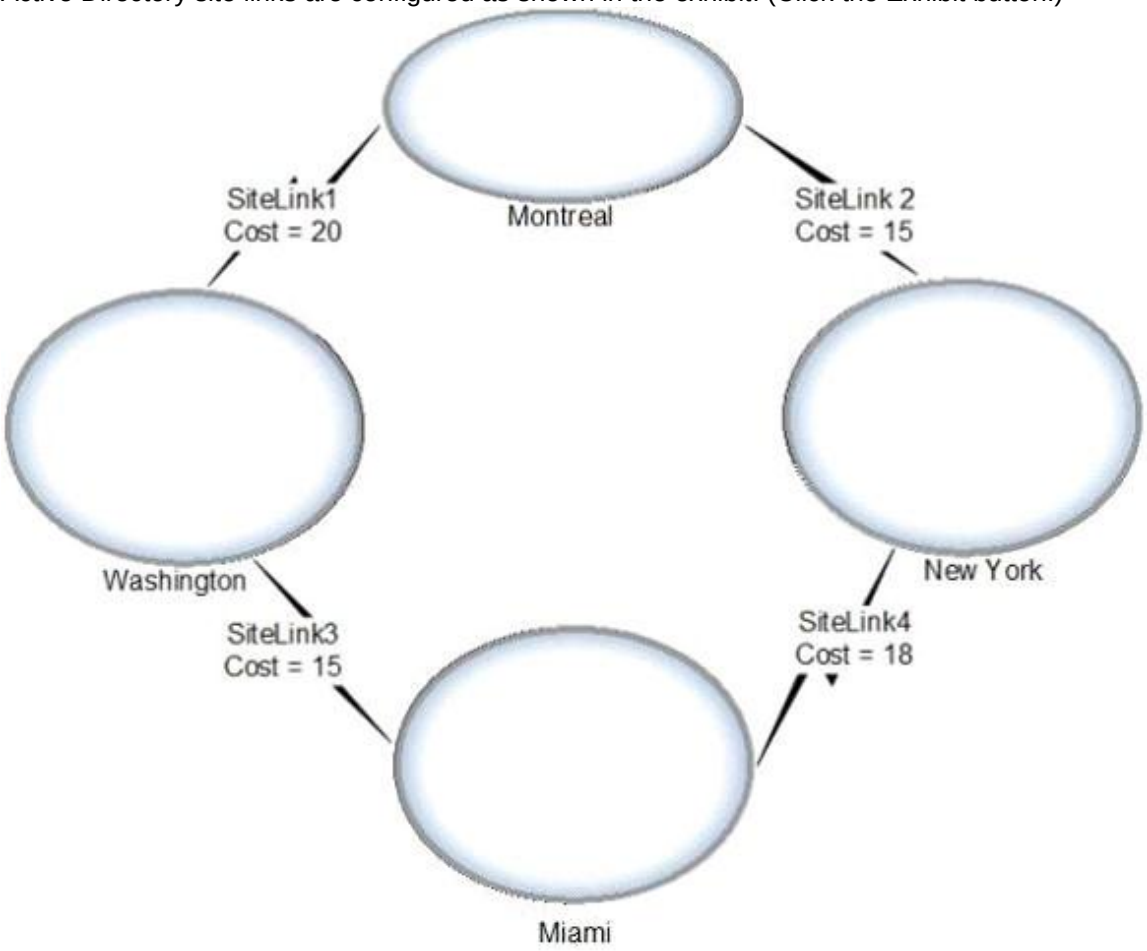
QUESTION 162
You have an Exchange Server 2013 organization named fabrikam.com. You have a distribution group named DL1 and a user named User1. The managedBy attribute of DL1 is fabrikam.com\users\User1. User1 attempts to add a user named User2 to DL1 and receives the following error message:
"Changes to the public group membership cannot be saved.
You do not have sufficient permissions to perform this operation on this object."
You need to ensure that User1 can add User2 to DLL. What are two possible ways to achieve this goal? (Each correct answer presents a complete solution. Choose two.)

A. From Exchange Management Shell, run New-ManagementRoleAssignment -Name "Default Role Assignment Policy-MyDistributionGroupMembership" -Policy "Default Role Assignment Policy" -Role "MyDistributionGroupMembership
B. From Exchange Admin Center, edit the Default Role Assignment Policy and select MyDistributionGroups
C. From Exchange Management Shell, run New-ManagementRoleAssignment -Name "Default Role Assignment Policy-MyDistributionGroups" -Policy "Default Role Assignment Policy" -Role "MyDistributionGroups"
D. From Exchange Admin Center, edit the Default Role Assignment Policy and select MyDistributionGroupMembership

Answer: AC
Explanation:
http://technet.microsoft.com/en-gb/library/jj657511(v=exchg.150).aspx
Role Assignment Policies cannot be managed via the EAC.

QUESTION 163
Your company has four offices. Each office connects to two of the other offices by using a direct WAN link. Each office is configured as an Active Directory site. The office connections and the

Active Directory site links are configured as shown in the exhibit. (Click the Exhibit button.)



You have Exchange Server 2013 organization that contains four servers. The servers are configured as shown in the following table.

Server name	Role	Data availability group (DAG)	Site location
EX1	Mailbox server Client Access server	No	Montreal
EX2	Mailbox server Client Access server	No	New York
EX3	Mailbox server Client Access server	No	Washington
EX4	Mailbox server Client Access server	No	Miami

You discover that email messages sent from the site in Montreal to the site in Miami are routed through the site in New York. You need to ensure that all of the email messages sent from the Montreal site to the Miami site are routed through the Washington site. What should you run?

A. Set-AdSite1ink Site1inkl -ExchangeCost 25
B. Set-AdSite Washington' -HubSiteEnabled $false
C. Set-AdSite1ink SiteUnkl -ExchangeCost 15
D. Set-AdSite New York' -Hubsiteenabled Sfalse

Answer: C

Explanation:

Set-AdSiteLink.

This cmdlet is available only in on-premises Exchange Server 2013. Use the Set-AdSiteLink cmdlet to assign an Exchange-specific cost to an Active Directory IP site link. You can also use this cmdlet to configure the maximum message size that can pass across an Active Directory IP site link.

EXAMPLE 1

This example assigns an Exchange-specific cost of 25 to the IP site link DEFAULT_IP_SITE_LINK and configures a maximum message size limit of 10 MB on the IP site link.

Set-AdSiteLink DEFAULT_IP_SITE_LINK -ExchangeCost 25 -MaxMessageSize 10MB

By default, Microsoft Exchange determines the least cost routing path by using the cost assigned to the Active Directory IP site link. You can use the Set-AdSiteLink cmdlet to assign an Exchange-specific cost to the Active Directory IP site link. The Exchange-specific cost is a separate attribute used instead of the Active Directory-assigned cost to determine the least cost routing path. This example sets an Exchange specific cost of 10 to the IP site link IPSiteLinkAB.

Set-AdSiteLink -Identity IPSiteLinkAB -ExchangeCost 10

http://technet.microsoft.com/en-us/library/bb123696(v=exchg.150).aspx

http://technet.microsoft.com/en-gb/library/bb266946(v=exchg.141).aspx

QUESTION 164

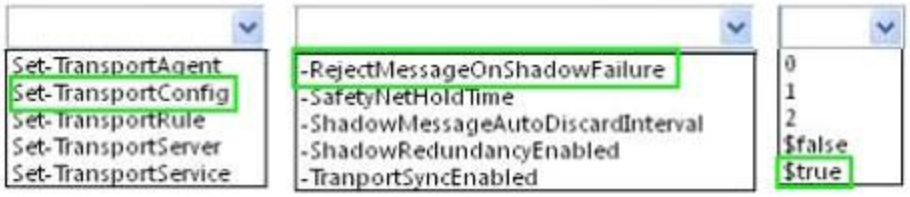
Hotspot Question

Your network contains an Active Directory forest. The forest contains two sites named Site1 and Site2. You have an Exchange Server 2013 organization. Site1 contains two Mailbox servers and one Client Access server. Site2 contains two Mailbox servers and two Client Access servers. You need to prevent messages that cannot be protected by shadow redundancy from being delivered. What command should you run? (To answer, select the appropriate options in the answer area.)

Answer Area

Answer:

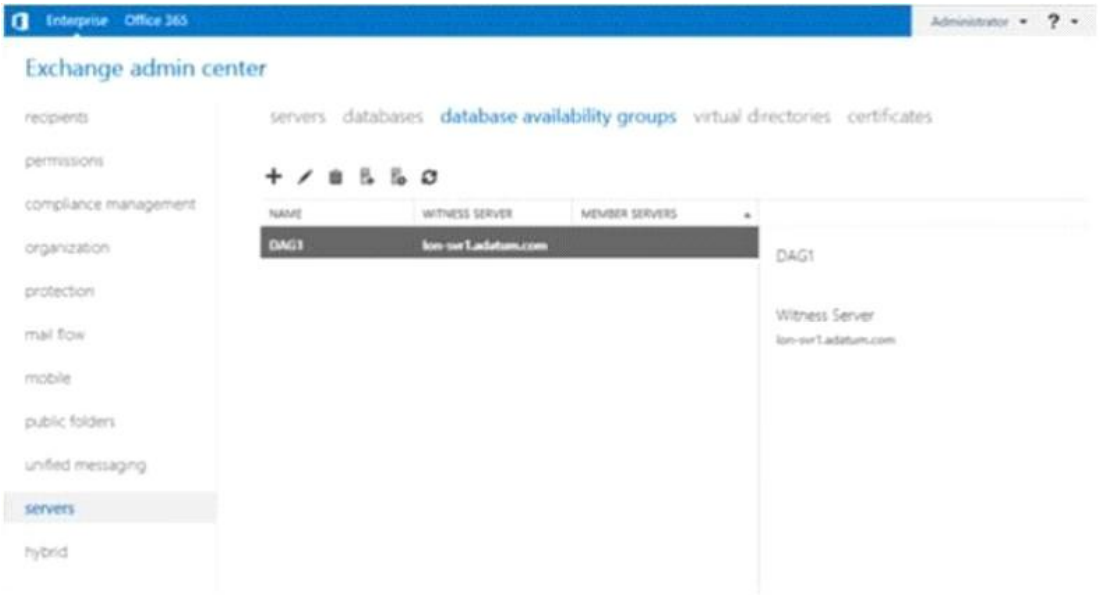
Answer Area



QUESTION 165

Hotspot Question

You have an Exchange Server 2013 organization that contains two Mailbox servers named EX01 and EX02. Both servers are in the same Active Directory site. On EX01, you create the first public folder mailbox in a database named DB1. You view the Exchange Admin Center as shown in the exhibit. (Click the Exhibit button.)



Use the drop-down menus to select the answer choice that completes each statement.

Answer Area

If the server hosting the active copy of the DB1 database is unavailable, clients will be [**answer choice**]

- unable to access public folders.
- able to access all public folder data.
- able to access cached public folder data.

The public folder hierarchy [**answer choice**]

- only exists on EX01.
- only exists on EX02.
- has replicas on both EX01 and EX02.

Answer:

Answer Area

If the server hosting the active copy of the DB1 database is unavailable, clients will be [**answer choice**]

- unable to access public folders.
- able to access all public folder data.
- able to access cached public folder data.

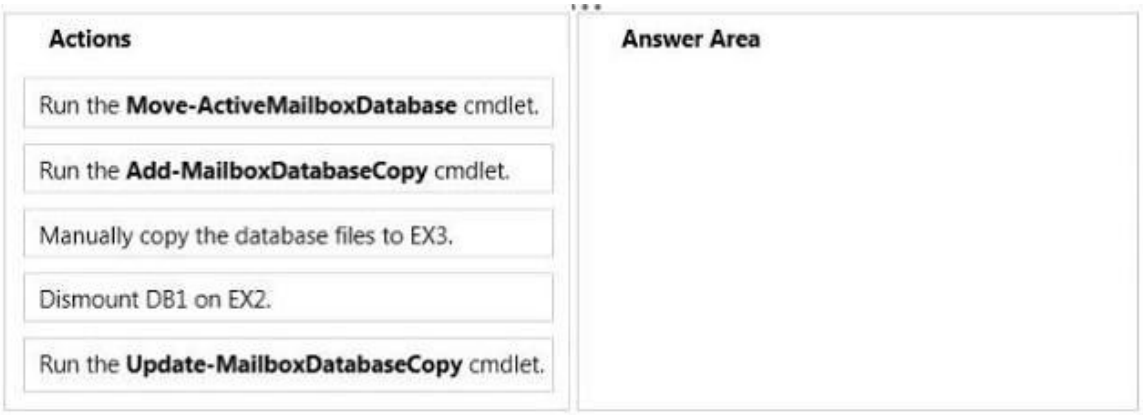
The public folder hierarchy [**answer choice**]

- only exists on EX01.
- only exists on EX02.
- has replicas on both EX01 and EX02.

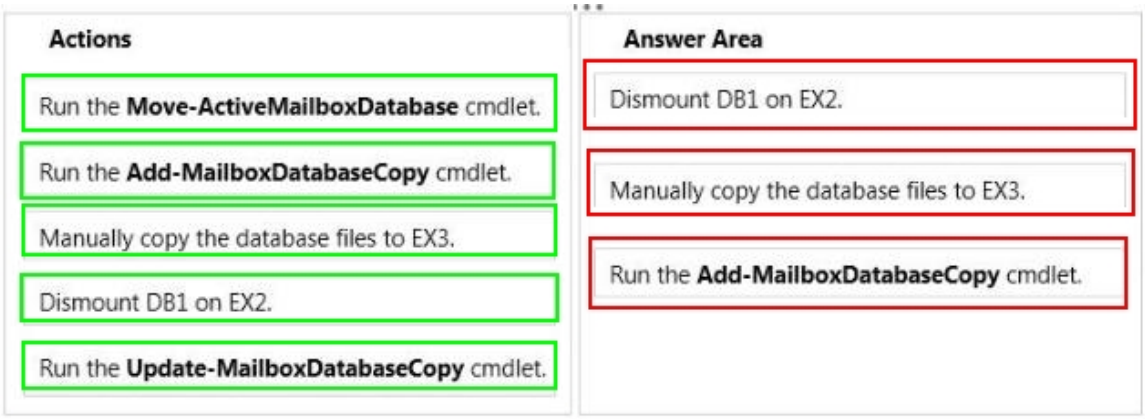
QUESTION 166

Drag and Drop Question

You have an Exchange Server 2013 organization that contains two servers named EX1 and EX2. EX1 and EX2 are the members of a database availability group (DAG) named DAG1. DAG1 contains a database named DB1. DB1 is active on EX1. You deploy a new Exchange Server 2013 server named Ex3. You add EX3 as a member of DAG1. You need to add a copy of DB1 to EX3 by using an offline copy of the database. Which three actions should you perform in sequence? (To answer, move the appropriate three actions from the list of actions to the answer area and arrange them in the correct order.)



