**Question 1**

Which two actions should you perform?

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).

Correct Answer: EF

Explanation/Reference:

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 that exist in the. The resulting scope of the 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 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).


**Question 2**

What are two possible recommendations?

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

Correct Answer: BC

Explanation/Reference:

B: Use of hardware load balancers is still supported for Exchange 2013.

C: In Exchange 2010, Microsoft introduced the concept of a Client Access array. After a Client Access array was configured for an Active Directory site, all Client Access servers in the site automatically became members of the array. 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.

Incorrect answers:

Not A: A: A DNS round robin could in theory be used entirely in place of a hardware load balancer – in fact it’s almost as effective as using Windows Network Load balancing. However, DNS Round robin is in fact no load balancer.

Not D: Windows Network Load Balancing (WNLB) can’t be used on Exchange servers where mailbox DAGs are also being used because WNLB is incompatible with Windows failover clustering. If you’re using an Exchange 2013 DAG and you want to use WNLB, you need to have the Client Access server role and the Mailbox server role running on separate servers.


**Question 3**

Which cmdlet should you use?

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
Correct Answer: B
Explanation/Reference:
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-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 device partnership information. We want wipe the device.

Question 4
What command should you run?

HOTSPOT

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.

Hot Area:

Correct Answer: A

Explanation/Reference:
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 A: 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 B: 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 C: 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.

Question 5
Your network contains an Active Directory forest named contoso.com.
Your network contains an Active Directory forest named contoso.com.
The forest contains the domain controllers configured as shown in the following table.

Correct Answer: A

Explanation/Reference:
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 supplied.
* 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 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.

Question 6
Which five actions should you perform in sequence before you can add EX2 to DAG2?

DRAG DROP

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

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.

Select and Place:

Correct Answer:

Explanation/Reference:

Note:

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 EX3
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 EX3 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.


Question 7
Which three actions should you perform?

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.

Correct Answer: CDF

Explanation/Reference:

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 OWA virtual directory.


Question 8
What should you recommend?

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:

1. The users must be able to download their email messages from multiple devices.
2. The users must be able to look up their SMTP server from Outlook Web App.
3. 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.

Select and Place:

Correct Answer:

Explanation/Reference:

Note:

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:\imap4\Logging.

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 requires 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.


Question 9
What should you do?
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.

Correct Answer: B
Explanation/Reference:
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 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.


Question 10
Which URL should you use?
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/ecp?ExchClientVer=15
D. https://EX01/ecp?ExchClientVer=15

Correct Answer: B
Explanation/Reference:

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 11
What should you recommend?
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.

<table>
<thead>
<tr>
<th>EX01</th>
<th>EX02</th>
<th>EX03</th>
<th>EX04</th>
</tr>
</thead>
<tbody>
<tr>
<td>2010</td>
<td>2013</td>
<td>2010</td>
<td>2013</td>
</tr>
</tbody>
</table>

EX01 and EX04 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?
A. Add a layer 4 hardware load balancer that balances RPC traffic
B. Add a layer 2 hardware load balancer that balances the traffic on port 443
C. Add a layer 7 hardware load balancer that balances RPC traffic
D. Duplicate all of the databases in DAG1 to both DAG1 members.

Correct Answer: B
Explanation/Reference:
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.

Question 12
What should you recommend?
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.

Correct Answer: A
Explanation/Reference:
There must be a writable copy of the global catalog at each site where an Exchange 2013 server is to be installed.

Question 13
Which groups should you add ExchangeAdmin?
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 ExchangeAdmin can deploy CU1 to the first server, The solution must minimize the number of permissions assigned to ExchangeAdmin.
To which groups should you add ExchangeAdmin?
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

Correct Answer: A
Explanation/Reference:
A: Both Schema Admins and Enterprise Admins membership is needed to update the schema and prepare AD
Prepare Active Directory and Domains
Before you install the release to manufacturing (RTM) version of Microsoft Exchange Server 2013 or later cumulative updates (CU1) on any servers in your organization, you must prepare Active Directory and domains.
The computers on which you plan to install Exchange 2013 must meet the system requirements.
Your domains and the domain controllers must meet the system requirements in "Network and directory servers" in Exchange 2013 System Requirements.
For multiple domain organizations running the following "Prepare*" commands, we recommend the following:
Run the commands from an Active Directory site that has an Active Directory server from every domain.
Run the first server role installation from an Active Directory site with a writeable global catalog server from every domain. Verify that replication of objects from the preceding actions is completed on the global catalog server in the Active Directory site before installing the first Exchange 2013 server to that site.
If you run the Exchange 2013 Setup wizard with an account that has the permissions required (Schema Admins, Domain Admins, and Enterprise Admins) to prepare Active Directory and the domain, the wizard automatically prepares Active Directory and the domain. For more information, see Install Exchange 2013 Using the Setup Wizard. However, you must first install the Active Directory management tools on the computer prior to preparing the schema or domains. To do this, see the Active Directory preparation section in Exchange 2013 Prerequisites.
You must specify the /IAcceptExchangeServerLicenseTerms parameter when you run Setup.exe to accept the Exchange 2013 license terms.

Question 14
What should you use?
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

Correct Answer: D
Explanation/Reference:
D. ADSI Edit would be the best choice to view permissions and group memberships assigned to an AD object.
NOT A: Although possible to view the permissions assigned on an AD object's ACL, group memberships cannot be viewed via ADSIEdit.
NOT B: Cannot view User/Group permissions in ADSI.
NOT C: Dsget can retrieve user/group members and memberships, but not the permissions assigned to the object.

Question 15
Which role groups should you identify?
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.
• Restore mailboxes from a recovery database.
• Create, mount, and dismount databases.
• View the status of the message queue.
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.)
Select and Place:
Correct Answer:

Explanation/Reference:
Understanding Management Role Groups: Exchange 2013 Help

Question 16
HOTSPOT
HOTSPOT
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.
Hot Area:

Correct Answer:

Explanation/Reference:
POP3 over SSL uses port 995 – not listed in the exhibit, therefore not load balanced
WLNB is not service only IP based affinity supported. Therefore the session will be cookie based (sticky) and the same real server will be referenced in each session reconnection.

Question 17
What command should you run?
HOTSPOT
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.)
Hot Area:

Correct Answer:

Explanation/Reference:

Question 18
Which cmdlet should you run?
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-MailboxJunkEmailConfiguration
B. Set-ContentFilterConfig
C. Set-MalwareFilterPolicy
D. Set-SenderFilterConfig

Correct Answer: B
Explanation/Reference:
Configure a Spam Quarantine Mailbox: Exchange 2013 Help

Question 19
What should you do next?
Your network contains an Active Directory forest. The forest contains a single domain named contoso.com. The network contains a legacy mail system that uses an 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.

Correct Answer: A
Explanation/Reference:
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.

Which functionality should you transfer to each server?

HOTSPOT

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

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.)

Hot Area:

Correct Answer:

Explanation/Reference:

Explanation:


In the console tree, navigate to Organization Configuration > Mailbox.

In the result pane, click the Offline Address Book tab, and then select the OAB for which you want to move the generation to a new server.

In the action pane, click Move.

On the Move Offline Address Book page, click Browse to open the Select Mailbox Server dialog box. Select the server to which you want to move the OAB generation process, and then click OK.

Click Move to move the OAB generation process to the new server.

View the status of the move operation. The wizard will move the generation of your OAB to the new server and copy the existing files for the OAB to the new server.

Click Back to make configuration changes.

On the Completion page, review the following, and then click Finish to close the wizard:

A status of Completed indicates that the task wasn’t completed. If the task fails, review the summary for an explanation, and then click Back to make any configuration changes.

Click Finish to close the wizard.


A distribution group expansion server This is the routing destination when a distribution group has a designated expansion server that’s responsible for expanding the membership list of the group. A distribution group expansion server is always a Hub Transport server or an Exchange 2013 Mailbox server.


FrontEnd Transport service – This service runs on all Client Access servers and acts as a stateless proxy for all inbound and outbound external SMTP traffic for the Exchange 2013 organization. The Front End Transport service doesn’t inspect message content, only communicates with the Transport service on a Mailbox server, and doesn’t queue any messages locally.

Question 21

What should you identify?

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

Correct Answer: A

Explanation/Reference:

Question 22

Which cmdlet should you run?

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-MailPublicFolder
B. Set-PublicFolder
C. Set-Mailbox
D. Add-PublicFolderCManPermission

Correct Answer: C

Explanation/Reference:

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 [email protected] -AcceptMessagesOnlyFrom “User1”

EXAMPLE 2

This example sets the primary SMTP address of the mail-enabled public folder [email protected] to [email protected]

Set-MailPublicFolder -Identity [email protected] -PrimarySmtpAddress [email protected]

References


Question 23
What command should you run before you deploy the first Exchange Server 2013 server?

HOTSPOT

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.)

Hot Area:

Correct Answer:

Explanation/Reference:

Explanation:

http://exchangeserverpro.com/how-to-install-exchange-server-2013/


Question 24

Which two tasks should you perform?

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/newprovisionetceservenex2 parameter.
D. Add Admin1 to the Delegated Setup management role group.

Correct Answer: CD

Explanation/Reference:


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, a user must be a member of the Server Management role group.

Question 25

What command should you run?

HOTSPOT

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.)

Hot Area:

Correct Answer:

Explanation/Reference:


The ExternalConnectionSettings parameter specifies the host name, port, and encryption type that Exchange uses when IMAP4 clients connect to their email from outside the corporate network.

Enter a value in the format: <HostName>::. The <Encryption Type> part of the multivalued value is optional. Valid values for <Encryption Type> are either TLS (Transport Layer Security) or SSL.

Question 26

What should you configure on a Client Access server?

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://mail.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.

Correct Answer: D

Explanation/Reference:


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 27
HOTSPOT
HOTSPOT
You have an Exchange Server 2013 organization that contains four servers. The servers are configured as shown in the following table.

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.

Hot Area:

Correct Answer:

Explanation/Reference:

The ShadowMessagePreferenceSetting parameter specifies the preferred location for making a shadow copy of a message. Valid values are:

- LocalOnly: A shadow copy of the message should only be made on a server in the local Active Directory site.
- RemoteOnly: A shadow copy of the message should only be made on a server in a different Active Directory site.
- PreferRemote: Try to make a shadow copy of the message in a different Active Directory site. If you specify this, try to make a shadow copy of the message on a server in the local Active Directory site.

The default value is PreferRemote.

The MaxRetriesForRemoteSiteShadow parameter specifies the maximum number of attempts to make a shadow copy of the message in a different Active Directory site. Valid input for this parameter is an integer between 0 and 255. The default value is 4. The total number of attempts to create a shadow copy of the message is controlled by the ShadowMessagePreferenceSetting parameter:

- If ShadowMessagePreferenceSetting is set to RemoteOnly, the total number of attempts to make a shadow copy of the message is the value of the MaxRetriesForRemoteSiteShadow parameter.
- If ShadowMessagePreferenceSetting is set to PreferRemote, the total number of attempts to make a shadow copy of the message is the value of the MaxRetriesForLocalSiteShadow and MaxRetriesForRemoteSiteShadow parameters added together.
- If ShadowMessagePreferenceSetting is set to LocalOnly, the value of MaxRetriesForRemoteSiteShadow is 0, and the MaxRetriesForRemoteSiteShadow parameter has no effect on the total number of attempts to create a shadow copy of the message.

If a shadow copy of the message isn’t created after the specified number of attempts, accepting or rejecting the message is controlled by the RejectMessageOnShadowFailure parameter.

Question 28
What should you run?
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.

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-AdSiteLink SiteLink1 -ExchangeCost 25
B. Set-AdSite Washington' -HubSiteEnabled $false
C. Set-AdSiteLink SiteUnkl -ExchangeCost 15
D. Set-AdSite New York' -HubSiteenabled $false

Correct Answer: C

Explanation/Reference:
Set-AdSiteLink: Exchange 2013 Help

Question 29
Which three actions should you perform in sequence?

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.)

Select and Place:
Correct Answer:

Explanation/Reference:
STEP 1: Dismount database on server hosting active copy.
STEP 2: Copy files to server that will be hosting passive copy
STEP 3: Run Add-DatabaseCopy cmdlet on server that will be hosting passive copy

**Question 30**
What command should you run?

HOTSPOT
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.)

**Correct Answer:**

Explanation/Reference:
Add-MailboxPermission: Exchange 2013 Help

**Question 31**
Which cmdlets should you use?

DRAG DROP
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 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.
Select and Place:

**Correct Answer:**

Explanation/Reference:
Add-ADPermission -Identity "User1" -User User2 -AccessRights ExtendedRight -ExtendedRights "Send As"
Set-Mailbox -Identity User5 -GrantSendOnBehalfTo User5

**Question 32**
Which cmdlet should you use?

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-TransportService
D. Set-TransportConfig

**Correct Answer:**

Explanation/Reference:

**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

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. The value of the DelayNotificationTimeout parameter should always be greater than the value of the TransientFailureRetryInterval parameter. You can use the following formula to calculate the value of the TransientFailureRetryInterval parameter:

The value of the TransientFailureRetryInterval parameter = Value of the DelayNotificationTimeout parameter / (PermissionsCount + 1)

**Question 33**
Which cmdlet should you use in a scheduled task?

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. Search-AdminAuditLog
B. Set-AdminAuditLogConfig
C. New-AdminAuditLogSearch

**Correct Answer:**

Explanation/Reference:
D. Write-AdminAuditLog

Correct Answer: C
Explanation/Reference:
New-AdminAuditLogSearch
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 [email protected],[email protected] -Name “Datacenter admin audit log”

Question 34
Which cmdlet should you run?
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

Correct Answer: D
Explanation/Reference:
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
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.

Question 35
What are two possible ways to achieve this goal?
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.comusersUser1.
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.)
B. From Exchange Admin Center, edit the Default Role Assignment Policy and select MyDistributionGroups
D. From Exchange Admin Center, edit the Default Role Assignment Policy and select MyDistributionGroupMembership.

Correct Answer: AC
Explanation/Reference:
Role Assignment Policies cannot be managed via the EAC.

Question 36
What should you do?
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.

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.

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

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.

Correct Answer: A
Explanation/Reference:
Question 37
What should you recommend?
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.
Correct Answer: C
Explanation/Reference:
NLB will not suffice in this scenario as it is not service aware. If IIS fails, or one of the IIS components fail, WLNB will not detect there is an issue with the CAS server.
“What we [Microsoft] recommend is a hardware load balancer for most deployments... there are several reasons...
Hardware load balancers provide you service awareness, so you can actually get down to the individual, not only the individual TCP port, TCP 443 as an example, but you can potentially get down to the individual application as part of that service, depending on the load balancer you deploy. So now you can know if the web service, or the EWS service I should say, is failed - but OWA is still functioning on the CAS array. And you could take that member out of service as the result of that one failure because maybe you have. Lync deployed and you rely heavily on the EWS service. “Why not Windows Network Load Balancing? Well - there’s several issues with it.
One - it only provides the ability to do IP-based affinity. So we don’t get the persistent capabilities that we need.
Two - it doesn’t provide service awareness... it’s “server-aware”. If the web service fails, Windows Network Load Balancing has no concept of that. It just continues to route requests to that and then the user has a broken experience.

Question 38
What should you do?
HOTSPOT
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.