Answer:

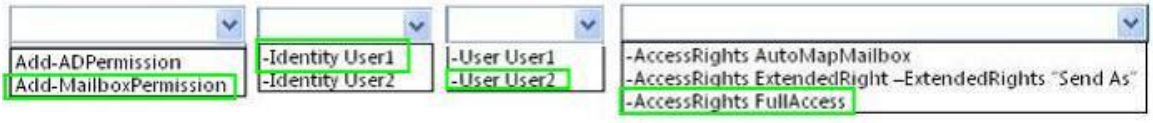


QUESTION 167
Hotspot Question
You have an Exchange Server 2013 organization. You have a user named User1 and a user named User2. Both users access their email by using Microsoft Outlook 2013. You need to ensure that User2 can access all of the email messages in the mailbox of User1 the next time User2 opens Outlook. What command should you run? (To answer, select the appropriate options in the answer area.)

Answer Area

Answer:

Answer Area

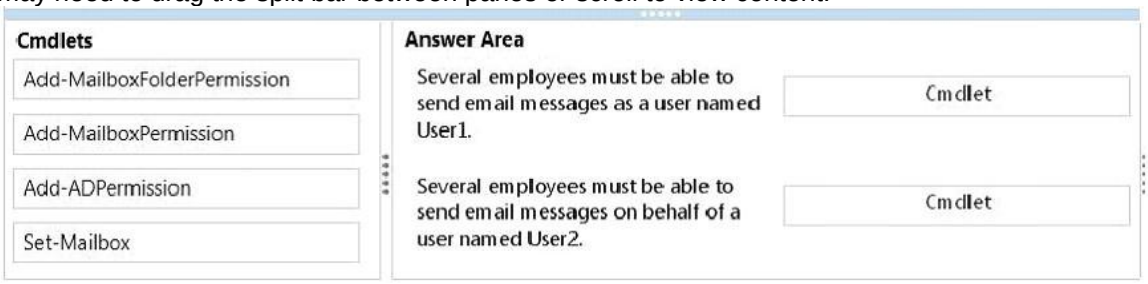


QUESTION 168
Drag and Drop Question

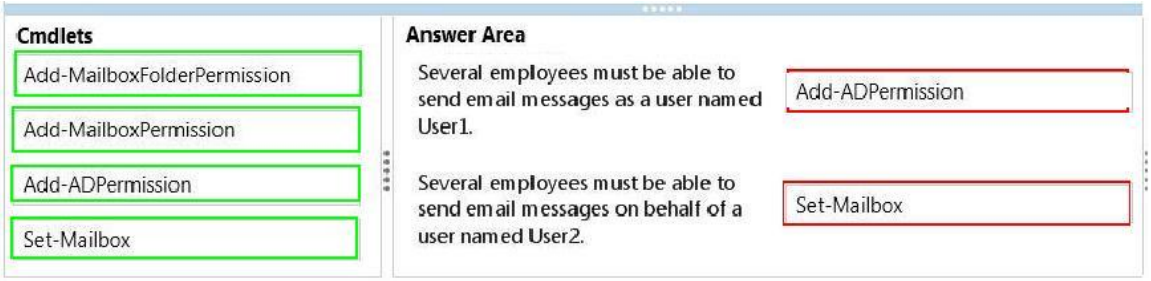
You have an Exchange Server 2013 organization that contains five servers. Several employees plan to use Microsoft Outlook to collaborate on some projects. You need to configure access to Outlook to meet the following requirements:

- Several employees must be able to send email messages as a user named User1.
- Several employees must be able to send email messages on behalf of a user named User2.

Which cmdlets should you use? To answer, drag the appropriate crndlet to the correct requirement in the answer area. Each crndlet may be used once, more than once, or not at all. Additionally, you may need to drag the split bar between panes or scroll to view content.



Answer:



QUESTION 169

You have an Exchange Server 2013 organization. You need to ensure that users receive a notification if the delivery of a message is delayed for more than one hour. Which cmdlet should you use?

A. Set-FrontEndTransportService
B. Set-MailboxTransportService
C. Set-Tra nsportConfig
D. Set-TransportService

Answer: D

Explanation:

http://technet.microsoft.com/en-us/library/jj215682(v=exchg.150).aspx

EXAMPLE 1

This example sets the DelayNotificationTimeout parameter to 1 hour for the Transport service on a Mailbox server named Mailbox01.

Set-TransportService Mailbox01 -DelayNotificationTimeout 1:00:00

DelayNotificationTimeout.

The DelayNotificationTimeout parameter specifies how long the server waits before it generates a delayed delivery status notification (DSN) message. The default value is 4 hours. To specify a value, enter it as a time span: dd.hh:mm:ss where d = days, h = hours, m = minutes, and s = seconds. For example, to specify 3.5 hours for this parameter, use 03:30:00. The valid input range for this parameter is from 00:00:01 through 30.00:00:00. The value of the DelayNotificationTimeout

parameter should always be greater than the value of the TransientFailureRetryCount parameter multiplied by the value of the TransientFailureRetryInterval parameter.

QUESTION 170

Hotspot Question

Your network contains an Active Directory forest named contoso.com. The forest contains two domains named contoso.com and nwtraders.com. You plan to deploy a new Exchange Server 2013 organization named Contoso. You need to ensure that you can deploy the first Exchange Server 2013 server to the forest root domain. What command should you run before you deploy the first Exchange Server 2013 server? (To answer, select the appropriate options in the answer area.)

Answer Area

Answer:

Answer Area

QUESTION 171

You have an Exchange Server 2010 organization. You deploy a server that has Exchange Server 2013 installed. You plan to install five additional servers that have Exchange Server 2013 installed. You are a member of the Organization Management management role group. Your company hires an external IT consultant named Admin1. The company's security policy states that all external consultants must have the minimum number of required permissions on the network. You need to ensure that Admin1 can install a server named EX2. The solution must meet the requirements of the security policy. Which two tasks should you perform? (Each correct answer presents part of the solution. Choose two.)

A. Add Admin1 to the Exchange Server role group.
B. Create a new management role and a new role assignment policy.
C. Run setup and specify the/newprovisionectservenex2 parameter.
D. Add Admin1 to the Delegated Setup management role group.

Answer: CD

Explanation:

http://technet.microsoft.com/en-gb/library/dd876881(v=exchg.150).aspx

Delegated Setup.

The Delegated Setup 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 2013. 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. Administrators who are members of the Delegated Setup role group can deploy servers running Exchange 2013 that have been previously provisioned by a member of the Organization Management role group. Members of the Delegated Setup role group can only deploy Exchange 2013 servers. They can't manage the server after it's been deployed.

To manage a server after it's been deployed, a user must be a member of the Server Management role group.

QUESTION 172

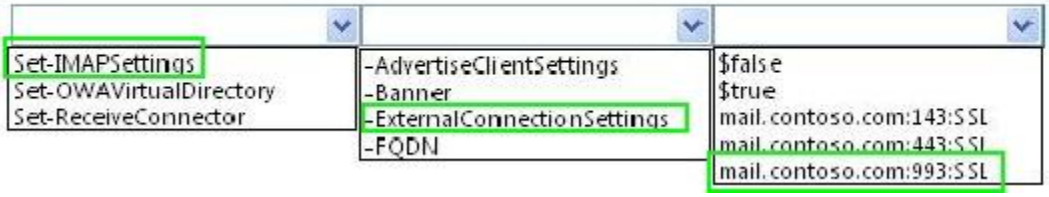
Hotspot Question

Your company has an Exchange Server 2013 organization named contoso.com. All users run Microsoft Outlook 2010 or Outlook 2013. The company recently acquired another company named A. Datum Corporation. All of the users at A. Datum run Linux-based computers and use a third-party IMAP client to access their email messages. You configure IMAP over SSL to use the external URL of mail.contoso.com. You need to publish the IMAP settings to Outlook Web App. What command should you run? (To answer, select the appropriate options in the answer area.)

Answer Area

Answer:

Answer Area



QUESTION 173

You have an Exchange Server 2013 organization. The help desk reports that users fail to access their mailbox by using the URL http://mail.contoso.com. All of the users successfully connect to their mailbox by using Exchange ActiveSync. You need to ensure that all of the users can access their mailbox by using the URL http://maif.contoso.com. What should you configure on a Client Access server?

A. From Internet Information Services (IIS) Manager, configure HTTP Response Headers on the OWA virtual directory.
B. From Exchange Admin Center, create a new Outlook Web App mailbox policy.
C. From File Explorer, modify the permissions of the Web.config file in the Default Web Site folder.
D. From Internet Information Services (IIS) Manager, configure HTTP Redirect on the default web site.

Answer: D

Explanation:

http://technet.microsoft.com/en-us/library/aa998359(v=exchg.150).aspx

Use IIS Manager to simplify the Outlook Web App URL and force redirection to SSL:

1. Start IIS Manager.
2. Expand the local computer, expand Sites, and then click Default Web Site.
3. At the bottom of the Default Web Site Home pane, click Features View if this option isn't already selected.
4. In the IIS section, double-click HTTP Redirect.
5. Select the Redirect requests to this destination check box.
6. Type the absolute path of the /owa virtual directory. For example, type

https://mail.contoso.com/owa.
7. Under Redirect Behavior, select the Only redirect requests to content in this directory (not subdirectories) check box.
8. In the Status code list, click Found (302).
9. In the Actions pane, click Apply.
10. Click Default Web Site.
11. In the Default Web Site Home pane, double-click SSL Settings.
12. In SSL Settings, clear Require SSL.
Note:
If you don't clear Require SSL, users won't be redirected when they enter an unsecured URL. Instead, they'll get an access denied error.

QUESTION 174

Hotspot Question
You have an Exchange Server 2013 organization that contains four servers. The servers are configured as shown in the following table.

Server name	Role	Active Directory site name
EX1	Mailbox server Client Access server	Site1
EX2	Mailbox server	Site1
EX3	Mailbox server Client Access server	Site2
EX4	Mailbox server	Site2

You run Get-TransportConfig and receive the output shown in the exhibit. (Click the Exhibit button.)

Use the drop-down menus to select the answer choice that completes each statement.

Answer Area

Shadow copies of messages will be created on [answer choice]

- servers in all sites.
- the local server only.
- servers in the same site only.
- servers in the remote site only.

The maximum duration that shadow copies of messages will be stored is [answer choice]

- two minutes.
- three hours.
- two days.
- four day.

Answer:

Answer Area

Shadow copies of messages will be created on [answer choice]

- servers in all sites.
- the local server only.
- servers in the same site only.
- servers in the remote site only.

The maximum duration that shadow copies of messages will be stored is [answer choice]

- two minutes.
- three hours.
- two days.
- four day.

QUESTION 175

You have an Exchange Server 2013 organization. You deploy the anti-spam features of Exchange Server 2013. You need to specify the spam quarantine mailbox. Which cmdlet should you run?

A. Set-Mai IboxJunkEmailConfiguration
B. Set-ContentFilterConfig
C. Set-MalwareFilterPolicy
D. Set-SenderFilterConfig

Answer: B

Explanation:

Configure a Spam Quarantine Mailbox.

Messages determined to be spam by the Content Filter agent can be directed to a spam quarantine mailbox. If the spam confidence level (SCL) quarantine threshold is enabled, all messages that are quarantined are wrapped as non-delivery reports (NDR) and are sent to the SMTP address that you specify as the spam quarantine mailbox. You can review quarantined messages and release them to their intended recipients by using the Send Again feature in Microsoft Outlook. By default, anti-spam features aren't enabled in the Transport service on a Mailbox server. Typically, you only enable the anti-spam features on a Mailbox server if your Exchange organization doesn't do any prior anti-spam filtering before accepting incoming messages. For more information, see Enable Anti-Spam Functionality on a Mailbox Server. The person responsible for the spam quarantine mailbox can view potentially private and sensitive messages, and then send mail on behalf of anybody in the Exchange organization.

Step 1: Verify content filtering is enabled.

Run the following command to verify the Content Filter agent is installed and enabled on the

Exchange server:
Get-TransportAgent "Content Filter Agent"
Run the following command to verify content filtering is enabled:
Get-ContentFilterConfig | Format-List Enabled
Step 2: Create a dedicated mailbox for spam quarantine.
To create a dedicated spam quarantine mailbox, follow these steps:
- Create a dedicated Exchange database
We recommend that you create a dedicated database for the spam quarantine mailbox. The spam quarantine mailbox should have a large database, because if the storage quota limit is reached, messages will be lost. For more information, see Manage Mailbox Databases in Exchange 2013.
- Create a dedicated mailbox and user account
We recommend that you create a dedicated mailbox and Active Directory user account for the spam quarantine mailbox.
Step 3: Specify the spam quarantine mailbox
Set-ContentFilterConfig -QuarantineMailbox <SmtpAddress>
This example sends all messages that exceed the spam quarantine threshold to spamQ@contoso.com.
Set-ContentFilterConfig -QuarantineMailbox spamQ@contoso.com
http://technet.microsoft.com/en-us/library/aa996791.aspx
http://technet.microsoft.com/en-us/library/aa997692(v=exchg.141).aspx
http://technet.microsoft.com/en-us/library/bb123746(v=exchg.150).aspx
http://jjstellato.blogspot.co.uk/2013/01/exchange-2013-enable-antispam-and.html

QUESTION 176
Your network contain an Active Directory forest. The forest contains a single domain named contoso.com. The network contains a legacy mail system that uses a SMTP namespace of contoso.com. You plan to deploy Exchange Server 2013. There will be a period of interoperability while the email is migrated from the legacy system to Exchange Server 2013. During the period of interoperability, you need to ensure that all incoming email is received by an Exchange Server 2013 server, and then routed to the legacy mail system if an Exchange Server email recipient cannot be found. You configure the firewall in the perimeter network to route SMTP traffic to the Exchange Server 2013 organization. What should you do next?

A. Modify the existing accepted domain for contoso.com and create a new Send connector.
B. Add a new external relay accepted domain for contoso.com and create a new Send connector.
C. Add a new authoritative domain for contoso.com and create a new email address policy.
D. Add a new internal relay accepted domain for contoso.com and create a new email address policy.

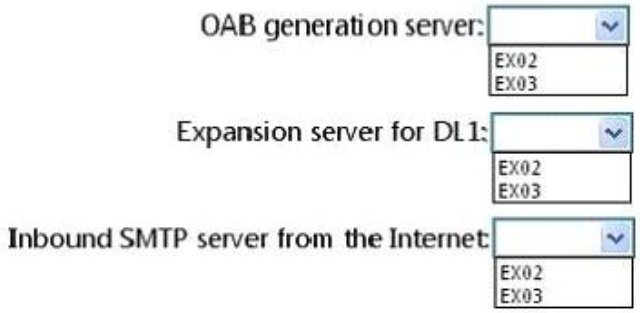
Answer: A
Explanation:
http://technet.microsoft.com/en-gb/library/bb124423(v=exchg.150).aspx
Step 1: Modify accepted domain for contoso.com and make it an internal relay domain.
Step 2: Create a new send connector which routes mail for the contoso.com namespace to the legacy namespace -if a recipient cannot be found in the Exchange org.

QUESTION 177
Hotspot Question
You have an Exchange Server 2013 organization that contains three servers. The servers are configured as shown in the following table.

Server name	Role(s)	Configuration
EX01	Mailbox server Client Access server	OAB generation server Expansion server for DL1
EX02	Client Access server	*Not applicable*
EX03	Mailbox server	*Not applicable*

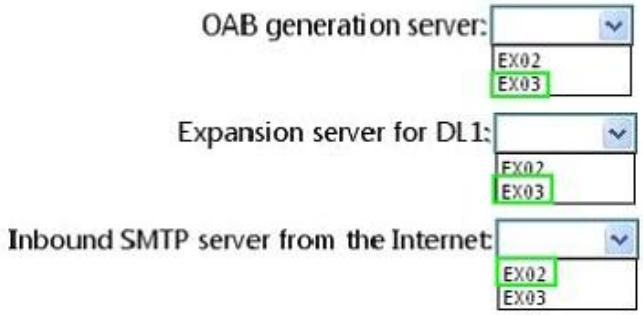
All inbound email messages from the Internet are routed through EX01. You plan to remove EX01 from the organization. You need to ensure that all of the functionalities of EX01 are transferred to EX02 and EX03. The solution must minimize administrative effort. Which functionality should you transfer to each server? (To answer, select the appropriate server for each functionality in the answer area.)

Answer Area



Answer:

Answer Area



QUESTION 178

Hotspot Question

You have an Exchange Server 2013 organization that contains a database availability group (DAG) named DAG1. DAG1 contains two servers named EX01 and EX02. On EX01, you have three networks. The networks are configured as shown in the following table.

Network name	Subnet	Connected to
DAG1\DAGNetwork01	192.168.1.0/24	Corporate LAN
DAG1\DAGNetwork02	10.0.0.0/24	EX02
DAG1\DAGNetwork03	10.1.0.0/24	iSCSI

You need to ensure that DAGNetwork02 is the primary replication network and DAGNetwork03 is

configured for iSCSI traffic only. What two commands should you run? (To answer, select the appropriate options in the answer area.)

Answer Area

Answer:

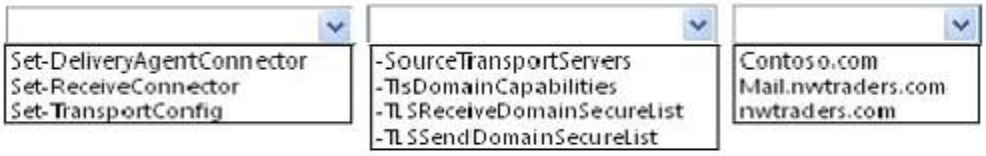
Answer Area

QUESTION 179

Hotspot Question

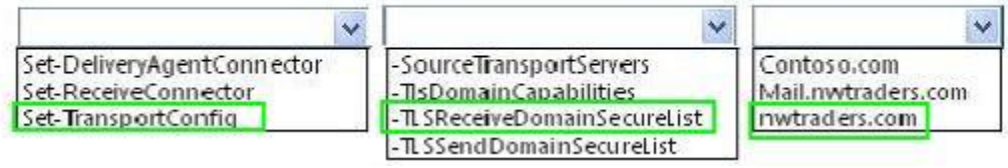
You have an Exchange Server 2013 organization that contains an accepted domain named contoso.com. A partner company has an Exchange Server 2013 organization named mvtraders.com. Nwtraders.com contains an SMTP server named mail.nwtraders.com. Both organizatiosn only use certificates from the same trusted third-party certification authority (CA). You need to ensure that all email messages received from the SMTP domain named nwtraders.com are protected by using mutual TLS. What command should you run? (To answer, select the appropriate options in the answer area.)

Answer Area



Answer:

Answer Area



QUESTION 180

You have an Exchange Server 2013 organization that contains 5,000 mailboxes. A user named User1 tests several Windows Phone devices. You need to ensure that User1 can connect more than 20 Windows Phone devices to his mailbox. Which cmdlet should you run?

A. Set-ThrottlingPolicy

B. Set-MobileMailboxPolicy
C. Set-ActiveSyncMailboxPolicy
D. Set-CasMailbox

Answer: A
Explanation:
Example 1:
Set-ThrottlingPolicy-EasmaxDevices 20
Example 2:
New-Throttlingpolicy "Increased ActiveSync Devices" -EasMaxDevices 20
Set-Mailbox steve-ThrottlingPolicy "Increased ActiveSync Devices"
Example 3:
Set-Throttlingpolicy "Increased ActiveSync Devices" -EasMaxDevices 20
http://technet.microsoft.com/en-gb/library/dd298094(v=exchg.150).aspx
http://www.msexchange.org/kbase/ExchangeServerTips/ExchangeServer2010/Mobility/HowtoincreasethemaximumnumberofActiveSyncDevicesforaUser.html
http://thoughtsofanidlemind.com/2014/01/15/eas-device-partnerships/
http://www.slipstick.com/exchange/cmdlets/allow-more-activesync-devices/

QUESTION 181
You deploy an Exchange Server 2013 organization to a test network for evaluation. You install the Mailbox server role and the Client Access server role on a server named ex01.contoso.com. You do not perform any other configurations. All of the ports from the Internet to ex01.contoso.com are open. You successfully connect to ex01.contoso.com from the Internet and from the internal network. You need to identify which types of Exchange Server clients will connect successfully to the organization without any further configurations. What should you identify?

A. internal Outlook Web App connections
B. Android Phones using Activesync
C. Windows RT devices running the Mail app
D. Windows Phones that use Exchange ActiveSync

Answer: A
Explanation:
Not B
All Android Phones require the AllowNonProvisionableDevices parameter set to $True to sync successfully out of box with Exchange 2013 and this parameter is set to $false by default.
Not C
All Windows RT devices running the mail App require the AllowNonProvisionableDevices parameter set to $True to sync successfully out of box with Exchange 2013 and this parameter is set to $false by default.
Not D
All Windows Phones require the AllowNonProvisionableDevices parameter set to $True to sync successfully out of box with Exchange 2013 and this parameter is set to $false by default. The AllowNonProvisionableDevices parameter specifies whether all mobile phones can synchronize with the server running Exchange. When set to $true, the AllowNonProvisionableDevices parameter enables all mobile phones to synchronize with the Exchange server, regardless of whether the phone can enforce all the specific settings established in the Exchange ActiveSync policy. This also includes mobile phones managed by a separate device management system. When set to $false, this parameter blocks mobile phones that aren't provisioned from synchronizing with the Exchange server. The default value is $false.
http://technet.microsoft.com/en-gb/library/bb123756(v=exchg.141).aspx
http://exchangeserverpro.com/activesync-policies-cause-test-activesyncconnectivity-to-fail/

QUESTION 182
You have an Exchange Server 2013 organization. You create a public folder. You assign an email address to the public folder. You need to ensure that only a user named User1 can add content to the public folder by using email. Which cmdlet should you run?

A. Set-MailPublkFolder
B. Set-PublicFolder
C. Set-Mailbox
D. Add-PublicFolderCMentPermission

Answer: A
Explanation:
Set-MailPublicFolder.
This cmdlet is available in on-premises Exchange Server 2013 and in the cloud-based service. Use the Set-MailPublicFolder cmdlet to configure the mail-related settings of mail-enabled public folders. If you want to configure basic settings that aren't mail related, use the Set-PublicFolder cmdlet.
EXAMPLE 1
Set-MailPublicFolder -Identity MyPublicFolder@contoso.com -AcceptMessagesOnlyFrom "User1"
EXAMPLE 2
This example sets the primary SMTP address of the mail-enabled public folder MyPublicFolder@contoso.com to MyPublicFolder@fabrikam.com.
Set-MailPublicFolder -Identity MyPublicFolder@contoso.com -PrimarySmtpAddress MyPublicFolder@fabrikam.com
http://technet.microsoft.com/en-us/library/aa997560(v=exchg.150).aspx
http://technet.microsoft.com/en-us/library/bb123707(v=exchg.150).aspx
http://technet.microsoft.com/en-gb/library/bb397214(v=exchg.150).aspx

QUESTION 183
You have an Exchange Server 2013 organization that contains 20 servers. You plan to deploy Exchange Server 2013 RTM Cumulative Update 1 (CU1) to the first Exchange server in the organization. You need to ensure that a user named ExehangeAdmin can deploy CU1 to the first server. The solution must minimize the number of permissions assigned to ExehangeAdmin. To which groups should you add ExehangeAdmin?

A. Schema Admins, Domain Admins, and Enterprise Admins
B. Schema Admins, Domain Admins, and Delegated Setup
C. Domain Admins and Organization Management
D. Enterprise Admins and Organization Management

Answer: A
Explanation:
http://technet.microsoft.com/en-us/exdeploy2013/Checklist?state=2419-W-CABEAgAAQAAAAUEAAQAAAAg~
A: Both Schema Admins and Enterprise Admins membership is needed to update the schema and prepare AD.
NOT B: Delegated Setup can be used to install the 2nd server, not the first.
NOT C: Both Schema Admins and Enterprise Admins membership is needed to update the schema and prepare AD. The user account installing the server is added to the Organization Management group during installation.
NOT D: Both Schema Admins and Enterprise Admins membership is needed to update the schema and prepare AD. The user account installing the server is added to the Organization Management group during installation.

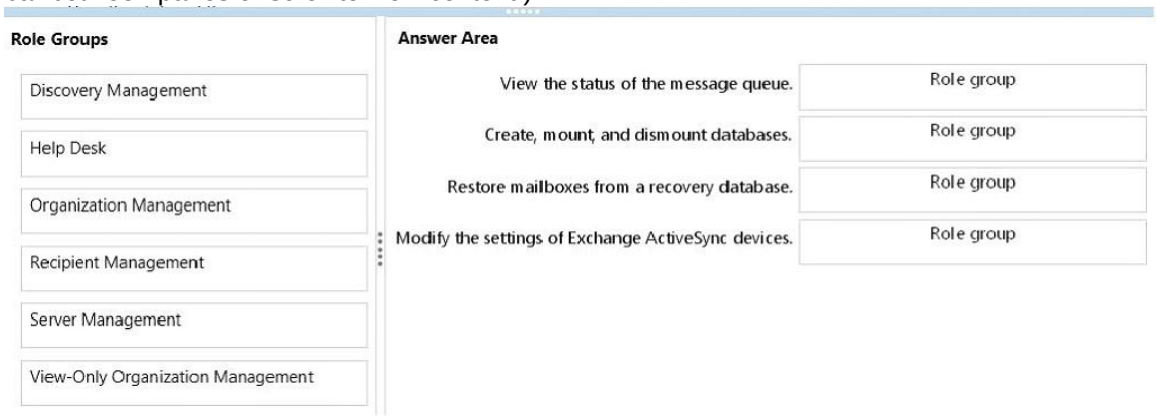
QUESTION 184
You have an Exchange Server 2013 organization. An Active Directory administrator is concerned about the permissions assigned to a group named Exchange Trusted Subsystem. Exchange Trusted Subsystem has a member named Exchange Windows Permissions. You need to show the Active Directory administrator all of the permissions assigned to Exchange Trusted Subsystem. What should you use?

A. ADSI Edit
B. Active Directory Sites and Services
C. Dsget
D. Active Directory Users and Computers

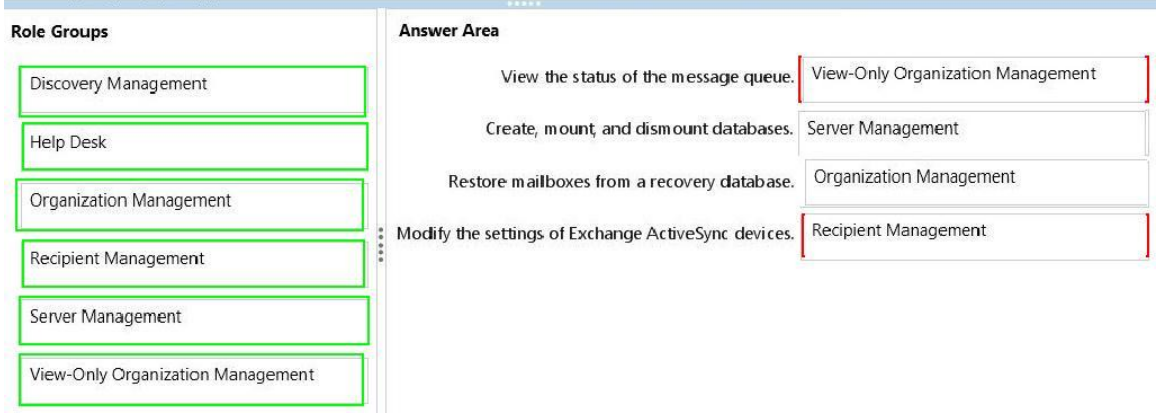
Answer: A
Explanation:
http://technet.microsoft.com/en-us/library/cc773354(v=WS.10).aspx

QUESTION 185
Drag and Drop Question You have an Exchange Server 2013 organization. You plan to delegate the following administrative tasks:
- View the status of the message queue.
- Create, mount, and dismount databases.
- Restore mailboxes from a recovery database.
- Modify the settings of Exchange ActiveSync devices.

You need to identify which role group must be used to delegate each administrative task. The solution must ensure that the role group that has the fewest administrative privileges is used. Which role groups should you identify? (To answer, drag the appropriate role groups to the correct tasks. Each role group may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.)