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.)
Hot Area:

Correct Answer:

Explanation/Reference:
Configure Mail Flow and Client Access: Exchange 2013 Help
Autodiscover Service: Exchange 2013 Help

Question 39
What should you run?
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-CASLoadBalancer cmdlet
C. The Configure-EnterprisePartnerApplication.ps1 script
D. The Set-AutoDiscover.ps1 script
Correct Answer: C
Explanation/Reference:

Question 40
What command should you run?
HOTSPOT
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 should you run? (To answer, select the appropriate options in the answer area.)
Hot Area:

Correct Answer:
**Question 41**

What should you recommend?

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:

1. All deleted mailboxes must be recoverable for up to six months after they are deleted.
2. 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

**Correct Answer:** B

**Explanation/Reference:**

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.

**Question 42**

Which two cmdlets should you run?

You have an Exchange Server 2013 organization that contains four servers. All users access their email by using Microsoft Outlook 2010. An administrator deploys a shared mailbox named Project. You assign all of the users in the marketing department Full Access permissions to Project. You discover that Project automatically appears in Outlook to all of the marketing department users. You need to ensure that Project only appears in Outlook to the marketing department users who add the mailbox manually to their Outlook profile. Which two cmdlets should you run? (Each correct answer presents part of the solution. Choose two.)

A. Remove-MailboxPermission
B. Set-Mailbox
C. Remove-Mailbox
D. Add-MailboxPermission
E. New-Mailbox

**Correct Answer:** AB

**Explanation/Reference:**

Set-Mailbox: Exchange 2013 Help

Remove-MailboxPermission: Exchange 2013 Help

**Question 43**

What should you do first?

You have an Exchange Server 2013 organization. The organization contains a Mailbox server that hosts several databases, including a database named ExecsDB. ExecsDB contains the mailboxes of the company executives. The hard disk that contains ExecsDB fails. You replace the hard disk with a new disk, and then you mount the database. You create a recovery database in an alternate location, and then you restore the database files for ExecsDB to the alternate location. You need to ensure that all data is consistent before merging the mailbox data into the dial-tone database. What should you do first?

A. Run the isinteg.exe command and specify the -fk parameter.
B. Run the Move-ActiveMailboxDatabase cmdlet.
C. Run the Update-MailboxDatabaseCopy cmdlet.
D. Run the eseutil.exe command and specify the /R parameter.

**Correct Answer:** A

**Explanation/Reference:**

Perform a Dial Tone Recovery


**Question 44**

What command should you run?

HOTSPOT

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.)

**Hot Area:**

**Correct Answer:**

**Explanation/Reference:**
Question 45
What should you do on EX1?

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

Correct Answer: C

Explanation/Reference:
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 the Outlook 2013 to authenticate with Exchange, is set to Basic. Internet Information Services (IIS) authentication, which is used to allow Exchange servers to communicate, is set to NTLM and Basic.

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, is set to NTLM and Basic.

Question 46
What command should you run?

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 should you do?
A. Configure Site3 as a hub site.
B. Modify the expansion server setting of D_Sales.
C. Modify the SubmissionServerOverrideList list on MBX1.
D. Set the IISAuthenticationMethods value to Basic and NTLM.

Correct Answer: D

Explanation/Reference:

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 the Outlook 2013 to authenticate with Exchange, is set to Basic. Internet Information Services (IIS) authentication, which is used to allow Exchange servers to communicate, is set to NTLM and Basic.

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, is set to NTLM and Basic.

Question 47
What should you do?

Your company has four offices. Each office is configured as an Active Directory site.

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

A user named User1 is in a distribution group named D_Sales. The mailbox of User1 is in a database that is active on MBX4 and is configured to use MBX5 as an expansion server.

You need to ensure that email sent to D_Sales from the Internet is received by CAS1, and then routed from MBX1 to MBX4.

What should you do?
A. Configure Site1 as a hub site.
B. Modify the expansion server setting of D_Sales.
C. Modify the SubmissionServerOverrideList list on MBX1.
D. Configure Site3 as a hub site.

Correct Answer: D

Explanation/Reference:

As the messages are routed from sender, the transport server is responsible for routing to recipient. When the transport server is not specified, the message is routed based on the routing destination specified. If no routing destination is specified, the message is routed to the first transport server in the transport service.

When a hub site is used, all email traffic from the sites configured to use the hub site is affected.
The question states that email sent to D_Sales needs to be rerouted, not all traffic.
There is no mention of the need for hub sites, AD site costs, or other sites with internet facing CAS servers.
Exchange 2013 Mail Flow

**Question 48**
What should you identify?
Your company has two offices. Each office is configured as an Active Directory site.
You have an Exchange Server 2013 organization that contains four servers. The servers are configured as shown in the following table.

<table>
<thead>
<tr>
<th>MBX1 and MBX2 are members of a database availability group (DAG) named DAG1. A mailbox database named DB1 has a copy on each Mailbox server. DB1 is active on MBX2. You are creating a disaster recovery plan for the organization. You need to identify how email messages will be received for the mailboxes on DB1 if the Exchange Server transport services fail on MBX2 because of messages in the poison message queue. What should you identify?</th>
</tr>
</thead>
<tbody>
<tr>
<td>A. Email messages will be queued on MBX1, and then delivered directly to the mailboxes on MBX2.</td>
</tr>
<tr>
<td>B. The Exchange Server transport services will restart automatically, and then put all delivery queues in a Retry state.</td>
</tr>
<tr>
<td>C. The Exchange Server transport services will restart automatically, and then purge the poison messages.</td>
</tr>
<tr>
<td>D. Email messages will be queued on CAS1 or CAS2, and then delivered directly to the mailboxes on MBX2.</td>
</tr>
</tbody>
</table>

Correct Answer: B
Explanation/Reference:
Queues: Exchange 2013 Help
Message Retry, Resubmit, and Expiration Intervals: Exchange 2013 Help

**Question 49**
What should you run?
You have an Exchange Server 2013 organization.
You are troubleshooting an email delivery problem.
You need to disable temporarily the antimalware scanning on a server that has Exchange Server 2013 installed. The solution must ensure that the antimalware engine continues to download updates.
What should you run?
A. The Set-TransportConfig cmdlet
B. The New-MalwareFilterPolicy cmdlet
C. The Disable-Antimalwarescanning.ps1 script
D. The Set-MalwareServer cmdlet

Correct Answer: D
Explanation/Reference:
Disable or Bypass Anti-Malware Scanning
Important:
Bypassing malware filtering should only be done when troubleshooting a problem. You should restore malware filtering after you have finished troubleshooting.
To temporarily bypass malware filtering, run the following command:
Set-MalwareFilteringServer <ServerIdentity> -BypassFiltering $true
To restore malware filtering, run the following command:
Set-MalwareFilteringServer <ServerIdentity> -BypassFiltering $false

**Question 50**
What should you do?
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 two mailbox databases named DB1 and DB2. DB1 is active on EX1. DB2 is active on EX2.
A disk on EX2 fails. DB2 fails over to EX1.
Users who have mailboxes in DB2 report that Microsoft Outlook can no longer connect to the Exchange Server organization.
You discover that DB2 is dismounted on EX1.
When you attempt to mount DB2 on EX1, the operation fails.

You need to identify what prevents DB2 from mounting on EX1.
What should you do?
A. Run the Resume-MailboxDatabaseCopy cmdlet.
B. Run the Update-MailboxDatabaseCopy cmdlet.
C. Run the eseutil.exe command and specify the A parameter.
D. Run the eseutil.exe command and specify the/mft parameter.

Correct Answer: B
Explanation/Reference:

**Question 51**
Which servers should you identify for each name?
DRAG DROPP
You are migrating an existing Exchange Server 2007 organization to Exchange Server 2013. You expect the migration to last several weeks. The servers in the organization are configured as shown in the following table.

<table>
<thead>
<tr>
<th>Select and Place:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Users who have mailboxes on all of the servers will access Outlook Anywhere by using the mail.contoso.com name. You need to recommend which servers must be associated to the autodiscover.contoso.com and mail.contoso.com names. Which servers should you identify for each name?</td>
</tr>
<tr>
<td>To answer, drag the appropriate servers to the correct name in the answer area. Each server 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.</td>
</tr>
</tbody>
</table>

Correct Answer: C

Explanation/Reference:
Configure Mail Flow and Client Access: Exchange 2013 Help
Autodiscover Service: Exchange 2013 Help

Question 52
Which tool should you use?
You have an Exchange Server 2013 organization.
Each user has an In-Place Archive.
You discover that several items in a user’s In-Place Archive are corrupt.
You need to ensure that the user can access the corrupt items.
Which tool should you use?
A. The Repair-FilerIntegrity cmdlet
B. The Isinteg command
C. The New-MailboxRepairRequest cmdlet
D. The Eseutil command

Correct Answer: C

Explanation/Reference:
New-MailboxRepairRequest
New-MailboxRepairRequest -Mailbox ayla -CorruptionType
ProvisionedFolder,SearchFolder,AggregateCounts,Folderview -Archive
New-MailboxRepairRequest
This cmdlet is available only in on-premises Exchange Server 2013.
Use the New-MailboxRepairRequest cmdlet to detect and fix mailbox corruptions. You can run this command against a specific mailbox or against a database. While this task is running, mailbox access is disrupted only for the mailbox being repaired. If you’re running this command against a database, only the mailbox being repaired is disrupted. All other mailboxes on the database remain operational.
Examples
EXAMPLE 1
This example detects and repairs all folder views for the mailbox [email protected]
New-MailboxRepairRequest -Mailbox [email protected] -CorruptionType FolderView
EXAMPLE 2
This example only detects and reports on ProvisionedFolder and SearchFolder corruption issues to Ayla Kol’s mailbox. This command doesn’t repair the mailbox.
New-MailboxRepairRequest -Mailbox ayla -CorruptionType ProvisionedFolder,SearchFolder -DetectOnly
EXAMPLE 3
This example detects and repairs AggregateCounts for all mailboxes on mailbox database MBX-DB01
New-MailboxRepairRequest -Database MBX-DB01 -CorruptionType AggregateCounts
EXAMPLE 4
This example detects and repairs all corruption types for Ayla Kol’s mailbox and archive.
New-MailboxRepairRequest -Mailbox ayla -CorruptionType ProvisionedFolder,SearchFolder,AggregateCounts,Folderview -Archive
EXAMPLE 5
This example creates a variable that identifies Ann Beebe’s mailbox and then uses the variable to specify the values for the Database and StoreMailbox parameters to create a request to detect and repair all corruption types.
$mailbox = Get-MailboxStatistics annb
New-MailboxRepairRequest -Database $mailbox.Database -StoreMailbox $mailbox.MailboxGuid –CorruptionType ProvisionedFolder,SearchFolder,AggregateCounts,Folderview

Question 53
Which three actions should you perform in sequence?
DRAG DROP
You have an Exchange Server 2013 organization that contains a database availability group (DAG) named DAG1. The organization contains three servers. The servers are configured as shown in the following table.

<table>
<thead>
<tr>
<th>Server</th>
<th>Role</th>
<th>Database Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>EX1</td>
<td>Primary</td>
<td>DB1, DB2</td>
</tr>
<tr>
<td>EX2</td>
<td>Secondary</td>
<td></td>
</tr>
<tr>
<td>EX3</td>
<td>Witness</td>
<td></td>
</tr>
</tbody>
</table>

You plan to create a public folder named Invoices.
You need to design a solution that ensures that users can access the Invoices public folder if one of the DAG members fails. The solution must ensure that the users can send email messages to the Invoices public folder.
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.)

Select and place:

Correct Answer:

Explanation/Reference:

Question 54
How many of each should you identify?
HOTSPOT
A school has 200 students and 10 classes. Each class has 20 students. Each class has one teacher. The school has five administrative staff members.
You need to design an Exchange Server 2013 organization for the school. The design must meet the following requirements:
Students must be able to view only the email addresses of the other students in their class, the teacher of their class, and the entire administrative staff.
Teachers must be able to view only the email addresses of the students in their class, all of the other teachers, and the entire administrative staff.

The administrative staff must be able to see the email addresses of everyone. Everyone will use Microsoft Outlook 2013 to view a list of all the users. You need to identify the minimum number of address lists, global address lists, Offline Address Books (OABs), and address book policies required for the design. How many of each should you identify? (To answer, select the appropriate numbers in the answer area.)

**Hot Area:**

**Correct Answer:**

**Explanation/Reference:**

I mocked this question up in my lab and could not come to a conclusive result.

**Address Lists:** 12
- Class 1-10 (1 AL each) Each Class AL contains respective class teacher Teachers (1 AL)
- Admin Staff (1 AL)
- Global Address Lists: 21
- Class 1-10 (1 GAL each containing respective Class AL and Admin Staff AL)
- Teachers (1 GAL each containing respective Class AL, Teachers AL, and Admin Staff AL)
- Admin Staff (1 GAL (default GAL) containing everybody)

**OAB’s:** 21 one OAB for each GAL

**Address Book Policies:** – 21

Only one GAL can be assigned per ABP, so if there are 21 GAL’s surely there would need to be 21 ABP’s? However, in my lab I only needed 20 ABP’s because the Admin staff used the default GAL therefore no ABP needs to be assigned. If a new GAL were created for them however, the 21 ABP’s would be applicable....

**Question 55**
What should you do?
You create a mailbox named ConfRoom1 as shown in the exhibit. (Click the Exhibit button.)

**Correct Answer: D**

**Explanation/Reference:**

New-Mailbox

This example creates a user in Active Directory and a resource mailbox for a conference room. The resource mailbox is located in Mailbox Database 1. The password must be reset at the next logon. The Exchange Management Shell prompts for the value of the initial password because it’s not specified.

New-Mailbox -UserPrincipalName [email protected] -Alias confmbx -Name ConfRoomMailbox – Database “Mailbox Database 1” – OrganizationalUnit Users -Room -ResetPasswordOnNextLogon True

**Question 56**
Which role group should you add User1?
Your company has an Exchange Server 2013 organization. All Exchange servers have the Client Access server role and the Mailbox server role installed. All of the servers are members of a database availability group (DAG) named DAG1. You need to ensure that a user named User1 can move mailboxes between the servers. The solution must minimize the number of permission assigned to User1. To which role group should you add User1?

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

**Correct Answer: D**

**Explanation/Reference:**

Recipient Management: Exchange 2013 Help

**Question 57**
Which three cmdlets should you run?
You have an Exchange Server 2013 organization that contains a server named Server1. Server1 has the Client Access server role and the Mailbox server role installed. You monitor the performance of Server1, and you discover that the Exchange Server transport services consume a high amount of processor resources. You need to limit the amount of processor resources that the Exchange Server transport services consume.

Which three cmdlets should you run?

A. New-WorkloadManagementPolicy, New-ThrottlingPolicy, and Set-ThrottlingPolicyAssociation
B. New-WorkloadPolicy, New-ThrottlingPolicy and Set-ExchangeServer
C. New-WorkloadPolicy, New-ThrottlingPolicy and Set-ThrottlingPolicyAssociation

**Correct Answer: D**

**Explanation/Reference:**

New-WorkloadPolicy

New-WorkloadPolicy -Name DublinImapWorkloadPolicy -WorkloadType classification CustomerExpectation
-WorkloadManagementPolicy DublinWorkloadManagementPolicy -WorkloadType Imap – DomainController Dublin02.Contoso.com

New-WorkloadManagementPolicy

New-WorkloadManagementPolicy Dublin02.contoso.com

Question 58
HOTSPOT
HOTSPOT
Your company has three main offices. Each office is configured as an Active Directory site as shown in the exhibit (Click the Exhibit button.)