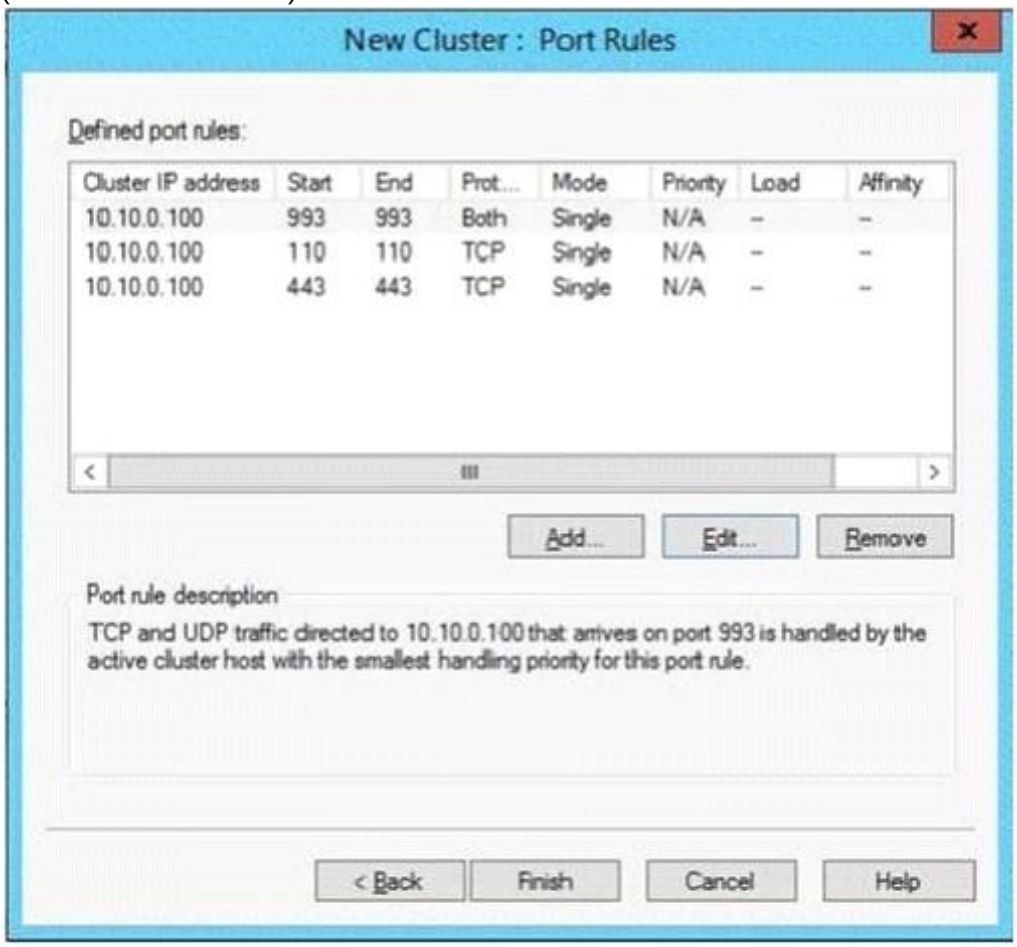
Answer:



QUESTION 186

Hotspot Question

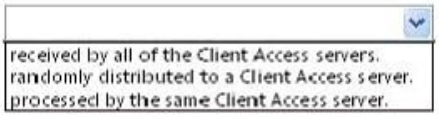
Your network contains three Exchange Server 2013 servers that have the Client Access server role installed. Each server is configured as a POP3 server and an IMAP4 server. You deploy the Network Load Balancing (NLB) feature on the servers and configure NLB as shown in the exhibit. (Click the Exhibit button.)



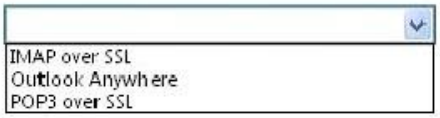
Use the drop-down menus to select the answer choice that completes each statement.

Answer Area

If a client has an existing connection to 10.10.0.100:443, subsequent connections will be [**answer choice**]



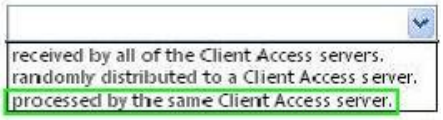
Connections that use [**answer choice**] will NOT be load balanced by NLB.



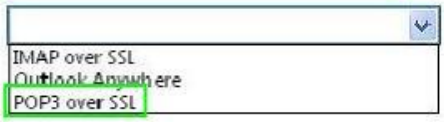
Answer:

Answer Area

If a client has an existing connection to 10.10.0.100:443, subsequent connections will be [**answer choice**]



Connections that use [**answer choice**] will NOT be load balanced by NLB.



QUESTION 187

Hotspot Question

You have an Exchange Server 2013 organization that contains three moderated distribution groups named DG1, DG2, and DG3. DG3 is a member of DG2. You need to exclude from moderation the email messages sent from the members of DG3 to the members of DG1. The solution must maintain moderation for the email messages sent from all other users. What command should you run? (To answer, select the appropriate options in the answer area.)

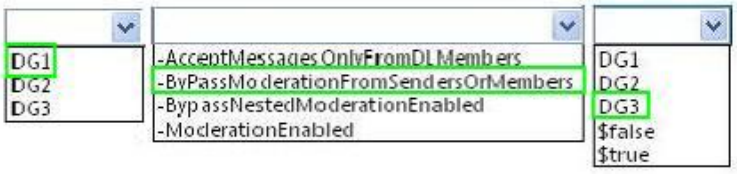
Answer Area

Set-DistributionGroup –Identity

Answer:

Answer Area

Set-DistributionGroup –Identity



QUESTION 188

You have an Exchange Server organization. The organization contains a server named EX01 that has Exchange Server 2010 installed and a server named EX02 that has Exchange Server 2013 installed. Your mailbox is hosted on EX01. You need to access the Exchange Adrnin Center (EAC). Which URL should you use?

A. https://EX01/ecp?ExchClientVer= 14
B. https://EX02/ecp?ExchClientVer= 15
C. https://EX02/eac?ExchClientVer=15
D. https://EX01/ecp?ExchCfientVer=15

Answer: B
Explanation:
http://www.cgoosen.com/2013/07/how-to-access-exchange-admin-center-eac-in-exchange-2013-during-coexistence/
http://consulting.risualblogs.com/blog/2013/06/26/exchange-2013-coexistence-ecp-redirects-to-2010-ecp-2/
http://msexchangeguru.com/2013/01/16/eac-exchange-2013/
http://blogs.technet.com/b/meamcs/archive/2013/05/04/exchange-2013-coexistence-ecp-your-mailbox-can-t-be-accessed-using-the-address-you-entered-please-obtain-the-correct-address.aspx

QUESTION 189
You have an Exchange Server 2013 organization. The organization contains four servers in the same Active Directory site. The servers are configured as shown in the following table. EXB and EX4 are members of a database availability group (DAG) named DAG1. All users use Microsoft Outlook 2013 to connect to their mailbox. You need to recommend a client access solution to ensure that all of the users can connect to their mailbox if EX1 or EX2 fails. What should you recommend?

Server name	Role
EX1	Client Access server
EX2	Client Access server
EX3	Mailbox server
EX4	Mailbox server

A. Add a layer 4 hardware load balancer that balances RPC traffic.
B. Add a layer 7 hardware load balancer that balances the traffic on port 443.
C. Add a layer 7 hardware load balancer that balances RPC traffic.
D. Replicate all of the databases in DAG1 to both DAG1 members.

Answer: B
Explanation:
In Exchange 2013, RPC over TCP has been disabled. All outlook communications are now through RPC over HTTP (Outlook Anywhere). This unifies the CAS protocol methods and provides a stable and reliable connectivity network between clients and server and between CAS and Mailbox Server. It also reduces the number of namespaces required. It also eliminates end user interruptions. Hence moving mailboxes around in DAG and moving mailboxes between mailbox databases are now easy.
http://blog.loadbalancer.org/load-balancing-exchange-2013/
http://windowsitpro.com/blog/exchange-2013-dumps-cas-arrays

QUESTION 190
Your company has a main office and three branch offices. The main office is located in Austin. The branch offices are located in Denver, San Diego, and Chicago. The network contains an Active Directory forest. The forest contains a single domain. Each office is configured as an Active

Directory site. The site in Austin contains four domain controllers that run Windows Server 2008 R2 and are configured as global catalog servers. The sites in Denver, San Diego, and Chicago each contain a read-only domain controller (RODC) that runs Windows Server 2008 R2. No other domain controllers exist on the network. You plan to deploy an Exchange Server 2013 organization. Exchange Server 2013 servers will be deployed in the Austin, Denver, and San Diego sites. Users from the Chicago site will access their mailbox remotely. You need to recommend changes to the Active Directory infrastructure to support the planned deployment of Exchange Server 2013. What should you recommend?

A. Replace the RODCs in the Denver and San Diego sites with domain controllers that are configured as global catalog servers.
B. Configure the RODCs in the Denver and San Diego sites as read-only global catalog servers.
C. Configure Active Directory automatic site coverage for the Chicago site.
D. Upgrade all of the RODCs to Windows Server 2012.

Answer: A
Explanation:
http://technet.microsoft.com/en-us/library/aa996719.aspx
There must be a writable copy of the global catalog at each site where an Exchange 2013 server is to be installed.

QUESTION 191
How would you disable the anti malware filtering and ensure that engine updates from microsoft are downloaded and updated.

A. Disable-Antimalwareagent.ps1
B. Set-malwarefilteringserver
C. Disable-Antimalwarescanning.ps1 (probable option)
D. Update-MalwareFilteringServer.ps1 (guessed option)

Answer: B
Explanation:
Disable or Bypass Anti-Malware Scanning.
Applies to: Exchange Server 2013.
In Microsoft Exchange Server 2013, you can disable or bypass malware filtering of all email messages in transit on a server. This must be done on a Mailbox server. You may want to disable Exchange 2013 malware filtering if you are using another product for malware filtering. When malware filtering is disabled, the Exchange malware agent is unhooked and not running, and engine updates are not kept up-to-date.
Important:
Bypassing malware filtering should only be done when troubleshooting a problem. When malware filtering is bypassed, the Exchange malware agent remains hooked, and engine updates are kept up-to-date. However, malware filtering is skipped while you attempt to resolve whatever problems you are encountering. After you have finished troubleshooting, you should restore malware filtering.
http://technet.microsoft.com/en-us/library/jj150526(v=exchg.150).aspx
http://www.ntweekly.com/?p=2813

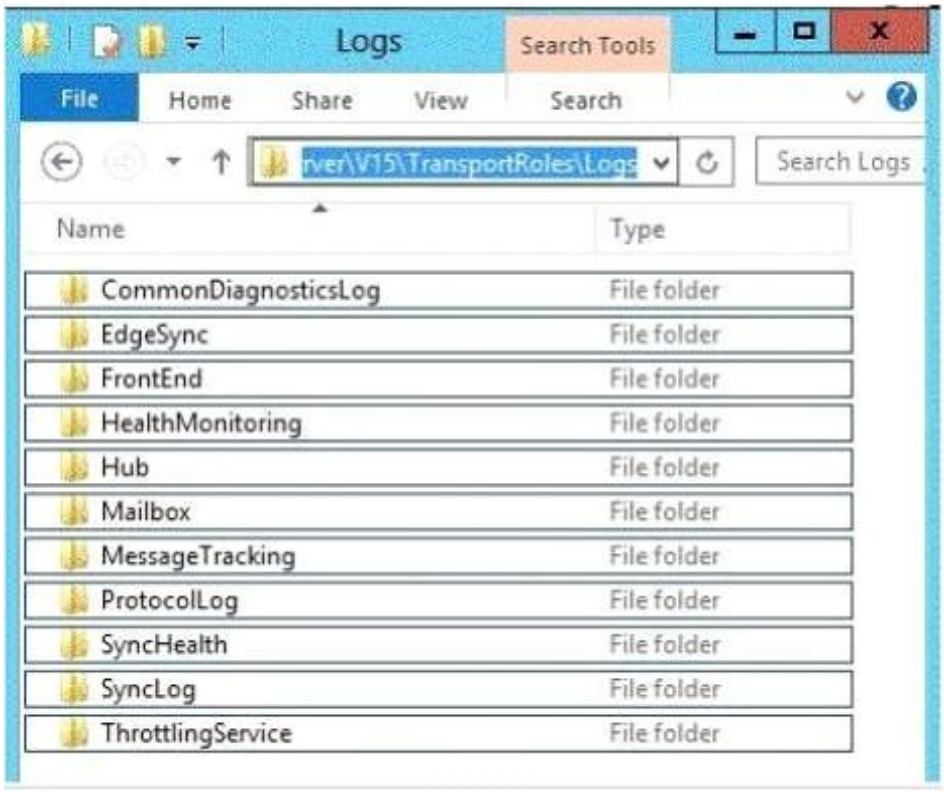
QUESTION 192
You need to install and configure anti-spam and antimalware filtering. Which servers should you install the anti-spam agents and enable the anti-spam and antimalware filtering? (Choose two.)

A. You should install the anti-spam agents on the Client Access Servers only.
B. You should install the anti-spam agents on the Mailbox servers only.

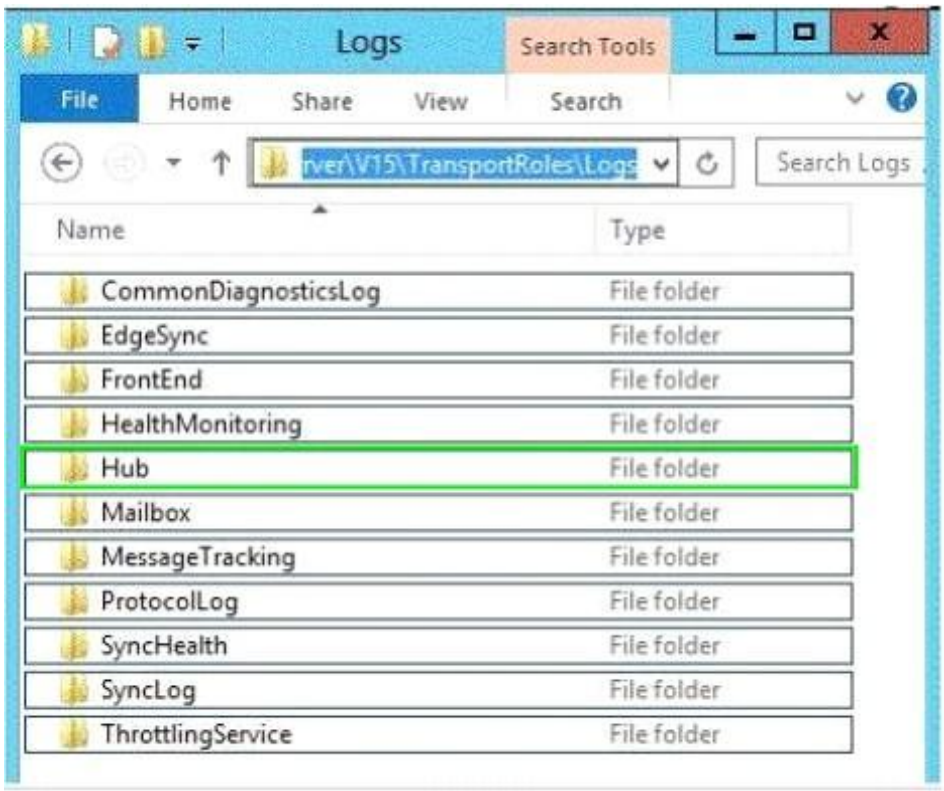
C. You should install the anti-spam agents on the Client Access Servers and the Mailbox Servers.
D. You should enable antimalware filtering on the Client Access Servers only.
E. You should enable antimalware filtering on the Mailbox servers only.
F. You enable antimalware filtering on the Client Access Servers and the Mailbox Servers.