You have an Exchange Server 2013 organization. Each office contains Exchange servers. All users access their mailbox by using Outlook Web App. All of the users have a mailbox on a server in their respective office.
Use the drop-down menus to select the answer choice that completes each statement.

Hot Area:

Correct Answer:

Explanation/Reference:

Question 59
Which command should you recommend running?
HOTSPOT
Your network contains two Active Directory sites named MainSite and DRSite.
You have an Exchange Server 2013 organization that contains two servers. The servers are configured as shown in the following table.

The active copy of DB1 is located on EX1. There are typically 100 MB of log files queued on EX1. You need to recommend a procedure to allow administrators to mount the mailbox database copies on EX2 if EX1 fails. The recovery point objective (RPO) for mailbox data is 200 MB.
Which command should you recommend running? (To answer, select the appropriate options in the answer area.)

Hot Area:

Correct Answer:

Explanation/Reference:

The MountDialOverride parameter is used to override the auto database mount dial (AutoDatabaseMountDial) setting for the target server and specify an alternate setting. The following are possible values:
None
When using this value, the currently configured auto database mount dial setting on the target server will be used.
Lossless
This is the default value. When using this value, the database doesn’t automatically mount until all log files that were generated on the original active copy have been copied to the passive copy.
GoodAvailability
If you specify this value, the database automatically mounts immediately after a failover if the copy queue length is less than or equal to 6. If the copy queue length is greater than 6, the database doesn’t automatically mount. When the copy queue length is less than or equal to 6, Microsoft Exchange attempts to replicate the remaining logs to the passive copy and then mounts the database.
BestEffort
If you specify this value, the database automatically mounts regardless of the size of the copy queue length. Because the database will mount with any amount of log loss, using this value could result in a large amount of data loss.
BestAvailability
If you specify this value, the database automatically mounts immediately after a failover if the copy queue length is less than or equal to 12. The copy queue length is the number of logs recognized by the passive copy that needs to be replicated. If the copy queue length is more than 12, the database doesn’t automatically mount. When the copy queue length is less than or equal to 12, Exchange attempts to replicate the remaining logs to the passive copy and then mounts the database.

Question 60
Which sequence should you run the commands?
DRAG DROP
You have an Exchange Server 2013 organization.
You create a script named New-CustomMailbox.ps1 to create mailboxes based on your company’s requirements.
You create a role group named Mailbox Provisioning.
You need to ensure that the members of Mailbox Provisioning can create new mailboxes only by using New-CustomMailbox.ps1.
In which sequence should you run the commands? (To answer, move all of the commands from the list of commands to the answer area and arrange them in the correct order.)

Select and Place:

Correct Answer:

Explanation/Reference:

The Organization Management role group doesn’t, by default, have permissions to create or manage unscoped role groups. This is to prevent unscoped role groups from mistakenly being created or modified. The Organization Management role group can delegate the Unscoped Role Management role management role to itself and other role assignees. For more information about how to create an unscoped top-level management role.

STEP 1: Grant Organization Management group access to unscoped roles.
STEP 2: Create the Management Role
New-ManagementRole “Helpdesk Provisioning Script” -UnScopedTopLevel
STEP 3: Add management role entry to empty unscoped role.
Add-ManagementRoleEntry “Helpdesk Provisioning ScriptNew-CustomMailbox.ps1” -Parameters Name -UnScopedTopLevel
STEP 4: Assign management role to user group
New-ManagementRoleAssignment -Role "Helpdesk Provisioning Script" -SecurityGroup "Helpdesk Provisioning"

Question 61
What should you assign to the users of each company?
You have an Exchange Server 2013 organization that contains mailboxes for multiple companies.
You need to segment the address lists in the organization per company.
What should you assign to the users of each company?
A. Address book policies (ABPs)
B. Address lists
C. Global Address Lists (GALs)
D. Email address policies

Correct Answer: A

Explanation/Reference:
Technically, answers A and C are correct as users are “assigned” ABPs and GALs during the process of GAL segmentation.
I have chosen A as the answer however, as the overall process falls under the heading of “Address Book Policies”

Address Book Policies
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.

Question 62
Which command should you run?
HOTSPOT
Your network contains an Active Directory forest. The forest contains a single domain named contoso.com.
You have an Exchange Server 2013 organization that contains one Client Access server named CAS1 and one Mailbox server named MBX1.
You plan to enable Outlook Anywhere for remote access from non-domain joined client computers.
You deploy a trusted third-party certificate that has a subject name of mail.contoso.com.
Users report that they fail to access their email by using Microsoft Outlook 2013 when they work remotely from a non-domain joined client computer. From the internal network, the users can access their email by using Outlook 2013.
You verify that Autodiscover is configured remotely.
You need to ensure that the remote users can access their email by using Outlook Anywhere.
Which command should you run? (To answer, select the appropriate options in the dialog box in the answer area.)
Hot Area:

Correct Answer:

Explanation/Reference:
Set-OutlookAnywhere: Exchange 2013 Help

Question 63
What should you do?
Your network contains an Active Directory forest named contoso.com. The forest contains one domain.
You have an Exchange Server organization that contains three servers. The servers are configured as shown in the following table.

Remote users who have a mailbox hosted on EX1 report that they receive the following error message when they attempt to configure a Microsoft Outlook profile.

Remote users who have a mailbox hosted on EX3 can configure an Outlook profile successfully.
You need to ensure that the remote users who have a mailbox on EX1 can access their mailbox by using Outlook Anywhere.
What should you do?
A. On EX2, run Set-OutlookAnywhere
B. On EX2, run Set-CasMailbox
C. On EX1, run Enable-OutlookAnywhere
D. On EX1, run Set-OutlookAnywhere

Correct Answer: C

Explanation/Reference:
Enable-OutlookAnywhere: Exchange 2010 Help

Question 64
Which should you do?
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 -FrontendProxyEnabled:True parameter.
D. Run the Set-TransportConfig cmdlet and specify the -InternatSMTPServers:$null parameter.

Correct Answer: C
Question 65
Which setting should you change?
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

Correct Answer: A
Explanation/Reference:
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.

Question 66
What should you do first?
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 -PublicFolderDatabase parameter.

Correct Answer: C
Explanation/Reference:
Set Up Public Folders in a New Organization
New-Mailbox -PublicFolder -Name MasterHierarchy

Question 67
HOTSPOT
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 menu to select the answer choice that completes each statement.
Hot Area:

Correct Answer: 

Explanation/Reference:
Edge Transport Servers: Exchange 2013 Help

Question 68
What should you configure?
DRAG DROP
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.)

Select and Place:
Correct Answer:

Explanation/Reference:

**Question 69**

Which log folder should you review?

HOTSPOT

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.)

**Correct Answer:**

**Explanation/Reference:**
Set-TransportService: Exchange 2013 Help

**Question 70**

What should you recommend changing?

You are evaluating the implementation of a Database Availability Group (DAG).
You need to recommend changes to the planned implementation to minimize the loss of large email messages if a single DAG member fails.

What should you recommend changing?

A. The preference of the mail exchanger (MX) records
B. The duration of single item recovery
C. The intervals of shadow redundancy
D. The size of the transport dumpster

**Correct Answer:** C

**Explanation/Reference:**
Explanation:
Shadow redundancy intervals will need to be amended
SafetyNet is a component of Shadow Redundancy.
Example 1:
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.
Example 2:
SafetyNetHoldTime on Set-TransportConfig
2 days
How long successfully processed messages are retained in Safety Net. Unacknowledged shadow messages eventually expire from Safety Net after the sum of SafetyNetHoldTime and MessageExpirationTimeout on Set-TransportService.

**Question 71**

Which tool should you use?

A user fails to connect to his mailbox by using Outlook Anywhere. The user successfully connects to the mailbox by using an Exchange ActiveSync-enabled mobile device and Outlook Web App.

You need to identify what prevents the users from connecting to the mailbox by using Outlook Anywhere.

Which tool should you use?

A. Microsoft Outlook Connectivity Test
B. Microsoft Exchange RPC Extractor
C. Microsoft Exchange Server Profile Analyzer
D. Exchange Server MAPI Editor

**Correct Answer:** A

**Explanation/Reference:**
Explanation:
Outlook Web App
You can use Outlook Web App to access your Office 365 or other Microsoft Exchange-based email account via a web browser.
The URL (web address) you’ll use to sign in to Outlook Web App depends on the type of account you have.
Outlook Web App can be used to access any email account that’s hosted on a server that’s running Microsoft Exchange Server 2013.

Mobile devices that are enabled for Microsoft Exchange ActiveSync let users access most of their Microsoft Exchange mailbox data any time, anywhere.
There are many different mobile phones and devices enabled for Exchange ActiveSync. These include Windows Phones, Nokia mobile phones, Android phones and tablets, and the Apple iPhone, iPod, and iPad.
Although both phone and non-phone mobile devices support Exchange ActiveSync, in most Exchange ActiveSync documentation, we use the term mobile device.
Unless the feature or features we’re discussing require a cellular telephone signal, such as SMS message notification, the term mobile device applies to both mobile phones and other mobile devices such as tablets.
EXCHANGE SERVER SETTINGS:

- Outlook Anywhere (RPC over HTTP) allows you to use Outlook to connect to your Exchange server from remote locations without first connecting to the VPN. You can also/alternatively, use Outlook Web Access by logging in at https://mail.bu.edu or www.bu.edu/webmail.

- For remote connections, Outlook offers Outlook Anywhere, an alternative to VPN connections that allows you to use Outlook just as you normally do at your organization, without the need for any special connections or hardware, such as smart cards and security tokens. Outlook can connect to Exchange through the Internet by using remote procedure call (RPC) over HTTP.

- The Outlook Anywhere feature allows you to test your Exchange account remotely from the Internet when you are working outside your organization’s firewall. Text Outlook Anywhere Connectivity


  Applies to: Exchange Server 2013

  You can test for end-to-end client Outlook Anywhere connectivity by using either the Shell or the Exchange Remote Connectivity Analyzer (ExRCA). This includes testing for connectivity through the Autodiscover service, creating a user profile, and signing in to the user’s mailbox. All the required values are retrieved from the Autodiscover service.

Exchange Remote Connectivity Analyzer (ExRCA)
The Exchange Remote Connectivity Analyzer (ExRCA) is a web-based tool designed to test connectivity with a variety of Exchange protocols. You can access the ExRCA

https://www.testexchangeconnectivity.com/

The Microsoft Exchange Remote Connectivity Analyzer (ExRCA) can help you confirm that connectivity for your Exchange servers is configured correctly and diagnose any connectivity issues. The Remote Connectivity Analyzer website offers tests for Microsoft Exchange ActiveSync, Exchange Web Services, Microsoft Outlook, and Internet email.

- Use the Shell to test Outlook Anywhere connectivity

  To use the Shell to test Outlook Anywhere connectivity, use the Test-OutlookConnectivity cmdlet. Run the following command:

  Test-OutlookConnectivity -ProbeIdentity ‘OutlookMailboxDeepTestProbe’ -MailboxId [email protected] -Hostname contoso.com

  NOT B

  The Microsoft Exchange RPC Extractor is a command-line tool that can parse network captures and interpret remote procedure calls made from a client to Microsoft Exchange Server.

  RFX uses the information provided in the Microsoft Exchange Server protocol documentation to parse RPCs, remote operations (ROPs), and the parameters for each ROP.

  NOT C

  The Microsoft Exchange Server Profile Analyzer tool lets administrators collect estimated statistical information from a single mailbox store or across an Exchange Server organization.

  You can use the collected data to perform the following operations:

    - Analyze the performance and health of a mailbox server.
    - Improve capacity planning models.
    - Improve testing methodologies and tools.
    - Improve future client and server products.

  NOT D

  Use the Microsoft Exchange MAPI Editor to view and modify the contents of a Messaging API (MAPI) store directly.


Question 72

You need to create an exclusion for two helpdesk RBAC (Role Based Access Control) groups to not have access to managers.

You need to create an exclusion for two helpdesk RBAC (Role Based Access Control) groups to not have access to managers.

You will need to pick 3 powershell commands from the available choices:

A. New-ManagementRole, New-ManagementScope, Set-ManagementScope (Guessed)
B. New-ManagementScope, RecipientRestrictionFilter, New-ManagementRoleAssignment (Guessed)
C. New-ManagementScope, New-ManagementRoleAssignment, CustomRecipientWriteScope (Guessed)
D. Unsure of commands and correct answer

Correct Answer: C

Explanation/Reference:

- Only chose C as Microsoft recommends that you:
  - Define the scope,
  - Then the role,
  - Then the role group, and finally, the role assignment.

However it appears that the custom scope with a recipient filter has to be created in order to filter the scope for the 2 helpdesk role based access groups.

The scope, role, and role group assignments are linked by the role assignment itself.

Microsoft recommends that you first define the scope, then the role, then the role group, and finally, the role assignment.

Management role scopes

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). For more information about management roles, see Understanding Role Based Access Control.

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.
- Implicit: Implicit 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 allows 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.

The following sections describe each type of scope:

- Implicit Scopes
- Explicit Scopes
- Predefined Relative Scopes
- Custom Scopes
- Recipient Filter Scopes
- Configuration Scopes

Each role can have the following types of scopes:

Recipient read scope The implicit recipient read scope determines what recipient objects the user assigned the management role is allowed to read from Active Directory.

Recipient write scope The implicit recipient write scope determines what recipient objects the user assigned the management role is allowed to modify in Active Directory.

Configuration read scope The implicit configuration read scope determines what configuration objects the user assigned the management role is allowed to read from Active Directory.

Configuration write scope The implicit configuration write scope determines what organizational, database, and server objects the user assigned the management role is allowed to modify in Active Directory.

Role Based Access Control Groups

Role Based Access Control (RBAC) is the permissions model used in Microsoft Exchange Server 2013. With RBAC, you don’t need to modify and manage access control lists (ACLs), which was done in Exchange Server 2007.

ACLs created several challenges in Exchange 2007, such as making ACLs without causing unintended consequences, maintaining ACL modifications through upgrades, and troubleshooting problems that occurred due to using ACLs in a non-standard way.

RBAC enables you to control, at both broad and granular levels, what administrators and end-users can do. RBAC also enables you to more closely align the roles you assign users and administrators to the actual roles they hold within your organization. In Exchange 2007, the server permissions model applied only to the administrators who managed the Exchange 2007 infrastructure. In Exchange 2013, RBAC now controls both the administrative tasks that can be performed and the extent to which users can now administer their own mailbox and distribution groups.

RBAC has two primary ways of assigning permissions to users in your organization, depending on whether the user is an administrator or a specialist user, or an end-user: management role groups and management role assignment policies.

Each method associates users with the permissions they need to perform their jobs. A third, more advanced method, direct user role assignment, can also be used.

Built-in Role Groups

Microsoft Exchange Server 2013 includes several management role groups by default. The following built-in role groups provide you with a preconfigured set of roles that you can assign to various administrator and specialist users in your organization.