Answer: BE
Explanation:
http://howexchangeworks.com/2013/06/connection-filtering-in-exchange-2013.html
In Exchange 2013, the anti-spam agents can only be installed on the Mailbox role. But, the connection filtering which is very useful in fighting spam emails is not available in 2013. Same goes for the attachment filter. Even though CAS proxies emails back and forth (if setup correctly), it is a stateless proxy and can't have any anti-spam agents on it.
http://www.jaapwesselius.com/2013/01/10/installing-exchange-server-2013-part-iii/
In Exchange 2013 the anti-spam functionality (through protocol agents) is running on the Mailbox Server and not on the Client Access Server so all mail, including all spam will hit the Mailbox Server when installed in a configuration as outlined in these blog post series. The anti-spam functionality is enabled using a Powershell script (.\EnableAntiSpamAgents.ps1) and offers Sender and Recipient filtering, content filtering, Sender Reputation and Sender ID filtering. To activate the ant-spam agents on the Mailbox Server open the Exchange Management Shell and enter the following commands:
`CD $Exscripts.\Install-AntiSpamAgents.ps1`
http://www.tlglearning.com/LinkClick.aspx?fileticket=dnonu0glRr8%3D&tabid=238
You can't enable the anti-spam agents on an Exchange 2013 Client Access Server.
https://social.technet.microsoft.com/Forums/exchange/en-US/5c9f1b51-4a93-4de4-964e-1f53afbb8e8b/how-to-configure-attachment-filter-agent-on-exchange-2013-
The Malware Filter runs on every 2013 Mailbox server to protect against malware and viruses.
http://blogs.dirteam.com/blogs/davestork/archive/2012/12/06/exchange-and-malware-protection.aspx

QUESTION 193
Hotspot Question
Your company has an Exchange Server 2013 organization. You configure domain security with a partner organization. You configure the required connectors. You plan to verify whether the partner organization configured the required settings for domain security. You enable logging for the Send connectors and the Receive connectors. You need to verify that the STARTTLS command is issued by an Exchange server when an email message is sent to the partner organization. Which log folder should you review? (To answer, select the appropriate folder in the answer area.)


Logs
Search Tools
File
Home
Share
View
Search
rver\V15\TransportRoles\Logs
Search Logs
Name
Type
CommonDiagnosticsLog File folder
EdgeSync File folder
FrontEnd File folder
HealthMonitoring File folder
Hub File folder
Mailbox File folder
MessageTracking File folder
ProtocolLog File folder
SyncHealth File folder
SyncLog File folder
ThrottlingService File folder

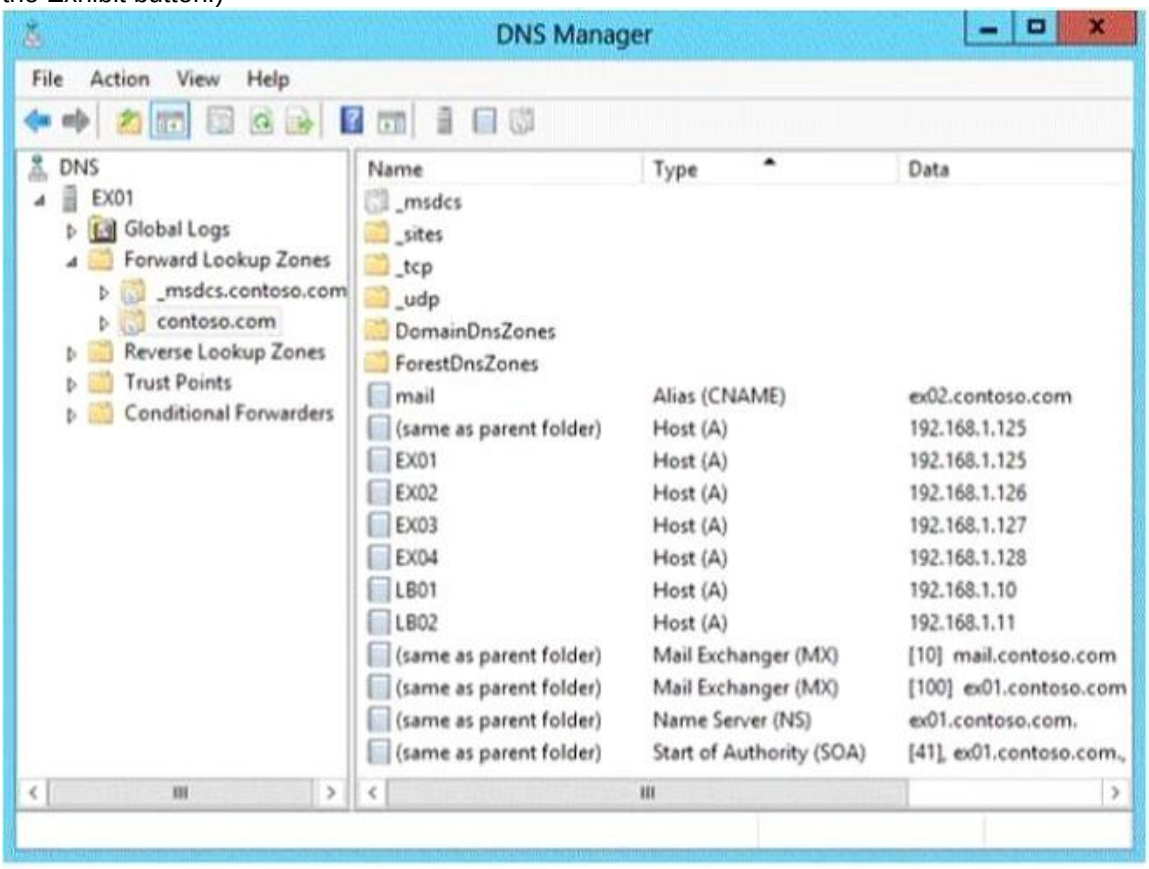
Answer:


Logs
Search Tools
File
Home
Share
View
Search
rver\V15\TransportRoles\Logs
Search Logs
Name
Type
CommonDiagnosticsLog File folder
EdgeSync File folder
FrontEnd File folder
HealthMonitoring File folder
Hub File folder
Mailbox File folder
MessageTracking File folder
ProtocolLog File folder
SyncHealth File folder
SyncLog File folder
ThrottlingService File folder

QUESTION 194

Hotspot Question

Your company has an Exchange Server 2013 organization. All servers have the Client Access server role and the Mailbox server role installed. The DNS Manager is shown in the exhibit. (Click the Exhibit button.)



Use the drop-down menus to select the answer choice that completes each statement.

Answer Area

The server named [**answer choice**] receives all incoming email from the Internet.

EX01
EX02
EX03
EX04
LB01
LB02

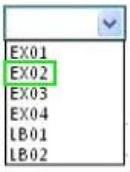
To load balance the inbound SMTP communication between two Exchange servers, [**answer choice**]

set the priority value of ex01.contoso.com to 10.
create a service location (SRV) record for EX02 that has a weight of 100.
create a mail exchanger (MX) record for LB01 that has a priority value of 10.
create a mail exchanger (MX) record for LB01 that has a priority value of 100.

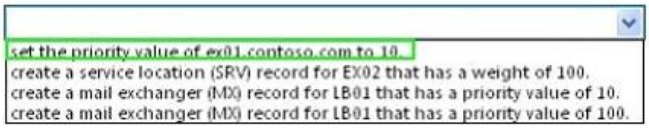
Answer:

Answer Area

The server named [**answer choice**] receives all incoming email from the Internet.



To load balance the inbound SMTP communication between two Exchange servers, [**answer choice**]



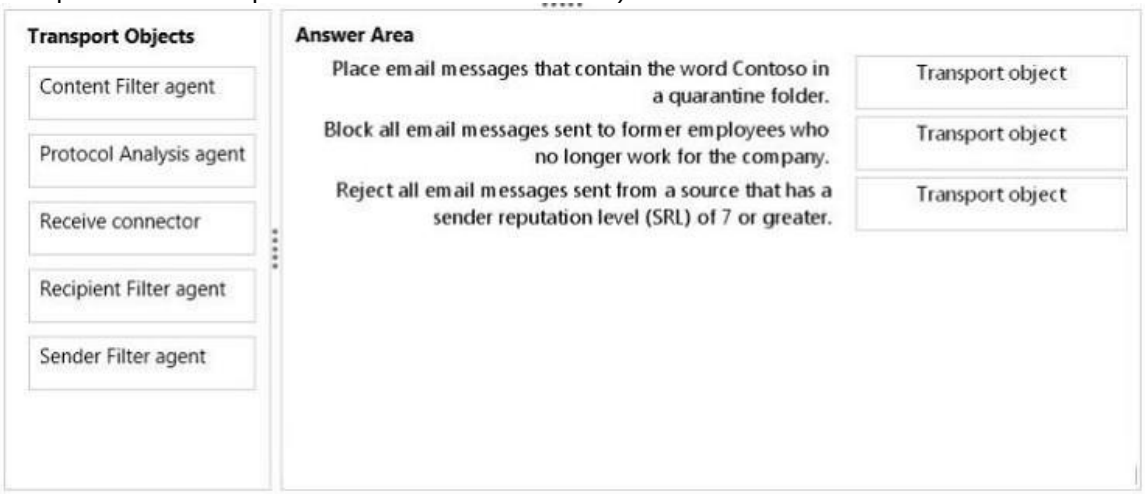
QUESTION 195

Drag and Drop Question

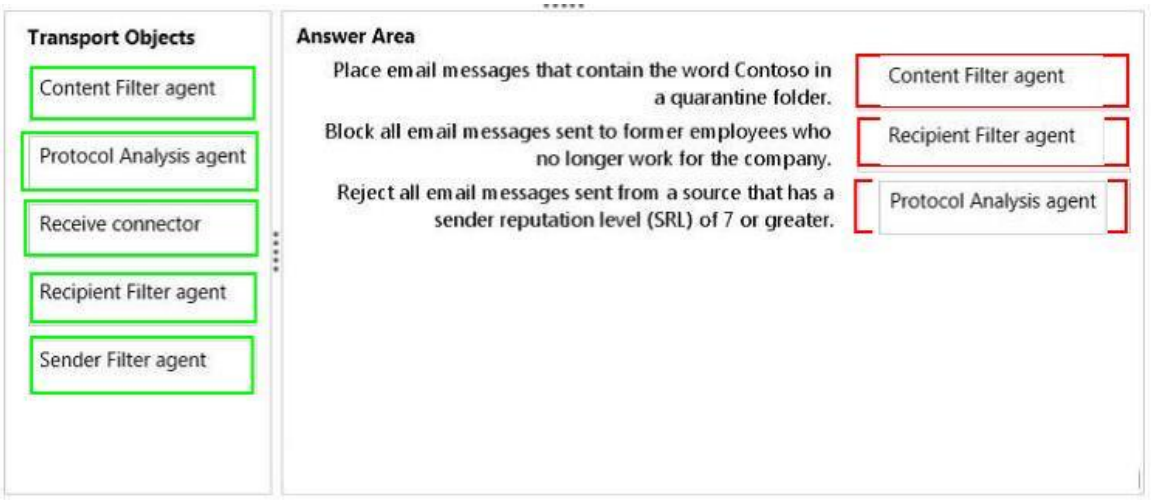
You have an Exchange Server 2013 organization that contains a server named EX1. EX1 has the Mailbox server role and the Client Access server role installed. You plan to enable anti-spam protection on EX1. You need to configure the message hygiene settings for email messages received from the Internet. The solution must meet the following requirements:

- Place email messages that contain the word Contoso in a quarantine folder.
- Block all email messages sent to former employees who no longer work for the company.
- Reject all email messages sent from a source that has a sender reputation level (SRL) of 7 or greater.

What should you configure? (To answer, drag the appropriate transport objects to the correct requirements. Each object may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.)



Answer:



QUESTION 196
Your company has offices in New York, Paris, and Montreal. An Active Directory site exists for each office. You have an Exchange Server 2013 organization that contains two servers in each site. One server in each site has the Mailbox server role installed and the other server in each site has the Client Access server role installed. You need to ensure that all of the outbound email from each site is routed through the Client Access server in that site. Which should you do?

A. Remove the Mailbox servers from the list of source servers on each Send connector.
B. Disable the Microsoft Exchange Transport service on each Mailbox server.
C. Run the Set-SendConnector cmdlet and specify the -FrontendProxyEnabted.True parameter.
D. Run the Set-TransportConfig cmdlet and specify the -InternatSMTPServers:$nult parameter.

Answer: C
Explanation:
http://exchangeserverpro.com/exchange-2013-front-end-proxy/
http://blogs.technet.com/b/exchange/archive/2013/01/25/exchange-2013-client-access-server-role.aspx
http://www.msexchange.org/articles-tutorials/exchange-server-2013/planning-architecture/exchange-2013-mail-flow-part3.html

QUESTION 197
You have an Exchange Server 2010 organization. Users access Outlook Web App by using the name mail.contoso.com. You deploy Exchange Server 2013 to the existing organization. You change the DNS record of mail.contoso.com to point to an Exchange Server 2013 Client Access server. The users report that they can no longer access their mailbox from Outlook Web App. The OWA virtual directory in Exchange Server 2010 is configured as shown in the exhibit. (Click the Exhibit button.) You need to ensure that the users on Exchange Server 2010 can access Outlook Web App. Which setting should you change?

A. WindowsAuthentication
B. FormsAuthentication
C. LegacyRedirectType
D. FailbackUri

Answer: A
Explanation:
Windows Authentication (NTLM) needs to be enabled on the Exchange 2010 Client Access Server to enable the Exchange 2013 Client Access Server to proxy connections.
Exchange Server Deployment Assistant.
Enable and configure Outlook Anywhere.
To allow your Exchange 2013 Client Access server to proxy connections to your Exchange 2007 and Exchange 2010 servers, you must enable and configure Outlook Anywhere on all of the Exchange 2007 and Exchange 2010 servers in your organization. If some Exchange 2007 or Exchange 2010 servers in your organization are already configured to use Outlook Anywhere, their configuration must also be updated to support Exchange 2013. When you use the steps below to configure Outlook Anywhere, the following configuration is set on each Exchange 2007 and Exchange 2010 server: The Outlook Anywhere external URL is set to the external hostname of the Exchange 2013 server. Client authentication, which is used to allow clients like Outlook 2013 to authenticate with Exchange, is set to Basic. Internet Information Services (IIS) authentication, which is used to allow Exchange servers to communicate, set to NTLM and Basic.