Organization Management
- View-Only Organization Management
- Recipient Management
- HelpDesk
- Compliance Management
- Records Management
- Discovery Management
- Public Folder Management
- Server Management
- Delegated Setup

RBAC has two primary ways of assigning permissions to users in your organization, depending on whether the user is an administrator or a specialist user, or an end-user: management role groups and management role assignment policies.

Each method associates users with the permissions they need to perform their jobs. A third, more advanced method, direct user role assignment, can also be used.

Built-in Role Groups
Microsoft Exchange Server 2013 includes several management role groups by default. The following built-in role groups provide you with a preconfigured set of roles that you can assign to various administrator and specialist users in your organization.

Organization Management
- View-Only Organization Management
- Recipient Management
- UM Management
- HelpDesk
- Hygiene Management
- Compliance Management
- Records Management
- Discovery Management
- Public Folder Management
- Server Management
- Delegated Setup

How to use -Exclude switch in Remove-Item cmdlet in PowerShell

Today I was trying to remove some junk folders and files in a specific folder. But I don’t want to remove all of file and folder. I want to keep few folders. Then I think that I should use the -Exclude switch with Remove-Item cmdlet.

I tried to use -Exclude switch but somehow I failed to get it working because I didn’t know the exact pattern used by -Exclude switch. After few minutes of testing I get it done and I thought I should share this tip with you.

In $Lenovo variable I specified the folder path in which I want to remove the items.

I want to Exclude folder name “System”, “temp” and file name “updates.ser” and all .XML Files in -Exclude switch give the folder name which you don’t want to delete, no need to put the in a double quotes “” in folder name. You can provide multiple folder name separated by comma.

in pattern matching make sure you put the wild cards in double quotes “”.

Powershell commands

New-ManagementScope (Example)

Example 1

This example creates the Protected Exec Users exclusive scope. Users that contain the string “VP” in their title match the recipient filter for the scope. When the exclusive scope is created, all users are immediately blocked from modifying the recipients that match the exclusive scope until the scope is associated with a management role assignment. Additional role assignments are associated with other exclusive scopes that match the same recipients, those assignments can still modify the recipients.

New-ManagementScope -Name “Protected Exec Users” -RecipientRestrictionFilter { Title -Like “*VP*” } -Exclusive

New-ManagementRoleAssignment

This example assigns the Eng Help Desk role to the Eng HD Personnel role group. The assignment restricts the recipient write scope of the role to the Engineering OU.

New-ManagementRoleAssignment -Role “Eng Help Desk” -SecurityGroup “Eng HD Personnel” -RecipientOrganizationalUnit -Name “Engineering/OU”

New-ManagementRole

Use the New-ManagementRole cmdlet to create a management role based on an existing role or create an unscoped management role.

Example 1

This example creates the management role Redmond Journaling View-Only based on the Journaling parent role.

New-ManagementRole -Name “Redmond Journaling View-Only” -Parent Journaling

New-ManagementRoleGroup

Use the New-ManagementRoleGroup cmdlet to create a management role group on a server running Microsoft Exchange Server 2013.

Example 1

This example creates a role group. The Mail Recipients and Mail Enabled Public Folders roles are assigned to the role group, and the users Kim and Martin are added as members.

New-ManagementRoleGroup -Name “Limited Recipient Management” -Roles “Mail Recipients”, “Mail Enabled Public Folders” -Members Kim, Martin

Look here:
Understanding Management Role Scopes

As we need to set deny access we want to set explicit recipient filter scope for the existing helpdesk group, removing the managers from the scope.

Then create a new RBAC group and implicit scope the managers mailboxes. So my guess would be something like
New-ManagementRole -Name "Management role for CEO"
New-ManagementScope -Name "Management Scope for CEO" -RecipientRestrictionFilter { Title -Like "*CEO*" } -Exclusive
Set-ManagementScope "Helpdesk Users" -RecipientRestrictionFilter { Company -eq 'Contoso users' -and Function -like 'CEO'
As we do not know what RBAC setup already exists, this kind of smells like Microsoft, but hey this is a start.

Question 73
Which three actions should you recommend performing in sequence?

DRAG DROP
You need to recommend a solution to deploy the Outlook app
Which three actions should you recommend performing in sequence? (To answer, move the appropriate three actions from the list of actions to the answer area and arrange them in the order)
(Apps for Outlook can help you personalize your messages or speed up the way you access information on the web. For example, the Bing Maps app that comes with Outlook shows an online map whenever you open a message that contains a street address. http://office.microsoft.com/en-us/store/apps-for-outlook-FX102804983.aspx
Select and Place:

Correct Answer:

Explanation/Reference:

STEPS:
1. RUN THE $DATA=GET-CONTENT -PATH "C:APPSSOCIALMEDIAPP.XML" -ENCODING BYTE – READCOUNT 0 COMMAND Establishes the Data variable which defines the location of the Outlook App.
2. RUN THE NEW-APP -FILEDATA $DATA COMMAND
This statement and the above statement install socialmediapp.xml
3. RUN THE SET-APP CMDLET
Enables the app
Set-App
Use the Set-App cmdlet to set configuration properties on an app object.
Enables the app
EXAMPLE 1
This example changes the organization app FinanceTestApp, which was installed to everyone in the organization, to be provided to specific users on the finance team and to be enabled by default.
Set-App -OrganizationApp -Identity 7a774f0c-7a6f-11e0-85ad-07fb4824019b -ProvidedTo SpecificUsers -UserList $a -DefaultStateForUser Enabled
If the app is enabled for the entire organization, users can activate the new app when viewing mail or calendar items within Microsoft Outlook or Microsoft Office Outlook Web App. If an installed app isn’t enabled, users can enable the app from Outlook Web App Options. Similarly, if an app is installed, an administrator can enable the app from the Exchange Administration Center or by using the Enable-App or Set-App cmdlet.

NOT Get-App
Use the Get-App cmdlet to return information about the installed app.
EXAMPLE 1
This example returns the list of apps installed for user Tony. The Exchange Management Shell returns the name of the app, whether the app is enabled, and the app version number.
Get-App -Mailbox Tony
NOT Install the Outlook App
Not appropriate for this scenario
$Data=Get-Content -Path "C:AppsSocialMediaApp.xml" -Encoding Byte -ReadCount 0 command
$Data variable defines the path where the outlook app exists
New-App -FileData $Data command
Use the New-App cmdlet to install apps for Outlook.
EXAMPLE 1
This example installs the Finance Test app manifest file that has been copied to the local hard disk.
$Data=Get-Content -Path "C:AppsFinanceTestApp.xml" -Encoding Byte -ReadCount 0
New-App -FileData $Data
New-App: Exchange 2013 Help
Set-App: Exchange 2013 Help

Question 74
How would you disable the anti malware filtering and ensure that engine updates from microsoft are downloaded and updated.
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-mailwarefilteringserver
C. Disable-Antimalwarescanning.ps1 (probable option)
D. Update-MalwareFilteringServer.ps1 (guessed option)

Correct Answer: C
Explanation/Reference:
To disable malware filtering, run the following command & Save: ExchangeInstallPathScriptsDisable-Antimalwarescanning.ps1
This example installs the Finance Test app manifest file that has been copied to the local hard disk. $Data=Get-Content -Path "C:AppsFinanceTestApp.xml" -Encoding Byte -ReadCount 0

Question 75
Which servers should you install the anti-spam agents and enable the anti-spam and antimalware filtering?
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.

Use the Set-SenderReputationConfig cmdlet to modify the sender reputation configuration on a Mailbox server or an Edge Transport server.

Use the Set-TransportConfig cmdlet to modify the transport configuration settings for the whole Exchange organization.

Set-TransportConfig not required in this scenario

Explanation/Reference:
Correct Answer: C

Question 76
What should you do next?
You need to ensure that all emails with the words "Free Credit Check" are rejected unless the email is sent to Finance Distribution Group.

You are configuring Anti-Spam Filtering on Server1.

Server1 runs Mailbox Server Role and Client Access Server Role.

You are configuring Anti-Spam Filtering on Server1.

You need to ensure that all emails with the words "Free Credit Check" are rejected unless the email is sent to Finance Distribution Group.

You also need to ensure that all emails from partner company Domain name adatum.com bypass the Anti-Spam Filter.

You run the Add-ContentFilterPhrase and add the words "Free Credit Check"

What should you do next?
A. Run the Set-TransportConfig and Set-ContentFilterConfig
B. Run the Set-SenderReputationConfig and Set-TransportConfig
C. Run the Set-ContentFilterConfig and Set-RecipientFilterConfig
D. Run the Set-SenderFilterConfig and Set-RecipientFilterConfig

Correct Answer: C

Explanation/Reference:
NOT A
Set-TransportConfig not required in this scenario
Use the Set-TransportConfig cmdlet to modify the transport configuration settings for the whole Exchange organization.

NOT B
Set-TransportConfig not required in this scenario
Use the Set-TransportConfig cmdlet to modify the transport configuration settings for the whole Exchange organization.

NOT C
Use the Set-SenderReputationConfig cmdlet to modify the sender reputation configuration on a Mailbox server or an Edge Transport server.

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.

NOT D
Who sent the emails is not required in this scenario
Use the Set-SenderFilterConfig cmdlet to modify the Sender Filter agent configuration:

EXAMPLE 1
This example makes the following modifications to the Sender Filter agent configuration:
- It enables blocking of blank senders.
- It blocks messages from lucernepublishing.com and all subdomains.
- It adds [email protected] and [email protected] to the blocked senders list without affecting any existing entries.

NOT E
You enable antimalware filtering on the Client Access Servers and the Mailbox Servers.

F. You enable antimalware filtering on the Client Access Servers and the Mailbox Servers.
E. You should enable antimalware filtering on the Mailbox servers only.
D. You enable antimalware filtering on the Client Access Servers only.
C. You enable antimalware filtering on all Exchange servers.
B. You enable antimalware filtering on the Mailbox servers only.
A. You enable antimalware filtering on the Client Access Servers only.

Correct Answer: BE

Question 77
Which WAN link or links should you identify?
Your network contains an internal network and a perimeter network. The internal network contains four offices. The perimeter network is located in a separate office.

Each internal office has a direct WAN link to all other internal offices.

Your network contains an internal network and a perimeter network. The internal network contains four offices. The perimeter network is located in a separate office.

Each internal office has a direct WAN link to all other internal offices.

Each of the four offices that make up the internal network is configured as an Active Directory site. The Active Directory sites and site links are configured as shown in the exhibit. (Click the Exhibit button.)

Your company has an Exchange Server 2013 organization. Each site contains two servers that have the Mailbox server role and the Client Access server role installed. To the perimeter network, you deploy two servers that have Exchange Server 2010 Service Pack 2 (SP2) and the Edge Transport server role installed. You configure an Edge Subscription to Site1. You deploy a new email notification application to Site4. The application will send 25,000 email messages daily to external recipients. You need to identify which WAN links will have increased traffic from the new email application. Which WAN link or links should you identify? (Each answer presents part of the solution. Choose all that apply.)

A. The WAN link between Site4 and the perimeter network
B. The WAN link between Site1 and Site3
C. The WAN link between Site1 and the perimeter network
D. The WAN link between Site4 and Site1
E. The WAN link between Site4 and Site2

Correct Answer: CE

Explanation/Reference:
C: The traffic will increase on the single WAN link on the perimeter network.
E: The traffic will increase between Site4 and Site2 since the cost of this link (5) plus the cost of the link between Site2 and Site1 (1) is lower than the cost of the direct link between Site4 and Site1 (10).

Incorrect answers:
Not A: There is no WAN link between Site4 and the perimeter network.
Not B: The cost of the WAN link between Site1 and Site3 is high (10). This path will not be chosen.
Not D: There is no WAN link between Site4 and Site1.

Question 78
Which three actions should you perform?
You have an Exchange Server 2007 organization. You recently deployed a server that has Exchange Server 2013 installed. The Exchange Server organization contains three servers. The servers are configured as shown in the following table.

Server2 contains a mailbox for a user named User1. You move the mailbox of User1 to Server3. After the move, User1 fails to access his mailbox by using Outlook Web App. Users who have mailboxes on Server1 and Server2 can access their mailboxes by using Outlook Web Access. You need to ensure that User1 can access his mailbox from the Internet by using Outlook Web App at https://mail.contoso.com. The solution must ensure that users who have mailboxes on Server1 and Server2 can continue to use Outlook Web Access. Which three actions should you perform? (Each correct answer presents part of the solution. Choose three.)

A. Export the certificate on Server1 and import the certificate to Server3.
B. On all of the Exchange servers, install a new certificate that contains the mail.contoso.com and legacy.contoso.com names.
C. Redirect all of the traffic from the Internet for mail.contoso.com to Server3.
E. Create a host (A) record named legacy.contoso.com that points to Server1.

Correct Answer: ABE

Explanation/Reference:
Client Connectivity in an Exchange 2013 Coexistence Environment

Question 79
Which cmdlet should you run?
You host Exchange Server 2013 organizations for several hundred tenants. The infrastructure contains several custom transport agents. You need to prevent the transport agents from overloading the processors on one of the Exchange servers. Which cmdlet should you run?
A. Set-WorkloadPolicy
B. Set-ResourcePolicy
C. Set-TransportAgent
D. Set-ThrottlingPolicy

Correct Answer: A

Explanation/Reference:

Question 80
Which three commands should you run?
DRAG DROP
You have an Exchange Server 2013 organization that contains a server named EX1. You have a user named User1 in the marketing department. You need to prevent User1 from submitting more than 50 email messages per minute to the Exchange Server organization by using Microsoft Outlook. Which three commands should you run?
To answer, move the three appropriate commands from the list of commands to the answer area and arrange them in the correct order. Select and Place:

Correct Answer:

Explanation/Reference:
Note:
Box 1:
* Use the New-ThrottlingPolicy cmdlet to create a non-default user throttling policy.
* The MessageRateLimit parameter specifies the number of messages per minute that can be submitted to transport.

Box 3:

Question 81
Which three actions should you perform?

You have an Exchange Server 2013 organization that contains four servers named EX1, EX2, EX3, and EX4. All of the servers are members of a database availability group (DAG) named DAG1.

Each server has a copy of a mailbox database named DB1. DB1 has the following characteristics:

- The replay lag time on EX4 is set to 14 days.
- Single item recovery on all of the servers is set to 14 days.
- None of the servers have Volume Shadow Copy Service (VSS) backups.

EX4 has a folder named F:RDB that is used to store database files during restore operations. Twenty days ago, a user named User1 deleted an email message that had a subject of “Sales Report”. You need to restore the deleted email message to the mailbox of User1.

You copy the lagged database and the log files that are older than 20 days to F:RDB.

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.

Select and Place:

Correct Answer: D

Explanation/Reference:

Reference: Create a Recovery Database
Reference: Restore Data Using a Recovery Database

Question 82
Which cmdlet should you run?

EX1 and EX2 are members of a database availability group (DAG) named DAG1. DAG1 contains four mailbox databases. All databases are active on EX1 and replicate to EX2.

You start an unplanned maintenance on EX1 and shut down EX1.

You discover that the databases do not mount on EX2.

You restart EX1 and the databases mount automatically on EX1.

You need to identify what prevents the databases from switching over successfully to EX2.

Which cmdlet should you run?