QUESTION 198
You have an Exchange Server 2013 organization that contains two Mailbox servers and two Client Access servers. You have a database availability group (DAG) that contains both Mailbox servers. You need to deploy public folders. What should you do first?

A. Run the New-PublicFolderDatabase cmdlet and specify the -Server parameter.
B. Run the New-PublicFolder cmdlet and specify the -Path parameter.
C. Run the New-Mailbox cmdlet and specify the -Publicfolder parameter.
D. Run the New-MailboxDatabase cmdlet and specify the -PublicFotderDatabase parameter.

Answer: C
Explanation:
Set Up Public Folders in a New Organization.
New-Mailbox -PublicFolder -Name MasterHierarchy
http://www.msexchange.org/articles-tutorials/exchange-server-2013/migration-deployment/migrating-publicfolders-exchange-2013-part1.html
http://www.msexchange.org/articles-tutorials/exchange-server-2013/migration-deployment/migrating-publicfolders-exchange-2013-part2.html

QUESTION 199

You have an Exchange Server 2013 organization. You need to install the Hub Transport server role on a new server. You install all the prerequisites for the Hub Transport role on the server. What should you do next?

A. From Windows PowerShell, run the Add-WindowsFeature cmdlet.
B. From Windows PowerShell, run the Install-TransportAgent.ps1 script.
C. At the command prompt, run Setup.com /M:Install /R:HT.
D. At the command prompt, run ServerManagerCmd.exe -IP Exchange-HUB.xml.

Answer: C

QUESTION 200
You have an Exchange Server 2013 server that has the Mailbox, Hub Transport, and Client Access server roles installed. You need to ensure that users can send and receive e-mail by using Windows Live Mail or Microsoft Outlook Express. What should you do on the server?

A. Install and then configure the SMTP server feature.
B. Start the Microsoft Exchange POP3 service and then set the startup type to Automatic.
C. Modify the properties of the MSExchangePOP3 (TCP-in) Windows Firewall rule.
D. Modify the properties of the MSExchangeMailSubmission - RPC (TCP-in) Windows Firewall rule.

Answer: B
Explanation:
By default, pop3 is set to manual.

QUESTION 201
You have an Exchange Server 2013 server named Server1. Server1 has a single mailbox database named DB1. You configure deleted items to be retained for 30 days. You need to ensure that each item that passes the retention period is removed daily between 2:00 and 6:00. What should you do?

A. Run the Set-RetentionPolicy cmdlet.
B. Run the Start-ManagedFolderAssistant cmdlet.
C. Modify the maintenance schedule for DB1.
D. Modify the messaging records management (MRM) schedule for Server1.

Answer: C
Explanation:
In the question it says nothing about a Retention policy.
To configure deleted items to be retained for 30 days we can do it on a database level, using this cmdlet:
Set-MailboxDatabase -Identity "DB1" -DeletedItemRetention 30.00:00:00
And after the above, configure the maintenance of DB1 using the Set-MailboxDatabase cmdlet with the - MaintenanceSchedule parameter.

QUESTION 202
You have an Exchange Server 2013 organization. You need to create a resource record in DNS to support Autodiscover from the Internet. What type of resource record should you create?

A. Host (A)
B. Text (TXT)
C. Pointer (PTR)

D. Mail exchange (MX)

Answer: A

QUESTION 203
You have an Active Directory forest named contoso.com. You install a new Exchange Server 2013 organization that contains a Client Access server named CAS1. You need to configure certificates in the organization to support the following client connections:
`Autodiscover Outlook Anywhere Exchange ActiveSync`
What should you do?

A. Reissue a self-signed certificate to CAS1.
B. Configure the default Web site on CAS1 to require SSL.
C. Issue a trusted certificate that contains multiple subject alternate names.
D. Install Active Directory Rights Management Service (AD RMS) on a member server.

Answer: C

QUESTION 204
You have an Exchange Server 2013 organization. The organization is authoritative for the domain contoso.com. You create a federated trust. You need to ensure that federated partners can automatically locate the Client Access servers in the organization. What should you create from an external DNS server?

A. an A record for autodiscover.contoso.com
B. an A record for FederatedSharing.contoso.com
C. an SRV record for _autodiscover._TCP._msdcs.contoso.com
D. an SRV record for _FederatedSharing._UDP._msdcs.contoso.com

Answer: A
Explanation:
As mentioned in another question, this should actually be a CNAME record, according to Technet, but I left this in here as an A record for contoso.com would need creating before the CNAME for autodiscover.contoso.com. The exam will only mention CNAME records though.

QUESTION 205
You have an Exchange Server organization. The organization contains a server named EX01 that has Exchange Server 2010 installed and a server named EX02 that has Exchange Server 2013 installed. Your mailbox is hosted on EX01. You need to access the Exchange Admin Center (EAC). Which URL should you use?

A. https://EX01/ecp?ExchClientVer= 14
B. https://EX02/ecp?ExchClientVer= 15
C. https://EX02/eac?ExchClientVer=15
D. https://EX01/ecp?ExchCfientVer=15

Answer: B
Explanation:
http://technet.microsoft.com/en-us/library/jj150562(v=exchg.150).aspx
If you're in a coexistence scenario, where you're running Exchange 2010 and Exchange 2013 in the same organization, and your mailbox is still housed on the Exchange 2010 Mailbox server, the browser will default to the Exchange 2010 ECP. You can access the EAC by adding the Exchange version to the URL. For example, to access the EAC whose virtual directory is hosted on the Client

Access server CAS15-NA, use the following URL: https://CAS15-NA/ecp?ExchClientVer=15. Conversely, if you want to access the Exchange 2010 ECP and your mailbox resides on an Exchange 2013 Mailbox server, use the following URL: https://CAS14-NA/ecp?ExchClientVer=14.

QUESTION 206

Your network contains an Active Directory forest named contoso.com. The forest contains the domain controllers configured as shown in the following table.

Domain controller name	Active Directory domain	Active Directory site	Operations master role
DC1	Contoso.com	East	Domain naming, PDC emulator, RID master
DC2	Contoso.com	West	Schema master, infrastructure master
DC3	Contoso.com	West	*Not applicable*
DC4	Operations.contoso.com	West	PDC emulator, RID master
DC5	Operations.contoso.com	West	Infrastructure master

You plan to deploy an Exchange Server 2013 organization to the forest. A company policy prevents administrators from logging on to DC2 to perform installations. You need to prepare the Active Directory schema for the planned Exchange Server deployment. You verify that your user account has all the required permissions to achieve the task. The solution must minimize changes to the Active Directory infrastructure.

A. Move the schema master role to DC1, and then run Exchange setup.
B. Deploy a member server to contoso.com, and then move the server to the West site. Run adprep.exe from the member server.
C. Log on to DC3 and then run Exchange setup.
D. Log on to any server in the West site, and then run Exchange setup.

Answer: A

Explanation:

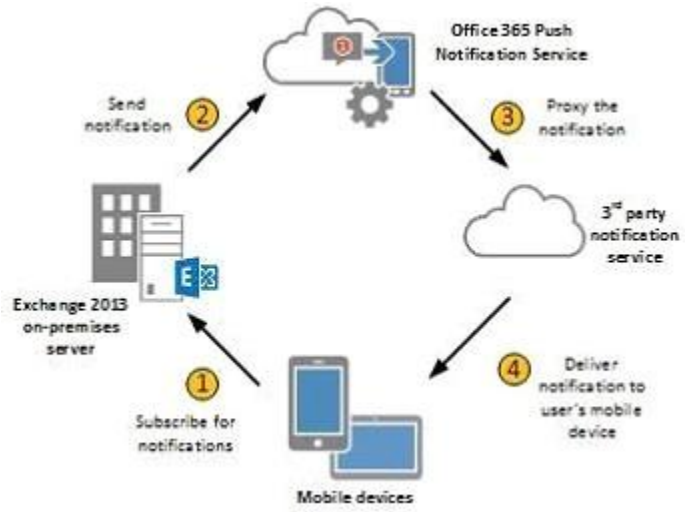
Prepare Active Directory and domains for Exchange 2013. The first step in getting your organization ready for Exchange 2013 is to extend the Active Directory schema. Exchange stores a lot of information in Active Directory but before it can do that, it needs to add and update classes, attributes, and other items. Before you extend your schema, there are a few things to keep in mind:
* The only way to extend the schema for Exchange is to use Setup.exe in Windows Command Prompt or use Exchange 2013 Setup. Other ways of extending the schema aren't supported.
* The computer where you'll run the command to extend the schema needs to be in the same Active Directory domain and site as the schema master.
We can accomplish this be by moving the schema master role to DC, and then run Exchange setup.
Incorrect answers:
Not B: Adprep is used to upgrade the Active Directory infrastructure forest to a newer version such as to Windows Server 2008. Adprep is not used for Exchange Server infrastructure changes.
Not C: Exchange Setup must be run from the Schema master. DC3 does not have the schema master role.
Not D: Only DC2 in the West site has the Schema master role. We cannot run Exchange Setup from the other servers in the West site.

https://technet.microsoft.com/en-us/library/bb125224%28v=exchg.150%29.aspx

QUESTION 207
You have an Exchange Server 2013 organization. A new policy requires that all iPhone users access their on-premises mailbox by using the OWA for iPhone app. You need to ensure that push notifications for the OWA for iPhone app are configured before the users install the app. Which three actions should you perform? Each correct answer presents part of the solution.

A. Configure Microsoft Azure Active Directory Sync (Azure AD Sync).
B. Modify the EWS virtual directory.
C. Enable push notifications proxy.
D. Enroll in Microsoft Office 365 for business.
E. Modify the OWA virtual directory.
F. Set up on premises Exchange 2013 to Office 365 Authentication.

Answer: CDF
Explanation:
Configuring push notifications proxying for OWA for Devices.
To enable push notifications, the admin must:
1. (D) Enroll your organization in Office 365 for business.
2. Update all on-premises servers to Exchange Server 2013 Cumulative Update 3 (CU3) or later.
3. (F) Set up On-premises Exchange 2013 to Office 365 Authentication.
4. (C) Enable push notifications from the on-premises Exchange Server 2013 to Office 365 and verify that push notifications are working.
Illustration below:



Incorrect answers:
Not A: There is no need to configure Microsoft Azure Active Directory Sync.
Not B: You do not have to modify the EWS virtual directory.
Not E: You do not have to modify the OWAvirtual directory.
https://technet.microsoft.com/en-us/library/dn511017%28v=exchg.150%29.aspx

QUESTION 208
You have an Exchange Server 2010 organization. You deploy several Exchange Server 2013 servers to the organization and you deploy the required certificates. You attempt to connect to an Exchange Server 2013 server by using Outlook Web App and you discover the error message shown in the exhibit. (Click the Exhibit button.)
Exhibit: * Missing*

You need to prevent the error message from appearing when users access Outlook Web App on the new servers. What should you do?

A. Remove the Exchange Server 2010 servers from the organization.
B. Run the Remove-ExchangeCertificate cmdlet.
C. From the Exchange Management Console, remove the certificates from the Exchange Server 2010 servers.
D. From the Exchange Admin Center, modify the properties of the OWA virtual directory.

Answer: B
Explanation:
We remove the Exchange Server 2010 servers certificates. The certificates are removed with the Remove- ExchangeCertificate cmdlet. Note that the Exchange 2010 SSL certificate can be re-used if it contains the correct namespaces. You can export the SSL certificate from Exchange 2010 and import it into Exchange 2013. However, if the names on the certificate are not correct, or the certificate is due to expire soon anyway, you may find it easier to simply acquire a new SSL certificate.
Incorrect answers:
Not A: We must remove the certificate for the Exchange Server 2010 servers. If you just remove the Exchange Server 2010 servers the certificates for them would still cause problems.
Not C: We cannot remove the certificates from the Exchange Management Console.
Not D: Modifying the OWA virtual directory would not address the certificate problem.
https://technet.microsoft.com/en-us/library/aa997569%28v=exchg.150%29.aspx

QUESTION 209
A company named Contoso, Ltd. has an Exchange Server 2013 organization that contains two servers. Contoso has a subsidiary named Fabrikam, Inc. All users have mailboxes in the Contoso organization. You implement an address book policy (ABP) for the users from Fabrikam. A company policy states that the users from Contoso must not be able to view the contact cards of the Fabrikam users. You need to implement a solution to meet the requirement of the company policy. Which two actions should you perform? Each correct answer presents part of the solution.

A. Run the New-TransportRule cmdlet.
B. Modify the properties of the ABP.
C. Run the Set-TransportConfig cmdlet.
D. Run the Set-Mailbox cmdlet.
E. Install and Enable the Address Book Policy Routing agent.
F. Modify the properties of the global address list (GAL).

Answer: EF
Explanation:
F: First we modify the properties of GAL of the ABP so that only Fabrikam users can access the ABP. An Address Book Policy consists of a subset of the various address objects. The resulting scope of an ABP is equal to that of the GAL contained in the policy, Note: Global address list (GAL) segmentation (also known as GAL segregation) is the process whereby administrators can segment users into specific populations to provide customized views of their organization's GAL. Address book policies (ABPs) allow you to segment users into specific groups to provide customized views of your organization's global address list (GAL). When creating an ABP, you assign a GAL, an offline address book (OAB), a room list, and one or more address lists to the policy. You can then assign the ABP to mailbox users, providing them with access to a customized GAL in Outlook and Outlook Web App. The goal is to provide a simpler mechanism to accomplish GAL segmentation for on- premises organizations that require multiple GALs.
E: If you're using ABPs, and you don't want users in separate virtual organizations to view each other's potentially private information, you can turn on the Address Book Policy Routing agent. The

ABP Routing agent is a Transport agent that controls how recipients are resolved in your organization. When the ABP Routing agent is installed and configured, users that are assigned to different GALs appear as external recipients in that they can't view external recipients' contact cards.
Incorrect answers:
Not A: The New-TransportRule cmdlet is used to create transport rules in your organization, but transport rules does not affect the ABP.
Not B: The properties of the ABP would not affect which users can view contact information or not. This is decided by the GAL of the ABP.
Not C: The Set-TransportConfig cmdlet is used to modify the transport configuration settings for the whole Exchange organization, but it would not affect the ABP.
Not D: We can use the Set-Mailbox cmdlet with the AddressBookPolicy parameter to assign the ABP to users, but here the ABP is already implemented for the users (and we assume it has already been assigned to the users).
https://technet.microsoft.com/en-us/library/hh529948%28v=exchg.150%29.aspx

QUESTION 210
Your company has a main office and three branch offices. You have an Exchange Server 2013 organization. The main office contains five Exchange servers. Each branch office contains two Exchange servers. All of the servers have all of the Exchange server roles installed. Each branch office contains one database availability group (DAG). You need to recommend a load balancing solution for the branch offices. The solution must ensure that both servers in each office are the targets of all client connections. What are two possible recommendations? Each correct answer presents a complete solution.

A. DNS round robin
B. Layer 4 hardware load balancers
C. CAS arrays
D. Network Load Balancing (NLB) clusters

Answer: AB
Explanation:
In current builds of Exchange 2013, no configuration of a Client Access array is required, because the deployment of a load balanced and highly available service is much simpler.
https://technet.microsoft.com/en-us/library/jj898588(v=exchg.150).aspx

QUESTION 211
You have an Exchange Server 2013 organization named contoso.com that contains 10 servers. Your company purchases a company named Fabrikam, Inc. Fabrikam has an Exchange Server organization named fabrikam.com. All of the email messages sent between the organizations is routed over the Internet. You need to ensure that the email messages sent from contoso.com to fabrikam.com are encrypted. What is best way to achieve the goal? More than one answer choice may achieve the goal. Select the BEST answer.

A. Create a Send connector of type Partner.
B. Instruct all of the users in contoso.com to use SMIME.
C. Modify the Authentication settings for the Send connectors in contoso.com.
D. Create a federation trust between the organizations.

Answer: A
Explanation:
Create a Send connector to send email to a partner, with Transport Layer Security (TLS) applied If you want to ensure secure, encrypted communication with a partner, you can create a Send connector that is configured to enforce Transport Layer Security (TLS) for messages sent to a

partner domain. TLS provides secure communication over the Internet.
See step 2 below:
1. In the EAC, navigate to Mail flow > Send connectors, and then click Add.
2. In the New send connector wizard, specify a name for the send connector and then select Partner for the Type. When you select Partner, the connector is configured to allow connections only to servers that authenticate with TLS certificates. Click Next.
3. Verify that MX record associated with recipient domain is selected, which specifies that the connector uses the domain name system (DNS) to route mail. Click Next.
4. Under Address space, click Add . In the Add domain window, make sure SMTP is listed as the Type. For Fully Qualified Domain Name (FQDN), enter the name of your partner domain. Click Save.
5. For Source server, click Add . In the Select a server window, select a Mailbox server that will be used to send mail to the Internet via the Client Access server and click Add. After you've selected the server, click Add. Click OK.
6. Click Finish.
Incorrect answers:
Not B: We should not depend on the users to set up encryption. We can enforce by configuring the send connection partner setting.
Not C: The authentication setting is not used to set up encrypted e-mail.
Not D: A federation trust is used to share resources in a forest, not to enforce encryption of email.
https://technet.microsoft.com/en-us/library/jj657514%28v=exchg.150%29.aspx

QUESTION 212
You have an Exchange Server 2013 organization that contains two Edge Transport servers. The Edge Transport servers are configured to perform recipient filtering. You deploy a new Edge Transport server named Edge3. You need to ensure that Edge3 performs recipient filtering. What should you do?

A. Create a new Edge Subscription for Edge3.
B. Run the Set-TransportConfig cmdlet on Edge3.
C. Export the Edge Subscription from an existing Edge Transport server and import the Edge Subscription to Edge3.
D. Run the ExportEdgeConfig.ps1 and the ImportEdgeConfig.ps1 scripts.

Answer: D
Explanation:
We copy the configuration from an existing Edge Transport server with the ExportEdgeConfig.ps1 script and apply to new server Edge3 with ImportEdgeConfig.ps1 script.
Note: Configure Edge Transport server using cloned configuration.
You can use the provided Exchange Management Shell scripts (located in % ExchangeInstallPath %Scripts) to duplicate the configuration of an Edge Transport server. This process is referred to as cloned configuration. Cloned configuration is the practice of deploying new Edge Transport servers based on 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. Two Shell scripts are used to perform cloned configuration tasks:
* ExportEdgeConfig.ps1 Exports all user-configured settings and data from an Edge Transport server and stores that data in an XML file.
* ImportEdgeConfig.ps1 During the validate configuration step, the ImportEdgeConfig.ps1 script checks the exported XML file to see whether the server-specific export settings are valid for the target server.
Incorrect answers:
Not A: We do not need to create a new Edge subscription.
Not B: The Set-TransportConfig cmdlet is used to modify the transport configuration settings for the whole Exchange organization, but we just to copy the configuration of an Edge Transport server.

Not C: There are no commands to export and import Edge subscriptions.
https://technet.microsoft.com/en-us/library/aa996008%28v=exchg.150%29.aspx

QUESTION 213
You have an Exchange Server 2013 on-premises organization and a Microsoft Office 365 tenant. All mailboxes are hosted on-premises. You need to implement an archiving solution for all users. The solution must ensure that all mailbox content older than 18 months is moved to Personal Archives in Office 365. What should you implement?

A. A default policy tag (DPT)
B. A retention policy
C. A personal tag
D. A retention policy tag (RPT)
E. A retention hold

Answer: B
Explanation:
To apply one or more retention tags to a mailbox, you must add them to a retention policy and then apply the policy to mailboxes. In our case we would need a default policy tag and then add it to a retention policy.
Incorrect answers:
Not B: We cannot apply a Default policy tag (DPT) to a mailbox. We would need to add it to a retention policy.
Note: DPT actions include:
* Move to archive
* Delete and allow recovery
* Permanently delete
Users can't change DPTs applied to a mailbox.
Not C: Personal tags allow your users to determine how long an item should be retained, but we need to implement a solution for all users.
Not D: The available actions for Retention policy tag (RPT) are:
* Delete and allow recovery
* Permanently delete.
RPT have no archive action.
Not E: A retention hold is used to halt retention policy, but we should not halt retention.
Reference: https://technet.microsoft.com/en-us/library/dd297955%28v=exchg.150%29.aspx

QUESTION 214
In Europe, your company has one main office and five branch offices. In Asia, the company has one main office and five branch offices. Each main office contains a data center. The network contains an Active Directory forest. The forest contains a single domain named contoso.com. Each office is configured as an Active Directory site. All client computers are joined to the domain. You plan to deploy Exchange Server 2013 servers to both data centers. You need to recommend a client connectivity solution that meets the following requirements:
- Users who connect from the Internet must be configured automatically to connect to their mailbox by using Outlook Anywhere.
- Users from the branch offices must use Outlook Anywhere to connect to the Client Access servers in their respective region.
What should you include in the recommendation?

A. A service connection point (SCP) in Active Directory and a host (A) record in the public DNS zone
B. A service location (SRV) record in the internal DNS zone and a service location (SRV) record in the public DNS zone
C. A service connection point (SCP) in Active Directory and an inbound port rule for TCP 389

D. A service location (SRV) record in the public DNS zone and an inbound port rule for TCP

Answer: B

Explanation:

You must provide a host service (SRV) resource record in DNS for Outlook clients to discover the Autodiscover service by using DNS. We should provide two SRV records, one for the internal DNS zone and one for the public DNS zone.

Incorrect answers:

Not A: Service Connection Points (SCPs) are objects in Active Directory that hold information about services, but SCP would not be useful for setting up Outlook Anywhere. Instead we need to configure the DNS.

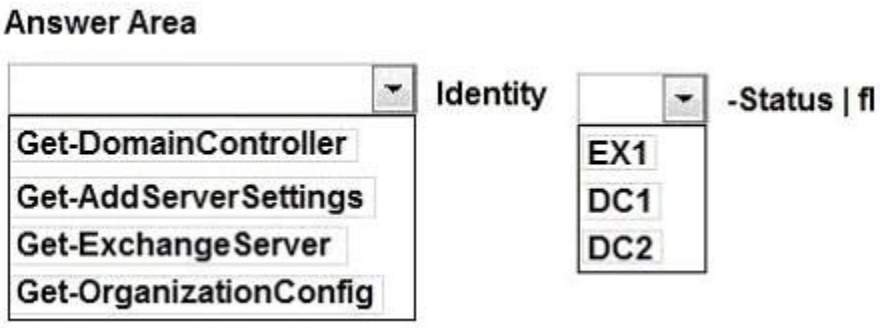
Not CD: TCP port 389 is the LDAP protocol, but Outlook Anywhere does not use this port so there is no need for a port rule for it. The Windows RPC over HTTP Proxy component, which Outlook Anywhere clients use to connect, wraps remote procedure calls (RPCs) with an HTTP layer. This allows traffic to traverse network firewalls without requiring RPC ports to be opened.

https://social.technet.microsoft.com/forums/exchange/en-US/957873ea-ea46-468e-843e-fae939ee1b82/srv-records-to-enable-auto-discover-for-outlook-anywhere

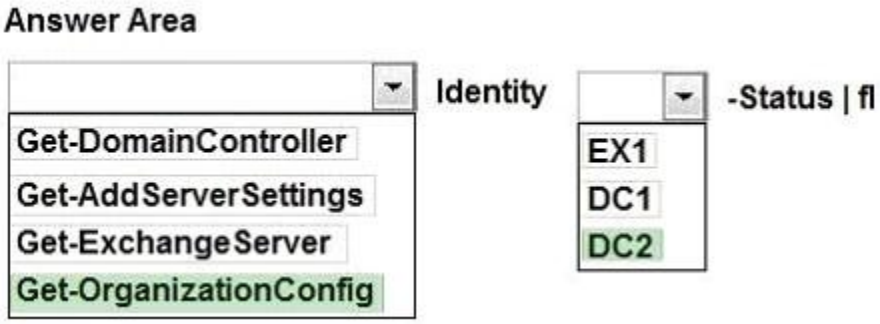
QUESTION 215

Drag and Drop Question

You have an Exchange Server 2013 organization that contains a server named EX1. The network contains two domain controllers named DC1 and DC2. You plan to make changes to the Active Directory infrastructure and to remove DC2 from the network. You need to verify whether EX1 writes Active Directory changes to DC2. What command should you run? To answer, select the appropriate options in the answer area.



Answer:



Explanation:

The Get-OrganizationConfig cmdlet is used to get configuration data for an Exchange organization. We should specify DC2 as we are interested if information from EX1 is propagated to DC2.

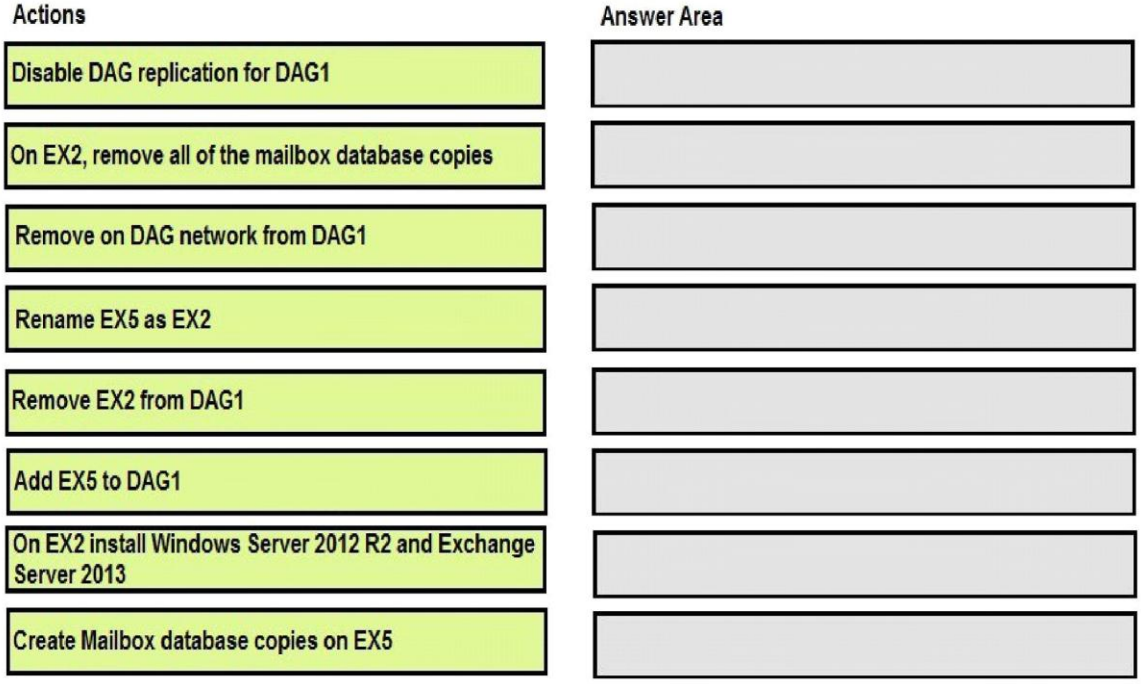
Example: This example gets the organization configuration information for the domain controller ContosoDC.

Get-OrganizationConfig -DomainController ContosoDC
Incorrect answers:
Not Get-ExchangeServer: The Get-ExchangeServer cmdlet is used to obtain the attributes of a specified Exchange server, but we are not interested in the attributes of EX1, we want to know if EX1 propagates changes to DC2.
Not Get-DomainController: The Get-DomainController cmdlet is used to view a list of domain controllers that exist in your organization, but we are interested in Active Directory information not a list of the Domain controllers.
Not Get-AddServerSettings: The Get-AdServerSettings cmdlet is used to view the Active Directory Domain Services (AD DS) environment settings in the current Windows PowerShell session, but we are not interested in PowerShell sessions.
https://technet.microsoft.com/en-us/library/aa997571%28v=exchg.150%29.aspx

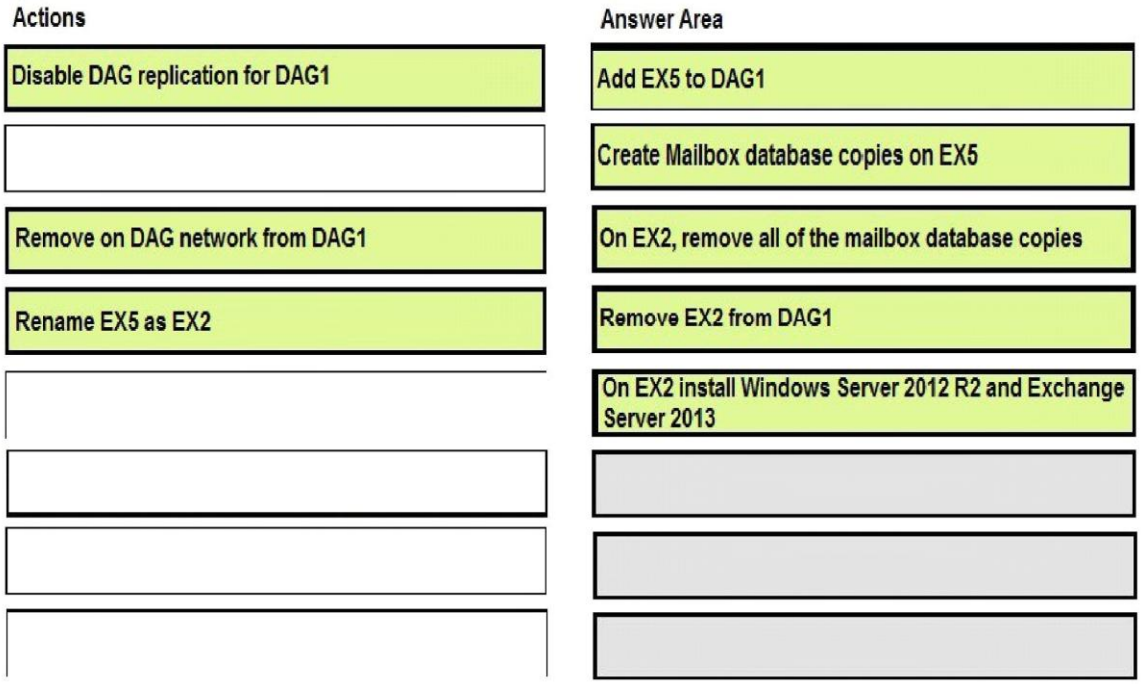
QUESTION 216
Drag and Drop Question
You have an Exchange Server 2013 organization that contains the servers configured as shown in the following table.