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

Correct Answer: D

Explanation/Reference:

Test-ReplicationHealth: Exchange 2013 Help

Question 83
What should you do first?

Your company has three offices. Each office is configured as an Active Directory site.

You have three servers that have Exchange Server 2013 installed named EX1, EX2 and EX3. All three servers have the Client Access server role and the Mailbox server role installed. The Active Directory site links and costs are configured as shown in the exhibit. (Click the Exhibit button.)

Site B is designated as a hub site.

EX2 fails. You discover that all email messages sent from the users in Site A to the users in Site C are queued on a server in Site A. You need to ensure that the email messages are sent to Site C as quickly as possible.

What should you do first?

A. Modify the Active Directory site link costs.
B. Configure Site A as a hub site.
C. Modify the Exchange-specific site link cost.
D. Remove the hub site.

Correct Answer: D
Explanation/Reference:

**Question 84**
Which three actions should you perform?

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.

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.

Contoso.

A: Use the Set-TransportConfig cmdlet to modify the transport configuration settings for the whole Exchange organization.

**Explanation/Reference:**

A: Run the set-transportconfig -tlssenddomainsecurelist contoso.com command.
B. 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.
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.

**Correct Answer: ADF**

**F.** 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.
**E.** Run the set-transportconfig -tlssenddomainsecurelist adatum.com command.
**D.** Run the New-SendConnector cmdlet and specify the domainsecureenabled parameter.

**Question 85**
Which cmdlet should you use?

You have an Exchange Server 2013 organization that contains five servers. Your company has a finance department, a marketing department, and a research department. Users in the marketing department are prevented from creating more than two Exchange ActiveSync device associations. Users in the research department are prevented from creating more than two Exchange ActiveSync device associations.

Which cmdlet should you use?

A. Set-ThrottlingPolicyAssociation
B. Set-ResourcePolicy
C. Set-ActiveSyncMailboxPolicy
D. Set-CASMailbox

Correct Answer: A
Explanation/Reference:

**Set-ThrottlingPolicyAssociation: Exchange 2013 Help**

**Set-ThrottlingPolicyAssociation: Exchange 2013 Help**

**Question 86**
Which three commands should you run?

You have an Exchange Server 2013 organization that contains three servers that have Exchange Server 2013 installed and one server that has Exchange Server 2010 installed.

You create the custom RBAC roles shown in the following table.

<table>
<thead>
<tr>
<th>Role</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managers</td>
<td>IT Administrators manage all of the users in the forest.</td>
</tr>
<tr>
<td>Help Desk</td>
<td>The Seattle helpdesk manages all of the users in an organizational unit (OU) named Seattle. The Miami helpdesk manages all of the users in an OU named Miami.</td>
</tr>
</tbody>
</table>

You need to recommend which commands must be run to prevent only the members of both help desks from modifying the properties of users who have a department attribute value of "Manager".

Which three commands should you run? (Each correct answer presents part of the solution. Choose three.)

A. new-managementscope "executive users exclusive scope" -recipientrestrictionfilter { department -eq "manager" } -exclusiveforce
B. new-managementroleassignment -name "managers" -securitygroup "managers" -role "mail recipients" -exclusiverecipientwritescope "executive users exclusive scope"
C. new-roleassignmentpolicy -name "limited end user policy" -roles "mypersonalinformation" -members admins
D. new-rolegroup -name "managers" -roles "mail recipients" -members admins
E. new-rolegroup -name "help desk" -roles "mail recipients" -members admins

Correct Answer: ABD
Explanation/Reference:

**Note:**

*(A) Use the New-ManagementScope cmdlet to create a regular or exclusive management scope. After you create a regular or exclusive scope, you need to associate the scope with a management role assignment. To associate a scope with a role assignment, use the New-ManagementRoleAssignment cmdlet.*

*(B) Use the New-ManagementRoleAssignment cmdlet to assign a management role to a management role group, management role assignment policy, user, or universal security group (USG).*

**Question 87**
Which two actions should you perform?

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. 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 (SCP) object in Active Directory to point to autodiscover.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 autodiscover.sales.contoso.com.

Correct Answer: BC

Explanation/Reference:
- 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.
- You will only need an autodiscover name for each SMTP domain that a user is likely to enter as their email address.

Autodiscover Service: Exchange 2013 Help

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.

Correct Answer: C

Explanation/Reference:
- 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. Enable-ExchangeCertificate: Exchange 2013 Help

Which cmdlet should you run?

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

Correct Answer: B

Explanation/Reference:

Use the New-Mailbox 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.

Use the Set-MailboxCalendarConfiguration cmdlet to apply calendar settings for users using Microsoft Office Outlook Web App calendars.

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.

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.

B New-Mailbox

Create a new Room Mailbox to schedule meetings in conference rooms, auditoriums, labs or other facilities

New-Mailbox -Name "<Room Name>" -Room

Example:

New-Mailbox -Name FL-ROOM1 -Room

A Look at Exchange Server 2013 Resource 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 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 90**
Which solutions should you recommend?

**HOTSPOT**
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.

**Hot Area:**

**Correct Answer:**

**Explanation/Reference:**
Exchange 2013 Virtualization: Exchange 2013 Help

**Question 91**
Which cmdlets should you use?

**DRAG DROP**
You have an Exchange Server 2013 organization that contains a server named Server1. A user named User1 has an administrative assistant named Assistant1. 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 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.)

Select and Place:

**Correct Answer:**

**Explanation/Reference:**
Add-MailboxFolderPermission
Use the Add-MailboxFolderPermission cmdlet to manage folder-level permissions for all folders within a user’s mailbox.

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

Add-ADPermission
Use the Add-ADPermission cmdlet to add permissions to an 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.

For information about the parameter sets in the Syntax section below, see Syntax.
Set-Mailbox -Identity John -DeliverToMailboxAndForward $true -ForwardingSMTPAddress [email protected]

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.

Add-ADPermission: Exchange 2013 Help
Active Directory Permissions Role: Exchange 2013 Help
Set-Mailbox: Exchange 2013 Help

Question 92
Which command should you run? (HOTSPOT)
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.)
Hot Area:

Correct Answer:

Explanation/Reference:
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.

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
Set-ExchangeServer: Exchange 2013 Help

Question 93
Which command should you run? (HOTSPOT)
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 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.)
Hot Area:

Correct Answer:

Explanation/Reference:
Note:
* Do not use the New-TransportRule cmdlet to create a transport rule in your organization.

/Example:
New-TransportRule “BlockMessagesBetweenSalesAndBrokerage” -BetweenMemberOf1 “Sales-Group” -BetweenMemberOf2 “Brokerage-Group” – ExceptIfFrom “Tony Smith”, “Pilar Ackerman” – ExceptIfSubjectContainsWords “Press Release”, “Corporate Communication” – RejectMessageEnhancedStatusCode “5.7.1” – RejectMessageReasonText “Email messages sent between the Sales department and the Brokerage department are prohibited.”

* Box 2:
The SmtpRejectMessageRejectText parameter specifies a text string to add to the rejection message. You must use this parameter with the SmtpRejectMessageRejectStatusCode parameter.

Incorrect:
* Do not use the New-DlpPolicy cmdlet to create data loss prevention (DLP) policies in your Exchange organization.
* No parameter -ClassificationID

Box 2: should be RejectMessageEnhancedStatusCode
The RejectMessageEnhancedStatusCode parameter specifies an enhanced status code to provide when rejecting messages. Valid values are 5.7.1 or between 5.7.1 and 5.7.999.

Note:
The transport rule can add a custom rejection message. To further customize the delivery status notification (DSN), you need to create a custom DSN message using the New-SystemMessage cmdlet.

If an enhanced status code isn’t specified, and only the RejectMessageReasonText parameter is used, the enhanced status code 5.7.1 is used. This parameter is used to define a rule action.
New-TransportRule: Exchange 2013 Help
Question 94
Which cmdlet should you run?
Your company has four regional offices and 20 branch offices. The regional offices connect to each other by using a 30-Mbps WAN link. Each branch office connects to its nearest regional office by using a 1-Mbps WAN link.
The network contains an Active Directory forest. The forest contains a domain controller in each office. Each office maps to an Active Directory site.
Each branch office site connects to the nearest regional office site by using an Active Directory site link.
You have an Exchange Server 2013 organization that contains one server in each office.
You need to implement a messaging solution to meet the following requirements:
- The users in the branch offices must only be able to send email messages that are up to 2 MB to the users in the other offices.
- The users in the regional offices must be prevented from sending email messages that are larger than 5 MB to the users in any of the regional offices.
Which cmdlet should you run?
A. Set-TransportRule
B. Set-ADSite
C. Set-AdSiteLink
D. Set-RoutingGroupConnector
Correct Answer: C
Explanation/Reference:
Explanation:
NOT A
Does not relate to message size
Set-TransportRule
Use the Set-TransportRule cmdlet to modify an existing transport rule in your organization.
For information about the parameter sets in the Syntax section below, see Syntax.
EXAMPLE 1
This example modifies the Sales Team Disclaimer transport rule. Modifying the value of one predicate doesn’t affect other predicates used in the rule’s conditions or exceptions and doesn’t affect actions on the same rule.
This example sets the FromMemberOf parameter to a value of Sales-Group, which specifies that the rule is applied if the sender of the message is a member of the Sales-Group distribution group.
Set-TransportRule "Sales Team Disclaimer" -FromMemberOf "Sales-Group"
NOT B
Does not relate to message size
Set-ADSite
Use the Set-ADSite cmdlet to configure the Exchange settings of Active Directory sites.
EXAMPLE 1
This example configures the Active Directory site named Default-First-Site-Name as a hub site.
Set-AdSite Default-First-Site-Name -HubSiteEnabled True
NOT D
Does not relate to message size
Set-RoutingGroupConnector
With routing groups and Routing Group connectors you can consolidate communication between servers by designating bridgehead servers that act as communication points between routing groups. For example, your organization may have a remote site connected through a wide-area-network (WAN) link to your main office. In this example, you can use a Routing Group connector to route Exchange traffic between a server at your main office and a server at your remote site.
C
The only command that deals with message size.
Set-AdSiteLink
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
Set-AdSiteLink: Exchange 2013 Help

Question 95
Which two tasks should you perform?
You have an Exchange Server 2013 organization named 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. Set-RoutingGroupConnector
E. Modify the Exchange ActiveSync policy that applies to User1’s mailbox.
F. Create a new mobile device mailbox policy.
Correct Answer: BE
Explanation/Reference:
Explanation:
NOT A
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.
Question 96
Which cmdlet should you run?
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

Correct Answer: A

Explanation/Reference:
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
Test-ServiceHealth
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
Get-AvailabilityReportOutage
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
Test-ReplicationHealth - Exchange 2013 Help

Question 97
Which two tasks should you perform?
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 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

Correct Answer: AB

Explanation/Reference:
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

You deploy an Active Directory forest that contains two domains named contoso.com and child.contoso.com.
You plan to deploy Exchange Server 2013 servers to the child.contoso.com domain.

You need to prepare Active Directory for the installation of the first Exchange Server 2013 servers.

Which command should you run in each domain? (To answer, drag the appropriate commands to the correct domains. Each command 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.)

Select and Place:

Correct Answer:

Explanation/Reference:

For more information about RBAC, see Understanding Role Based Access Control.

Delegated Setup: Exchange 2013 Help

References


A disconnected mailbox is a mailbox object in the mailbox database that isn’t associated with an Active Directory user account. There are two types of disconnected mailboxes:

- Disabled mailboxes
- Soft-deleted mailboxes

When a mailbox is disabled or deleted in the Exchange Administration Center (EAC) or using the Disable-Mailbox or Remove-Mailbox cmdlet in the Exchange Management Shell, Exchange retains the deleted mailbox in the mailbox database, and switches the mailbox to a disabled state. This is why mailboxes that are either disabled or deleted are referred to as disabled mailboxes. The difference is that when you disable a mailbox, the Exchange attributes are removed from the corresponding Active Directory user account, but the user account is retained. When you delete a mailbox, both the Exchange attributes and the Active Directory user account are deleted.

Disconnected and deleted mailboxes are retained in the mailbox database until the deleted mailbox retention period expires, which is 30 days by default. After the retention period expires, the mailbox is permanently deleted (also called purged). If a mailbox is deleted using the Remove-Mailbox cmdlet, it’s also retained for the duration of the retention period.

Important:
If a mailbox is deleted using the Remove-Mailbox cmdlet and either the Permanent or StoreMailboxIdentity parameter, it will be immediately deleted from the mailbox database. To identify the disabled mailboxes in your organization, run the following command in the Shell.

```
Get-MailboxDatabase | Get-MailboxStatistics | Where { $_.DisconnectReason -eq "Disabled" } | ft DisplayName, Database, DisconnectDate
```

Soft-deleted mailboxes

When a mailbox is moved to a different mailbox database, Exchange doesn’t fully delete the mailbox from the source mailbox database when the move is complete. Instead, the mailbox in the source mailbox database is switched to a soft-deleted state. Like disabled mailboxes, soft-deleted mailboxes are retained in the source database either until the deleted mailbox retention period expires or until the Remove-StoreMailbox cmdlet is used to purge the mailbox.

Run the following command to identify soft-deleted mailboxes in your organization.

```
Get-MailboxDatabase | Get-MailboxStatistics | Where { $_.DisconnectReason -eq "SoftDeleted" } | ft DisplayName, Database, DisconnectDate
```

NOT A
Need to modify the deleted mailbox retention settings
NOT C
Not related to an item but to databases
NOT D
Need to modify the deleted mailbox retention settings.

Explanation:

```
Set-MailboxDatabase -Identity MDB2 -DeletedItemRetention 365
```

The following command like Set-MailboxDatabase -Identity MDB4 –DeletedItemRetention 365 to hold content from being deleted off the Exchange server.

Journaling: With journaling, the organization can have exact copies of content captured and retained in a separate database (a "journaling database") to ensure the content has not been tampered with and is available for legal search and review at a future time Retention Policy: Content within an Exchange environment can be set to be retained (or purged) based on policies set on the Exchange databases, so either configured through the Exchange Admin console or through a PowerShell command like Set-MailboxDatabase -Identity MDB4 –RetentionPolicy 365 to hold content from being deleted off the Exchange server.

Personal Archives: Each user in Exchange can have their personal mailbox and an Archive mailbox where the archive mailbox can have content drag/dropped to the archive box for long term storage, similar to what users have historically used Personal Store (PST) files in the past. Unlike a PST file that is almost completely unmanaged by the organization (yet is still considered legal evidence), the Personal Archive in Exchange is part of the Exchange environment with content that can be searched, set for long term retention, and put on legal hold.

Configure Deleted Item Retention and Recoverable Items Quotas: Exchange 2013 Help
Question 101
Which three actions should you perform?

**DRAG DROP**

You have an Exchange Server 2013 organization that contains a database availability group (DAG). There are four copies of every mailbox database. One of the copies is a lagged copy configured to have a replay lag time of 14 days. All mailboxes have single item recovery enabled. All databases are configured to have a deleted item retention period of seven days.

A company executive reports that an email message, which was deleted 10 days ago, must be restored.

You need to ensure that you can recover the email message from the lagged copy of the mailbox database. The solution must preserve the lagged copy of the mailbox database.

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.

Select and Place:

---

**Correct Answer:**

**Explanation/Reference:**

**Explanation:**

1. Use the Move-ActiveMailboxDatabase cmdlet to perform a database or server switchover.
2. Use vssadmin to check that there could be VSS errors causing the datasources not to enumerate.

**Explanation:**

The key to matching log files and databases is the signature. You can view log file signatures by using the Exchange Server Database Utilities (Eseutil.exe) tool and viewing the log file header with the command Eseutil /l [log filename]. You can view database (.edb) and streaming database (.stm) file signatures by viewing the file header with Eseutil /mh [database filename].

A typical log file or database file signature looks like this:


Activating and recovering a lagged mailbox database copy is an easy process if you want the database to replay all log files and make the database copy current. If you want to replay log files up to a specific point in time, it’s a more difficult operation because you manually manipulate log files and run Exchange Server Database Utilities (Eseutil.exe).

Suspend-MailboxDatabaseCopy Use the Suspend-MailboxDatabaseCopy cmdlet to block replication and replay activities (log copying and replay) or activation for a database configured with two or more database copies.

For a variety of reasons, such as performing planned maintenance, it may be necessary to suspend and resume continuous replication activity for a database copy. In addition, some administrative tasks, such as seeding, require you to temporarily suspend a database copy.

We recommend that all replication activity be suspended when the path to the database or its log files is being changed.

You can suspend and resume database copy activity by using the LMC or by running the Suspend-MailboxDatabaseCopy and Resume-MailboxDatabaseCopy cmdlets in the Shell.

**EXAMPLE 1**

This example suspends replication and replay activity for the copy of the database DB1 hosted on the Mailbox server MBX3. An optional administrative reason for the suspension is specified.

Suspend-MailboxDatabaseCopy -Identity DB1MBX3-SuspendComment "Maintenance on MBX3" -NOT Move-ActiveMailboxDatabase

Not attempting to make a passive or lagged database active.

You need to ensure that you can recover the email message from the lagged copy of the mailbox database.

The solution must preserve the lagged copy of the mailbox database.

**STEPS**

No need to use Move-ActiveMailboxDatabase

1. Use the Suspend-MailboxDatabaseCopy cmdlet to block replication and replay activities (log copying and replay)
2. Use vssadmin to check that there could be VSS errors causing the datasources not to enumerate.

**Question 102**

Which command should you run on EX1 and EX3?

**DRAG DROP**

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.

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.)

Select and Place:

---

**Correct Answer:**

**Explanation/Reference:**

**Explanation:**

Enable-OutlookAnywhere
Exchange 2010 command
EX1 is an exchange 2010 server
Use the Enable-OutlookAnywhere cmdlet to enable Outlook Anywhere on a computer running Microsoft Exchange Server 2010 that has the Client Access server role installed. Running the Enable-OutlookAnywhere cmdlet enables the server to accept requests from Microsoft Office Outlook 2007 and Outlook 2003 client computers from the Internet by using Outlook Anywhere, also known as RPC over HTTP.

Disable-OutlookAnywhere
Need to enable it or disable it
Set-ClientAccessServer
Exchange 2013
Use the Set-ClientAccessServer cmdlet to set properties on specified Client Access server objects.
Set-OutlookAnywhere
Exchange 2013
Use the Set-OutlookAnywhere cmdlet to modify the properties on a computer running Microsoft Exchange Server 2013 enabled for Microsoft Outlook Anywhere. The syntax for the cmdlets to configure Outlook Anywhere look like the following:
Set-OutlookAnywhere -Identity 'rs_name (Default Web Site)'
In our example, to set the internal and external URL’s we will use the following:
Set-OutlookAnywhere -Identity 'rs_name' -ExternalHostName mail.ae.com -InternalHostName mail.ae.com
-ExternalClientAuthenticationMethod Ntlm
-ExternalClientsRequireSsl:True -InternalClientAuthenticationMethod Ntlm -InternalClientsRequireSsl:True
-IPAuthentication Ntlm -SSLOffloading:False
Remember to enter this all together on one line without pressing enter. The command may be long, but we successfully configured everything from a cmdlet without having to go into the IAC, logging in, clicking here, clicking there, etc...
Set-OutlookProvider
Exchange 2013
Use the Set-OutlookProvider cmdlet to set specific global settings using the msExchOutlookProvider attribute on the msExchAutoDiscoverConfig object in Active Directory.
For information about the parameter sets in the Syntax section below, see Syntax.
This example changes the duration that the Autodiscover service settings are valid for the Microsoft Outlook provider msExchAutoDiscoverConfig.
Set-OutlookProvider -Identity msExchAutoDiscoverConfig -TTL 2
Enable-OutlookAnywhere: Exchange 2010 Help
Set-OutlookAnywhere: Exchange 2013 Help

Question 103
What should you do?
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.

<table>
<thead>
<tr>
<th>Server</th>
<th>Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>EX1</td>
<td>Mailbox Server</td>
</tr>
<tr>
<td>EX2</td>
<td>Mailbox Server</td>
</tr>
</tbody>
</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?
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.

Correct Answer: B
Explanation/Reference:
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 Transport service on a Mailbox Server
Every message that’s sent or received by 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 database 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 antispam and antispoofing 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-spoofing agent, it’s put in the Submission queue.
- Submission: 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-address decoding, 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.
Messages in the poison message queue.
OWA DRAFTS FOLDER
http://thoughtsfandemlind.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 send 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 A C
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.
Mail Flow: Exchange 2013 Help

Question 104
Which two commands should you run?
You have an Exchange Server 2013 organization that contains two Mailbox servers named MBX1 and MBX2.
You create a database availability group (DAG) named DAG1. DAG1 is configured as shown in the exhibit. (Click the Exhibit button.)

Correct Answer: BC
Explanation/Reference:
Explanation:
You need to ensure that replication only occurs over the replication network.
If you would like to ‘force’ replication to only go over the Replication Network, then you definitely would like to disable replication on the MAPI Network, but if the NIC on the Replication Network goes down, it will start replicating over the MAPI NIC.
There is no way of blocking that behaviour and isn’t what you’d want anyway since DAGs actually cope quite fine with just 1 NIC.

DAG Networks
Each database availability group (DAG) network has several properties that you can configure, including the name of the DAG network, a description field for the DAG network, a list of subnets that are used by the DAG network, and whether the DAG network is enabled for replication.
You can configure a DAG network only when automatic configuration has been disabled for a DAG.
There are specific networking requirements that must be met for each DAG and for each DAG member. Each DAG must have a single MAPI network, which is used by a DAG member to communicate with other servers (for example, other Exchange 2013 servers or directory servers), and zero or more Replication networks, which are networks dedicated to log shipping and seeding.
Although a single network is supported, we recommend that each DAG have at least two networks: a single MAPI network and a single Replication network. This provides resiliency for the network and the network path, and enables the system to distinguish between a server failure and a network failure. Using a single network configuration prevents the system from distinguishing between these two types of failures.

M API
MAPI stands for Messaging Application Programming Interface, and it gives programs the ability to send email using your email program to do the actual sending.
Set-DatabaseAvailabilityGroup
The Set-DatabaseAvailabilityGroup cmdlet enables you to manage DAG properties that can’t be managed from the Exchange Administration Center (EAC), such as configuring network discovery, selecting the TCP port used for replication, and enabling datacenter activation coordination (DAC) mode.

Set-DatabaseAvailabilityGroupNetwork
Use the Set-DatabaseAvailabilityGroupNetwork cmdlet to configure a network for a database availability group (DAG). You can configure a variety of network properties, such as the name for the network, a description of the network, a list of one or more subnets that comprise the network, and whether the network is enabled for replication (log shipping and seeding).
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.
C
Ensures that you can configure a DAG network by turning the automatic configuration off:
The ManualDagNetworkConfiguration parameter
Specifies whether DAG networks should be automatically configured. If this parameter is set to False, DAG networks are automatically configured. If this parameter is set to True, you must manually configure DAG networks.
You can configure a DAG network only when automatic network configuration has been disabled for a DAG.
Need to manually configure the DAG NETWORK

NOT D

Need to turn the automatic DAG configuration off.

The ManualDagNetworkConfiguration parameter specifies whether DAG networks should be automatically configured. If this parameter is set to False, DAG networks are automatically configured. If this parameter is set to True, you must manually configure DAG networks.

You can configure a DAG network only when automatic network configuration has been disabled for a DAG.

NOT A

Does not disable the replication over the MAPI network as required in this scenario

B

Disables replication over the MAPI network as required in this scenario

Set-DatabaseAvailabilityGroup: Exchange 2013 Help
Set-DatabaseAvailabilityGroupNetwork: Exchange 2013 Help

Question 105

What are two possible ways to achieve this goal?

You have an Exchange Server 2013 organization that contains a server named Server1.

Server1 has an IP address of 10.1.100.16 and is configured to use a default gateway of 10.1.100.1.

You deploy a hardware load balancer that is configured to use the IP addresses of 192.168.101.31 and 10.1.100.31.

A user named User1 has a client computer that has an IP address of 102.168.101.201. User1 reports that he cannot view his mailbox by using Outlook Web App.

When you review the IIS logs on Server1, you discover the following information:

#Fields: date time cs-method cs-uri-stem s-port c-ip cs(Referer) sc-status
2013-01-09 00:08:55 POST /owa/ev.owa2 443 192.168.101.201 https://owa.fabrikam.com/owa/ 200

You need to ensure that User1 can access his mailbox successfully from Outlook Web App.

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

A. Configure the hardware load balancer to use the same certificate as the certificate used on Server1.
B. Configure the hardware load balancer to use source NAT (SNAT).
C. Configure the computer of User1 to ignore response headers.
D. Modify the default gateway of Server1.

Correct Answer: BD

Explanation/Reference:

Source NAT

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 servers to see the IP that made the connection.

They are then able to return the requested information correctly.

B. Configuring the hardware load balancer to use source NAT (SNAT) will resolve the problem.

D. Changing the default gateway of Server1 to that of the hardware load balancer will ensure that the connection to Server1 will be returned via the network load balancer and out to User1.

NOT A

Not a certificate problem.

NOT C

Not a http response header issue.

HTTP response header

The information, in the form of a text record, that a Web server sends back to a client's browser in response to receiving an HTTP request.

The response header contains the date, size and type of file that the server is sending back to the client and also data about the server itself.

The header is attached to the file being sent back to the client.

Question 106

Which command should you run?

You have an Exchange Server 2013 organization that is configured to filter email messages for spam and malware.

You need to modify the schedule for applying updates to the anti-spam and the antimalware definitions.

Which command should you run?

A. Update-MalwareFilteringServer.ps1
B. Set-MalwareFilteringServer
C. Set-SenderFilterConfig
D. Update-SafeList

Correct Answer: B

Explanation/Reference:

Microsoft Exchange Server 2013 administrators can manually download anti-malware engine and definition (signature) updates.

Update-MalwareFilteringServer.ps1 is used in manual updates not schedule updates.

NOT C

Not used for spam and malware updates.

Use the Set-SenderFilterConfig cmdlet to modify the Sender Filter agent configuration.

EXAMPLE 1

This example makes the following modifications to the Sender Filter agent configuration:

- It enables blocking of blank senders.
- It blocks messages from lucernepublishing.com and all subdomains.
- It adds [email protected] and [email protected] to the blocked senders list without affecting any existing entries.

Set-SenderFilterConfig -BlankSenderBlockingEnabled $true -BlockedDomainsAndSubdomains lucernepublishing.com -BlockedSenders @
{Add="[email protected]","[email protected]"
 NOT D

Use the Update-SafeList cmdlet to update the safelist aggregation data in Active Directory.

Safe list aggregation data is used in the built-in anti-spam filtering in Microsoft Exchange. EdgeSync replicates safelist aggregation data to Edge Transport servers in the perimeter network.

EXAMPLE 1

This example updates Safe Senders List data for the single user [email protected]

Update-SafeList [email protected]

B

Set-MalwareFilteringServer

Use the Set-MalwareFilteringServer cmdlet to configure the Malware agent settings in the Transport service on a Mailbox server.

Example 1
This example sets the following Malware agent settings on the Mailbox server named Mailbox01:
Sets the update frequency interval to 2 hours
Sets the time to wait between resubmit attempts to 10 minutes
Set-MalwareFilteringServer Mailbox01 -UpdateFrequency 120 -DefeferWaitTime 10
Set-MalwareFilteringServer - Exchange 2013 Help

Question 107
Which command should you run?

HOTSPOT
Your network contains an Active Directory forest named contoso.com. The forest contains two sites named Site1 and Site2.
You have an Exchange Server 2013 organization that contains two servers. The servers are configured as shown in the following table.

<table>
<thead>
<tr>
<th>Hot Area</th>
<th>Explanation/Reference:</th>
</tr>
</thead>
<tbody>
<tr>
<td>☐</td>
<td>The AutoDiscover service automatically configures user profile settings for clients running Microsoft Office Outlook 2007, Outlook 2010, or Outlook 2013, as well as supported mobile phones.</td>
</tr>
<tr>
<td>☐</td>
<td>Clients that connect to the AutoDiscover service by using the internal URL must belong to a listed site.</td>
</tr>
<tr>
<td>☐</td>
<td>The AutoDiscoverServiceInternalURI parameter specifies the internal URL of the AutoDiscover service.</td>
</tr>
<tr>
<td>☐</td>
<td>An administrator creates a new Active Directory site named Site3. The administrator creates mailboxes for the users in Site3. All of the mailboxes of the Site3 users are located on EX1.</td>
</tr>
<tr>
<td>☐</td>
<td>Site3 contains a domain controller named dc3.contoso.com. The Site3 users report that sometimes, when they open Microsoft Outlook, it takes a long time to access their mailbox.</td>
</tr>
<tr>
<td>☐</td>
<td>You need to reduce the amount of time it takes for the users to access their mailbox.</td>
</tr>
</tbody>
</table>

Correct Answer:

- The AutoDiscoverService parameter specifies the Autodiscover service for the specified server. You can use this parameter to point to an Autodiscover service other than the default one.
- The AutoDiscoverSiteScope parameter specifies the site for which the Autodiscover service is authoritative.
- The AutoDiscoverSiteScope parameter allows you to configure the Autodiscover service to work for a specific site scope.

For more information, see Set-ClientAccessServer.

SECTION1
Set-ClientAccessServer EX1
Use the Set-ClientAccessServer cmdlet to set properties on specified Client Access server objects. Use the Set-ClientAccessServer cmdlet to change AutoDiscover settings.
NOT Set-ExchangeServer
Use the Set-ExchangeServer cmdlet to set Exchange attributes in Active Directory for a specified server.
NOT Set-RPCClientAccess
Use the Set-RpCClientAccess cmdlet to manage the settings for the Exchange RPC Client Access service that’s running on a Microsoft Exchange Server 2010 Client Access server.

SECTION2
- AutoDiscoverSiteScope 'Site1;Site3'
The AutoDiscoverSiteScope parameter specifying the site for which the Autodiscover service is authoritative.
- The AutoDiscoverServiceInternalURI parameter specifies the service connection point (SCP) on the server where you install the Client Access service.
- The SCP object contains the authoritative list of Autodiscover service URLs for the forest. You can use the Set-ClientAccessServer cmdlet to update the SCP object.

Question 108
Which two actions should you perform?