Server name	Database availability group (DAG) name	Windows Server version
EX1	DAG1	Windows Server 2008 R2 Enterprise
EX2	DAG1	Windows Server 2008 R2 Enterprise
EX3	DAG2	Windows Server 2012 R2 Datacenter
EX4	DAG2	Windows Server 2012 R2 Datacenter
EX5	None	Windows Server 2008 R2 Standard

You need to add EX2 to DAG2. The solution must maintain redundancy for all mailbox databases. Which five actions should you perform in sequence before you can add EX2 to DAG2? To answer, move the appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Answer:



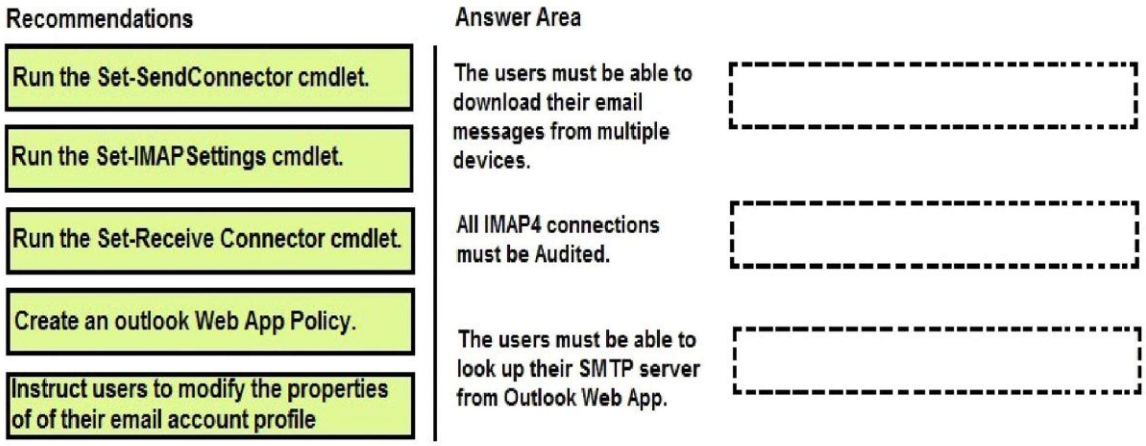
Explanation:

Box 1: Add EX5 to DAG1
We need to add EX5 to DAG1 for redundancy before we remove EX2.
Box 2: Create Mailbox database copies on EX5
We must set up EX5 mailbox database copies for redundancy before we remove EX2.
Box 3: On EX2, remove all of the mailbox database copies. We remove the DAG1 mailbox database copies from EX2. We must do this before removing EX2 from DAG1 as the Mailbox server must not host any replicated databases when it is removed.
Box 4: Remove EX2 from DAG1
Now can when EX5 being set up for DAG1 we can remove EX2 from DAG1.
Box 5: On EX2 install Windows Server 2012 R2 and Exchange Server 2013
As the other members of DAG2 run Windows Server 2012 R2 datacenter we upgrade EX2 to Windows Server 2012 R2 as well.
Incorrect answers:
* There is no need to disable DAG replication for DAG1.
* There is no need to remove the DAG network from DAG1.
* Nothing would be accomplished by renaming EX5 to EX2.
https://technet.microsoft.com/en-us/library/dd297956%28v=exchg.150%29.aspx

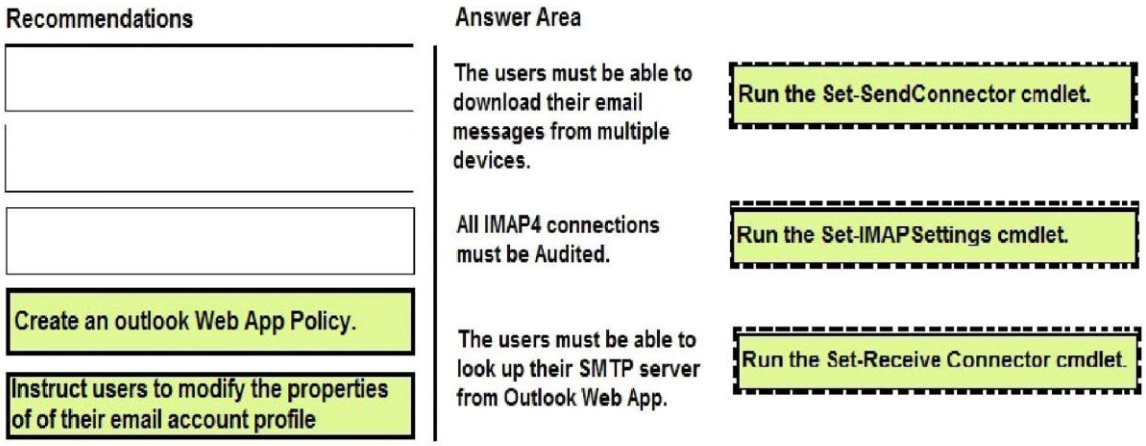
QUESTION 217

Drag and Drop Question
You have an Exchange Server 2013 organization. You need to recommend a solution to ensure that users can access their mailbox by using IMAP4. The solution must meet the following requirements:
- The users must be able to download their email messages from multiple devices.
- The users must be able to look up their SMTP server from Outlook Web App.
- All IMAP4 connections must be audited.
What should you recommend? To answer drag the appropriate recommendation to the correct

requirement. Each recommendation may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.



Answer:



Explanation:

Box 1: Run the Set-SendConnector cmdlet.

In Microsoft Exchange Server 2013, a Send connector controls the flow of outbound messages to the receiving server. They are configured on Mailbox servers running the Transport service. Most commonly, you configure a Send connector to send outbound email messages to a smart host or directly to their recipient, using DNS. By default, Microsoft Exchange Server 2013 doesn't allow you to send mail outside of your domain. To send mail outside your domain, you need to create a Send connector.

Box 2: You can set up logging with Set-IMAPSettings.

This example turns on IMAP4 protocol logging. It also changes the IMAP4 protocol logging directory to C:\Imap4Logging.

Set-ImapSettings -ProtocolLogEnabled $true -LogFileLocation "C:\Imap4Logging".

Note: The Set-ImapSettings cmdlet is used to set specific IMAP4 settings for the server running Microsoft Exchange Server 2013 that has the Client Access server role installed and that's running the Microsoft Exchange IMAP4 service.

Box 3: Run the Set-ReceiveConnector Settings cmdlet.

Exchange 2013 servers running the Transport service require Receive connectors to receive messages from the Internet, from email clients, and from other email servers. A Receive connector controls inbound connections to the Exchange organization.

Incorrect answers:
* A Web App Policy cannot be used to allow access their SMTP server from the Outlook Web app.
* We cannot rely on users to modify their email account profiles.
We need a centralized solution.
https://technet.microsoft.com/en-us/library/aa998252%28v=exchg.150%29.aspx

QUESTION 218
Drag and Drop Question
You have an Exchange Server 2013 organization that contains several servers in a single site. You run the Get-TransportConfig cmdlet and you receive the following output.

```
AddressBookPolicyRoutingEnabled          : False
AnonymousSenderToRecipientsRatePerHour   : 1800
ClearCategories                          : True
ConvertDisclaimerWrapperToEml            : False
DSNConversionMode                        : UseExchangeDSNs
ExternalDelayDsnEnabled                  : True
ExternalDsnDefaultLanguage               :
ExternalDsnLanguageDetectionEnabled      : True
ExternalDsnMaxMessageAttachSize          : 10 MB (10,485,760 bytes)
ExternalDsnReportingAuthority            :
ExternalDsnSendHtml                      : True
ExternalPostmasterAddress                :
GenerateCopyOfDSNFor                     : {}
HygieneSuite                             : Standard
InternalDelayDsnEnabled                  : True
InternalDsnDefaultLanguage               :
InternalDsnLanguageDetectionEnabled      : True
InternalDsnMaxMessageAttachSize          : 10 MB (10,485,760 bytes)
InternalDsnReportingAuthority            :
InternalDsnSendHtml                      : True
InternalSMTPServers                      : {}
JournalingReportNdrTo                    : <>
LegacyJournalingMigrationEnabled         : False
LegacyArchiveJournalingEnabled           : False
LegacyArchiveLiveJournalingEnabled       : False
SafetyNetHoldTime                        : 2.00:00:00
ShadowHeartbeatFrequency                 : 00:02:00
ShadowMessageAutoDiscardInterval         : 2.00:00:00
ShadowMessagePreferenceSetting           : PreferRemote
ShadowRedundancyEnabled                  : True
ShadowResubmitTimeSpan                   : 03:00:00
SupervisionTags                          : {Reject, Allow}
TLSReceiveDomainSecureList               : {}
TLSSendDomainSecureList                  : {}
VerifySecureSubmitEnabled                : False
VoicemailJournalingEnabled               : True
HeaderPromotionModeSetting               : NoCreate
Xexch50Enabled                           : True
```

Use the drop-down menus to select the answer choice that completes each statement.

Answer Area

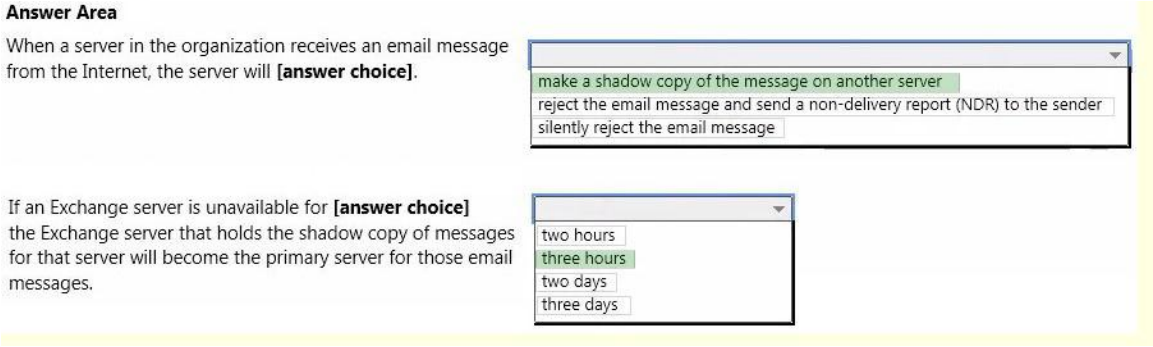
When a server in the organization receives an email message from the Internet, the server will **[answer choice]**.

- make a shadow copy of the message on another server
- reject the email message and send a non-delivery report (NDR) to the sender
- silently reject the email message

If an Exchange server is unavailable for **[answer choice]** the Exchange server that holds the shadow copy of messages for that server will become the primary server for those email messages.

- two hours
- three hours
- two days
- three days

Answer:



Explanation:

Box 1: make a shadow copy of the message on another server

From the exhibit we see that: ShadowRedundancyEnable: True With shadow redundancy in Microsoft Exchange Server 2013 the transport server makes a redundant copy of any messages it receives before it acknowledges successfully receiving the message back to the sending server.

Box 2: three hours

ShadowResubmitTimeSpan on Set-TransportConfig

3 hours

How long a server waits before deciding that a primary server has failed and assumes ownership of shadow messages in the shadow queue for the primary server that's unreachable.

https://technet.microsoft.com/en-us/library/dd351027%28v=exchg.150%29.aspx

https://technet.microsoft.com/en-us/library/dd351046%28v=exchg.141%29.aspx

https://technet.microsoft.com/en-us/library/dd351027(v=exchg.150).aspx

QUESTION 219

You have an Exchange Server 2013 organization. Users connect to their mailbox by using Microsoft Outlook 2013 and mobile devices. A user named User1 loses a mobile device. You need to wipe the mobile device remotely. Which cmdlet should you use?

A. Remove-MobileDevice
B. Clear-MobileDevice
C. Set-Mailbox
D. Remove-ActiveSyncDevice

Answer: B

Explanation:

The Clear-MobileDevice cmdlet deletes all user data from a mobile device the next time that the device receives data from the server running Microsoft Exchange Server 2013.

Incorrect answers:

Not A: The Remove-MobileDevice cmdlet is used to remove the mobile device partnership

information that you specify from a user's mobile device list stored in a mailbox on a computer running Microsoft Exchange Server 2013, but we don't just want to remove the partnership information. We want wipe the device.
Not C: The Set-Mailbox cmdlet is used to modify the settings of an existing mailbox, but we need to wipe the mobile device.
Not D: The Remove-ActiveSyncDevice cmdlet is used to remove the mobile device partnership information that you specify from a user's mobile device list stored in a mailbox on a computer running Microsoft Exchange Server 2013, , but we don't just want to remove the device partnership information. We want wipe the device.
https://technet.microsoft.com/en-us/library/jj218658%28v=exchg.150%29.aspx

QUESTION 220
You verify that one email message sent to one mailboxes on EX1 are delivered successfully. You also verify that all of mailbox databases on EX1 are mounted. Delete 20 GB of unnecessary data on EX1. You discover that the hard disk drive on EX1 has only 10 GB of free space. You delete 20 GB of unnecessary data on EX1. Users report that now they are receiving all of their email messages successfully to their mailbox. You need to ensure that EX1 will prevent the delivery of email messages to mailboxes only if less than 2 GB of hard disk space is available. What should you do?

A. Modify the Organization transport settings.
B. Disable the Safety Net feature.
C. Modify the EdgeTransportexe.config file.
D. Modify the mailbox database settings.

Answer: C
Explanation:
https://technet.microsoft.com/en-us/library/bb201658(v=exchg.160).aspx#File

QUESTION 221
.....