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.

Correct Answer: BE

Explanation/Reference:
Explanation:

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 basic resources:

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 exch01autodiscover* | 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 exch01ecp* | 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
LiveIdAuthentication : False
AdfsAuthentication : False
IIS FE: Anonymous, Basic
IIS BE: Anonymous, Basic

EWS
[PS] C:\Windows\system32>Get-WebServicesVirtualDirectory exch01ews* | 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 : False
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 exch01microsoft* | fl name, internal*, external*, *authentication
Name : Microsoft-Server-ActiveSync (Default Web Site)
InternalUrl : https://exch01.contoso.com/Exchange.asmx
InternalAuthenticationMethods : []
ExternalUrl :
ExternalAuthenticationMethods : []
IIS FE: Basic
IIS FE: Basic

OAB
[PS] C:\Windows\system32>Get-oabVirtualDirectory exch01oab* | fl name, internal*, external*, *authentication
Name : OAB (Default Web Site)
Question 109
Which three commands should you run in sequence?

You have an Exchange Server 2013 organization named adatum.com. The organization contains a server named Server1. Server1 is a member of a Database Availability Group (DAG) named DAG1. You have a user named Sales1 in the Sales department. You need to prevent Sales1 from submitting more than 75 email messages per minute to the Exchange Server organization by using Microsoft Outlook. Which three commands should you run in sequence? (To answer, move the appropriate three commands from the list of commands to the answer area and arrange them in the correct order.)

Select and Place:

Correct Answer:

Explanation/Reference:

The MaxOutboundConnections parameter specifies the maximum number of outbound connections that can be open at a time.

The Identity parameter specifies the server that you want to modify.

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

<table>
<thead>
<tr>
<th>DRAG DROP</th>
<th>Which three actions should you perform in sequence?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set-ThrottlingPolicyAssociation: Exchange 2013 Help</td>
<td></td>
</tr>
<tr>
<td>New-ThrottlingPolicy: Exchange 2013 Help</td>
<td></td>
</tr>
<tr>
<td>3. Set-mailbox -identity sales1 – throttlingpolicy $b</td>
<td>Attaches the throttling policy named limits to the user named Sales1</td>
</tr>
<tr>
<td>2. $b = get-throttlingpolicy limits</td>
<td>Establishes a variable $b with the attributes of the new throttling policy called limits</td>
</tr>
<tr>
<td>1. New-throttlingpolicy limits - messageratelimit 75</td>
<td>Creates a new throttling policy called limits with a limit of 75 email messages per minute being sent to the exchange server</td>
</tr>
</tbody>
</table>

The value of the MaxOutboundConnections parameter must be greater than or equal to the value of the MaxPerDomainOutboundConnections parameter.

Set-TransportServer Mailbox01 -DelayNotificationTimeout 13:00:00

This example sets the DelayNotificationTimeout parameter to 13 hours on server named Mailbox01.

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.

Use the Set-Mailbox cmdlet to modify the settings of an existing mailbox. You can use this cmdlet for one mailbox at a time.

Set-Mailbox -Identity John -DeliverToMailboxAndForward $true -ForwardingSMTPAddress [email protected]

The Identity parameter specifies the mailbox.

This parameter accepts the following values:

- Alias
- Example: JPhillips
- Canonical DN
- Display Name
- Example: Jeff Phillips
- Distinguished Name (DN)
- Example: CN=JPhillips,CN=Users,DC=Corp,DC=contoso,DC=com
- DomainAccount
- Example: AtlantaJPhillips
- GUID
- Example: fb456636-fe7d-4d58-9d15-5af57d0354c2
- Immutable ID
- Example: [email protected]
- Legacy Exchange DN
- Example: /o=Contoso/ou=AdministrativeGroup/cn=Recipients/cn=JPhillips
- SMTP Address
- Example: [email protected]
- UserPrincipalName
- Example: [email protected]
- The RecipientLimits parameter specifies the maximum number of recipients per message to which this mailbox can send.
- You must specify either an integer or unlimited.
- If you set this attribute on a mailbox, that mailbox setting overrides the value set for this attribute in the Transport service.
- The ThrottlingPolicy parameter specifies the identity of the throttling policy for this mailbox.
- New-throttlingpolicy limits
- Use the New-ThrottlingPolicy cmdlet to create a non-default user throttling policy.

EXAMPLE 1

This example creates a non-default user throttling policy that can be associated with specific users. Any parameter that you omit inherit the values from the default throttling policy GlobalThrottlingPolicy_

After you create this policy, you must associate it with specific users.

New-ThrottlingPolicy -Name ITUserPolicy -EwsMaxConcurrency 4 -ThrottlingPolicyScope Regular

The RecipientRateLimit parameter specifies the limits on the number of recipients that a user can address in a 24-hour period.

The MessageRateLimit parameter specifies the number of messages per minute that can be submitted to transport.

For messages submitted through the Mailbox server role (using Microsoft Outlook, Microsoft Office Outlook Web App, Exchange ActiveSync, or Exchange Web Services), this results in the deferral of messages until the quota for the user is available. Specifically, messages appear in the Outbox or Drafts folder for longer periods of time when users submit messages at a rate greater than the MessageRateLimit parameter.

For POP or IMAP clients submitting messages directly to transport using SMTP, clients receive a transient error if they submit at a rate that exceeds the MessageRateLimit parameter. Exchange attempts to connect and send the messages at a later time.

New-throttlingpolicy

Use the Get-ThrottlingPolicy cmdlet to view the user throttling settings for one or more throttling policies.

Set-transportserver-identity

Use the Set-TransportServer cmdlet to set the transport configuration options for the Transport service on Mailbox servers or for Edge Transport servers.

EXAMPLE 1

This example sets the DelayNotificationTimeout parameter to 13 hours on server named Mailbox01.

Set-TransportServer Mailbox01 -DelayNotificationTimeout 13:00:00

The Identity parameter specifies the server that you want to modify.

The MaxOutboundConnections parameter specifies the maximum number of outbound connections that can be open at a time.

The default value is 1000. The valid input range for this parameter is from 1 through 2147483647. If you enter a value of unlimited, no limit is imposed on the number of outbound connections.

For messages submitted through the Mailbox server role (using Microsoft Outlook, Microsoft Office Outlook Web App, Exchange ActiveSync, or Exchange Web Services), this results in the deferral of messages until the quota for the user is available. Specifically, messages appear in the Outbox or Drafts folder for longer periods of time when users submit messages at a rate greater than the MessageRateLimit parameter.

For POP or IMAP clients submitting messages directly to transport using SMTP, clients receive a transient error if they submit at a rate that exceeds the MessageRateLimit parameter. Exchange attempts to connect and send the messages at a later time.

New-throttlingpolicy limits

Use the New-ThrottlingPolicy cmdlet to create a non-default user throttling policy.

EXAMPLE 1

This example creates a non-default user throttling policy that can be associated with specific users. Any parameter that you omit inherit the values from the default throttling policy GlobalThrottlingPolicy_

After you create this policy, you must associate it with specific users.

New-ThrottlingPolicy -Name ITUserPolicy -EwsMaxConcurrency 4 -ThrottlingPolicyScope Regular

The RecipientRateLimit parameter specifies the limits on the number of recipients that a user can address in a 24-hour period.

The MessageRateLimit parameter specifies the number of messages per minute that can be submitted to transport.

For messages submitted through the Mailbox server role (using Microsoft Outlook, Microsoft Office Outlook Web App, Exchange ActiveSync, or Exchange Web Services), this results in the deferral of messages until the quota for the user is available. Specifically, messages appear in the Outbox or Drafts folder for longer periods of time when users submit messages at a rate greater than the MessageRateLimit parameter.

For POP or IMAP clients submitting messages directly to transport using SMTP, clients receive a transient error if they submit at a rate that exceeds the MessageRateLimit parameter. Exchange attempts to connect and send the messages at a later time.

New-throttlingpolicy

Use the Get-ThrottlingPolicy cmdlet to view the user throttling settings for one or more throttling policies.

Set-transportserver-identity

Use the Set-TransportServer cmdlet to set the transport configuration options for the Transport service on Mailbox servers or for Edge Transport servers.

EXAMPLE 1

This example sets the DelayNotificationTimeout parameter to 13 hours on server named Mailbox01.

Set-TransportServer Mailbox01 -DelayNotificationTimeout 13:00:00

The Identity parameter specifies the server that you want to modify.

The MaxOutboundConnections parameter specifies the maximum number of outbound connections that can be open at a time.

The default value is 1000. The valid input range for this parameter is from 1 through 2147483647. If you enter a value of unlimited, no limit is imposed on the number of outbound connections.

The value of the MaxOutboundConnections parameter must be greater than or equal to the value of the MaxPerDomainOutboundConnections parameter.

STEPS

1. New-throttlingpolicy limits messageratelimit 75 Creates a new throttling policy called limits with a limit of 75 email messages per minute being sent to the exchange server
2. $b = get-throttlingpolicy limits Establishes a variable $b with the attributes of the new throttling policy called limits
3. Set-mailbox -identity sales1 -throttlingpolicy $b Attaches the throttling policy named limits to the user named Sales1

New-ThrottlingPolicy: Exchange 2013 Help

Set-ThrottlingPolicy: Exchange 2013 Help

Create a Database Availability Group: Exchange 2013 Help

Correct Answer: Create a Database Availability Group: Exchange 2013 Help

Explanation/Reference:

Create a Database Availability Group: Exchange 2013 Help
Your company has a main office site and a disaster recovery site. The two sites connect to each other by using redundant WAN links. Each site connects directly to the Internet. Each site contains one Exchange Server 2013 server that is accessible from the Internet.

The company uses the @contoso.com email address suffix. The DNS records that can be resolved from the Internet are configured as shown in the following table.

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>mail2.contoso.com</td>
<td>MX</td>
<td>20</td>
</tr>
<tr>
<td>mail2.alias.contoso.com</td>
<td>CNAME</td>
<td>foo.example.com.</td>
</tr>
<tr>
<td>bar.example.com</td>
<td>A</td>
<td>192.0.2.23</td>
</tr>
<tr>
<td>mail2.alias.contoso.com</td>
<td>A</td>
<td>131.107.101.1</td>
</tr>
</tbody>
</table>

When the Internet link at the main office site fails, the company cannot receive incoming email from the Internet. You need to ensure that incoming email from the Internet is delivered to Server1. Incoming email from the Internet must be delivered to Server2 if Server1 is unavailable.

What should you create?

A. A CNAME record for the name mail.contoso.com that resolves to server2.contoso.com
B. An MX record that has a cost of 20 and resolves to mail.contoso.com
C. An MX record that has a cost of 20 and resolves to server2.contoso.com
D. An A record for the name mail.contoso.com that resolves to 131.107.101.1

Correct Answer: C

Explanation/Reference:

A CNAME record is an abbreviation for Canonical Name record and is a type of resource record in the Domain Name System (DNS) that specifies that another domain name is an alias of another, canonical domain name. Here “canonical” usually means: a more generally accepted or standard name.

For example, if there is a DNS zone as follows:

<table>
<thead>
<tr>
<th>Name</th>
<th>Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>bar.example.com</td>
<td>A</td>
<td>192.0.2.23</td>
</tr>
<tr>
<td>A MX record</td>
<td></td>
<td>A 192.0.2.23</td>
</tr>
<tr>
<td>CNAME record</td>
<td></td>
<td>foo.example.com.</td>
</tr>
</tbody>
</table>

A mail exchanger record (MX record) is a type of resource record in the Domain Name System that specifies a mail server responsible for accepting email messages on behalf of a recipient’s domain, and a preference value used to prioritize mail delivery if multiple mail servers are available. The set of MX records of a domain name specifies how email should be routed with the Simple Mail Transfer Protocol (SMTP).

A Record

An A (address) record is a DNS record that can be used to point your domain name and host names to a static IP address.

NOT A B C

Need to increase the cost associated with the MX record of Server2 so that Server1 is preferred over Server2 but Server2 will be used if Server1 is not available.

C

Need to increase the cost associated with the MX record of Server2 so that Server1 is preferred over Server2 but Server2 will be used if Server1 is not available.

There is already a CNAME (Alias) associated with mail.contoso.com which points to Server1.contoso.com.

D. Run Set-DistributionGroup Group2 -ModeratedBy Admin1 -BypassModerationFromSendersOrMembers Group1 -ModerationEnabled $true.

Question 112

Which two actions should you perform?

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 -ModeratedBy 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 Group2. Configure the transport rule to have an action of Forward the message for approval to Admin1.

Correct Answer: BC

Explanation/Reference:

Transport Rules

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.

Moderated Transport

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
encrypt communications between the Client Access server and the Mailbox server. The Client Access server trusts the self-signed certificate on the Mailbox server that created it. The subject and the name of the certificate match. The issuer and the subject are defined on the certificate. This self-signed certificate is used to

When you install Exchange 2013, a self-signed certificate is automatically configured on the Mailbox servers. A self-signed certificate is signed by the application

Self-signed Certificate

IMPORT THE SSL CERTIFICATE AND THEN ASSIGN IT TO OUTLOOK 2013

D LOOKS LIKE A BETTER RESPONSE.

UNABLE TO ASSOCIATE SET-CLIENTACCESSSERVER WITH CERTIFICATE ERROR

Explanation:

Explanation/Reference:

Correct Answer: A

Which cmdlet should you run?

You need to prevent the certificate warning message from occurring when the users open Outlook 2013.

The users do not receive a certificate error message or a certificate warning message when they open Outlook Web App.

The users report that when they open Outlook 2013, they receive a certificate warning message.

Correct Answer: A

Which cmdlet should you run?

You need to recover deleted items in a mailbox database for a user named User1.

C. New-ClientAccessArray
B. New-ExchangeCertificate
A. Set-ClientAccessServer

Which cmdlet should you run?

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

A. Run the New-MailboxRestoreRequest cmdlet.
B. Run the New-MailboxDatabase cmdlet and specify the Recovery parameter.
C. Restore DB1 from the tape backup to an alternate location.
D. Restore DB1 from the tape backup to the database’s original location.
E. Run the New-Mailbox cmdlet and specify the Recovery parameter.

Correct Answer: ABC

Explanation/Reference:

Explanation:

Recovery Database

A recovery database is a special kind of mailbox database that allows you to mount a restored mailbox database and extract data from the restored database as part of a recovery operation. You can use the New-MailboxRestoreRequest cmdlet to extract data from a recovery database. After extraction, the data can be exported to a folder or merged into an existing mailbox. Recovery databases enable you to recover data from a backup or copy of a database without disturbing user access to current data.

A

New-MailboxRestoreRequest cmdlet

Use the New-MailboxRestoreRequest cmdlet to restore a soft-deleted or disconnected mailbox. This cmdlet starts the process of moving content from the soft-deleted mailbox, disabled mailbox, or any mailbox in a recovery database into a connected primary or archive mailbox.

For information about the parameter sets in the Syntax section below, see Syntax.

EXAMPLE 1

To create a restore request, you must provide the DisplayName, LegacyDN, or MailboxGUID for the soft-deleted or disabled mailbox. This example uses the Get-MailboxStatistics cmdlet to return the DisplayName, LegacyDN, MailboxGUID, and DisconnectReason for all mailboxes on mailbox database MBDO1 that have a disconnect reason of SoftDeleted or Disabled.

Get-MailboxStatistics -Database MBDO1 | Where { $_.DisconnectReason -eq "SoftDeleted" -or $_.DisconnectReason -eq "Disabled" } | Format-List LegacyDN, DisplayName, MailboxGUID, DisconnectReason

This example restores the source mailbox with the MailboxGUID 1d20855f-d645-4d01-86e6-c24f9326ddd on mailbox database MBDO1 to the target mailbox with the alias Ayla.

New-MailboxRestoreRequest -SourceDatabase "MBDO1" -SourceStoreMailbox 1d20855f-d645-4d01-86e6-c24f9326ddd -TargetMailbox Ayla

B

Use the New-MailboxDatabase cmdlet to create a new mailbox database object in the database container in Active Directory.

For information about the parameter sets in the Syntax section below, see Syntax.

EXAMPLE 1

This example creates the mailbox database MailboxDatabase01. This example also specifies where to create the .edb database file, which is different than the default location.

New-MailboxDatabase -Name "MailboxDatabase01" -EdbFilePath C:\DatabaseFiles\MailboxDatabase01.edb

The Recovery parameter specifies that the new database is designated as a recovery database.

NOT D

Need to recover data from a backup or copy of a database without disturbing user access to current data.

Therefore restore to an alternate location.

NOT E

No recovery parameter exists for the New-Mailbox cmdlet.

Reference: Create a Recovery Database

Reference: Restore Data Using a Recovery Database

Correct Answer: ABC

Explanation:

Explanation:

UNABLE TO ASSOCIATE SET-CLIENTACCESSSERVER WITH CERTIFICATE ERROR

D LOOKS LIKE A BETTER RESPONSE.

IMPORT THE SSL CERTIFICATE AND THEN ASSIGN IT TO OUTLOOK 2013

Self-signed Certificate

When you install Exchange 2013, a self-signed certificate is automatically configured on the Mailbox servers. A self-signed certificate is signed by the application that created it. The subject and the name of the certificate match. The issuer and the subject are defined on the certificate. This self-signed certificate is used to encrypt communications between the Client Access server and the Mailbox server. The Client Access server trusts the self-signed certificate on the Mailbox server.
automatically, so no third-party certificate is needed on the Mailbox server. When you install Exchange 2013, a self-signed certificate is also created on the Client Access server. This self-signed certificate will allow some client protocols to use SSL for their communications. Exchange ActiveSync and Outlook Web App can establish an SSL connection by using a self-signed certificate.

Outlook Anywhere won’t work with a self-signed certificate on the Client Access server. Self-signed certificates must be manually copied to the trusted root certificate store on the client computer or mobile device. When a client connects to a server over SSL and the server presents a self-signed certificate, the client will be prompted to verify that the certificate was issued by a trusted authority. The client must explicitly trust the issuing authority. If the client confirms the trust, then SSL communications can continue.

Note:
By default, the digital certificate installed on the Mailbox server or servers is a self-signed certificate. You don’t need to replace the self-signed certificate on the Mailbox servers in your organization with a trusted third-party certificate. The Client Access server automatically trusts the self-signed certificate on the Mailbox server and no other configuration is needed for certificates on the Mailbox server.

Outlook 2013
When connecting to an Exchange server using Outlook 2013 you may encounter an SSL trust error.

This error occurs when the Exchange server is configured with a self-signed SSL certificate. Outlook makes connections to the Exchange server over HTTPS and therefore must trust the SSL certificate that is configured on the server, otherwise it will display those error messages to the end user.

To resolve the issue install a valid SSL certificate on the Exchange server from a trusted certificate authority.

See Exchange Server 2013 SSL certificates for more details on this as well as step by step instructions.

Set-ClientAccessServer
Use the Set-ClientAccessServer cmdlet to set properties on specified Client Access server objects.

For information about the parameter sets in the Syntax section below, see Syntax.

This example sets two properties on the Client Access server CAS-01.

Example:

This example sets two properties on the Client Access server CASMail.

Example:

Listing:
NOTE B
New-ExchangeCertificate
Not an Exchange 2013 command or any other Exchange version command

NOTE C
Exchange 2010 command
Use the New-CertificateExchange cmdlet to create an object that represents a load balanced array of Client Access servers within a single Active Directory site.

Example 1
This example creates the Client Access server array server.contoso.com.

New-CertificateExchange -Fqdn server.contoso.com -Site “Redmond” -Name “server.contoso.com”

Example 2
This example imports an existing certificate and private key from the PKCS #12 file ExportedCert.pfx.

Import-ExchangeCertificate -FileData ([Byte][73]$(Get-Content -Path c:certificatesExportedCert.pfx -Encoding byte -ReadCount 0)) -Password:(Get-Credential).password

Question 115
Which two cmdlets should you run?

Your network contains an Active Directory forest. The forest contains two sites named Montreal and New York. You have an Exchange Server 2013 organization that contains a Mailbox server and a Client Access server in each site. The users in the New York site report that the offline address book (OAB) is not updated after an extended WAN outage between the sites. The Montreal site contains the OAB generation server.

You need to ensure that the New York site users download the OAB from a server in the New York site.

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

A. Set-Mailbox
B. New-OfflineAddressBook
C. New-Mailbox
D. New-OabVirtualDirectory
E. Set-OfflineAddressBook

Correct Answer: AC

Explanation/Reference:
Creating a new Organization Mailbox is a two step process:

Step 1: Create a new arbitration mailbox
New-Mailbox -Arbitration -Name “OAB Seattle” -Database DB2Seattle -UserPrincipalName [email protected] -DisplayName “OAB Mailbox for Seattle”

Step 2: Enable OABGen capability
Set-Mailbox -Arbitration oabs -OABGen $true


Question 116
What should you do?

Your network contains an Active Directory forest. The forest contains one domain. The domain contains two sites and three domain controllers. The sites and domain controllers are configured as shown in the following table.

<table>
<thead>
<tr>
<th>Site</th>
<th>Domain Controllers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Montreal</td>
<td>DC1, DC2</td>
</tr>
<tr>
<td>New York</td>
<td>DC1, DC2, DC3</td>
</tr>
</tbody>
</table>

The sites connect to each other by using a WAN link.

You have an Exchange Server 2013 organization that contains two servers in the Main Office site.

In Branch1, you plan to deploy one server to the Exchange Server 2013 organization.

You need to ensure that all of the Exchange Server services in Branch1 are available if the WAN link fails after the planned deployment.

What should you do?

A. Create a site link bridge, and then configure Branch1 as a hub site.
B. Replace the domain controller in Branch1 with an RODC that runs Windows Server 2012.
C. Replace the domain controller in Branch1 with a writable domain controller that runs a Server Core installation of Windows Server 2008.
D. Create an additional site link, and then configure Branch1 as a hub site.

Correct Answer: C

Explanation/Reference:

A site link bridge connects two or more site links and enables transitivity between site links. Each site link in a bridge must have a site in common with another site link in the bridge. The Knowledge Consistency Checker (KCC) uses the information on each site link to compute the cost of replication between sites in one site link and sites in the other site links of the bridge. Without the presence of a common site between site links, the KCC also cannot establish direct connections between domain controllers in the sites that are connected by the same site link bridge.

By default, all site links are transitive.

This figure illustrates an organization’s hub-and-spoke network topology, consisting of two hub sites (A and B) and six satellite sites (C through H). The site links between all sites are named A-B, A-C, A-D, A-E, B-F, B-G, and B-H.

Hub Site
A hub site is based on having large numbers of outgoing links.
NOT A B D

If you want to install or operate any Exchange 2013 server in a site, you must have a writable global catalog in the same AD site.

Be aware that no versions of Exchange Server will make use of RODC or the Global Catalog server on a RODC although Exchange will work in the presence of RODC as long as writable versions of domain controllers and GCs are available.

C

If you want to install or operate any Exchange 2013 server in a site, you must have a writable global catalog in the same AD site.

The Global Catalog is the central repository of information about objects in a tree or forest but with a limited number of each objects attribute.

The domain controller that holds a copy of the Global Catalog is the Global Catalog Server.

The global catalog server makes it possible to search the entire AD DS forest without referrals to the domain controller that store the target of the search.

The global catalog server is also required for searching and processing domain logons in forests where universal groups is available. Be aware that no versions of Exchange Server will make use of RODC or the Global Catalog server on a RODC although Exchange will work in the presence of RODC as long as writable versions of domain controllers and GCs are available.

Question 117

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.)

Select and Place:

Correct Answer:

Explanation/Reference:

Autodiscover

Autodiscover is a service which is run on Exchange Client Access Servers. It is one of the new features it includes in Exchange 2007+

The Autodiscover service is used 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 118

Which cmdlet should you run?

You have an Exchange Server 2013 organization that contains two Client Access servers named SERVER1 and SERVER2 and two Mailbox servers named SERVER3 and SERVER4.

You have a firewall that controls all of the traffic between the internal network and the Internet.

SERVER3 and SERVER4 are prevented from communicating with Internet hosts.

SERVER1 and SERVER3 are in a site named Main. SERVER2 and SERVER4 are in a site named Main_2.
All outbound email is sent through SERVER1.
Main fails.
You discover that email messages for the Internet are queued on SERVER4.
You discover that all of the outbound email is queued on SERVER4 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-TransportService
C. Set-ExchangeServer
D. Set-ADSite
Correct Answer: A
Explanation/Reference:
Mailbox Server
In an Exchange Server 2013 organization the Mailbox server role is responsible for sending outbound email via a Send Connector.
When this option is enabled outbound email that is being sent via a Send Connector does not go directly out from the Mailbox server, and instead is proxied through a Client Access server in the site.
There is nothing complicated going on here, the Client Access server simply acts as a proxy for the connection so that the receiving host out on the internet sees the connection as coming from the Client Access server name and IP address rather than the Mailbox server.
IN THIS QUESTION THE CLIENT ACCESS SERVER (SERVER1) IS ACTING AS A PROXY SERVER FOR THE MAILBOX SERVERS.
NEED TO CHANGE THE SEND CONNECTOR SETTINGS IN ORDER FOR MAIL TO FLOW OUT FROM SERVER4 TO THE INTERNET.
A
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
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.
E
Set-TransportService
Use the Set-TransportService cmdlet to set the transport configuration options for the Transport service on Mailbox servers or for Edge Transport servers.
This example sets the TransientFailureRetryCount parameter to 3 and sets the TransientFailureRetryInterval parameter to 30 seconds for the Transport service on a Mailbox server named Mailbox01.
Set-TransportService Mailbox01 -TransientFailureRetryCount 3 -TransientFailureRetryInterval 00:00:30
NOT C
Will not resolve the issue
Set-ExchangeServer
Use the Set-ExchangeServer cmdlet to set Exchange attributes in Active Directory for a specified server.
For information about the parameter sets in the Syntax section below, see Syntax.
EXAMPLE 1
This example disables error reporting on the specified server.
Set-ExchangeServer -Identity TestServer.CONTOSO.COM -ErrorReportingEnabled: $false
NOT D
Will not resolve the issue
Set-ADSite
Use the Set-ADSite cmdlet to configure the Exchange settings of Active Directory sites.
EXAMPLE 1
This example configures the Active Directory site named Default-First-Site-Name as a hub site.
Set-ADSite Default-First-Site-Name -HubSiteEnabled $true

Question 119
Which cmdlet should you use in a scheduled task?
You have an Exchange Server 2013 organization named adatum.com. The organization contains five Mailbox servers and two Client Access servers.
You need to ensure that an administrator named user1 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-Mailbox
C. New-AdminAuditLogSearch
D. Set-ExchangeServer
E. Set-AdminAuditLogConfig
Correct Answer: C
Explanation/Reference:
Use Search-AdminAuditLog for searching through the audit logs.
Search-AdminAuditLog
Use the Search-AdminAuditLog cmdlet to search the contents of the administrator audit log.

For information about the parameter sets in the Syntax section below, see Syntax.

EXAMPLE 1
This example finds all the administrator audit log entries that contain either the New-RoleGroup or the New-ManagementRoleAssignment cmdlet.

Search-AdminAuditLog -Cmdlets New-RoleGroup, New-ManagementRoleAssignment

NOT B
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.

EXAMPLE 1
This example delivers John Woods's email messages to John's mailbox and also forwards them to Manuel Oliveira's ([email protected]) mailbox.

Set-Mailbox -Identity John -DeliverToMailboxAndForward True -ForwardingSMTPAddress [email protected]

NOT D
Set-ExchangeServer
Use the Set-ExchangeServer cmdlet to set Exchange attributes in Active Directory for a specified server.

For information about the parameter sets in the Syntax section below, see Syntax.

EXAMPLE 1
This example disables error reporting on the specified server.

Set-ExchangeServer -Identity TestServer-Contoso.com -ErrorReportingEnabled: $false

NOT E
NOT Set-AdminAuditLogConfig
Use the Set-AdminAuditLogConfig cmdlet to configure the administrator audit logging configuration settings.

EXAMPLE 1
This example enables administrator audit logging for every cmdlet and every parameter in the organization, with the exception of Get- cmdlets.

Set-AdminAuditLogConfig -AdminAuditLogEnabled: $true -AdminAuditLogCmdlets: * -AdminAuditLogParameters: *

C
New-AdminAuditLogSearch
Use the New-AdminAuditLogSearch cmdlet to search the contents of the administrator audit log and send the results to one or more mailboxes that you specify.

For information about the parameter sets in the Syntax section below, see Syntax.

EXAMPLE 1
This example finds all the administrator audit log entries that match the following criteria and sends the results to [mailto:[email protected]](mailto:[email protected]) and [mailto:[email protected]](mailto:[email protected]) SMTP addresses:

`Cmdlets Set-Mailbox Parameters UseDatabaseQuotaDefaults, ProhibitSendReceiveQuota, ProhibitSendQuota StartDate 01/24/2012 EndDate 02/12/2012`

New-AdminAuditLogSearch -Name "Mailbox Quota Change Audit" -Cmdlets Set-Mailbox -Parameters UseDatabaseQuotaDefaults, ProhibitSendReceiveQuota, ProhibitSendQuota -StartDate 01/24/2012 -EndDate 02/12/2012 -StatustMailRecipients: [mailto:[email protected]](mailto:[email protected]), [mailto:[email protected]](mailto:[email protected])`

New-AdminAuditLogSearch: Exchange 2013 Help

Question 120
Which two actions should you perform?

You have an Exchange Server 2013 organization.

You plan to deploy Exchange ActiveSync for mobile devices. Each mobile device will be authenticated by using certificates issued by an internal certification authority (CA).

You need to configure the organization to authenticate the mobile devices by using the certificates.

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

A. From Internet Information Services (IIS) Manager on each Client Access server, configure the Microsoft-Server-ActiveSync virtual directory to require client certificates.
B. From Exchange Admin Center, configure the Microsoft-Server-ActiveSync virtual directory to require client certificates.
C. From Internet Information Services (IIS) Manager on each Mailbox server, enable Active Directory Client Certificate Authentication.
D. From Internet Information Services (IIS) Manager on each Mailbox server, enable Active Directory Client Certificate Authentication.

Correct Answer: BC

Explanation/Reference:
Explanation:
NOT A
Enable Active Directory Client Certificate Authentication within IIS but configure the Microsoft-Server-ActiveSync virtual directory to require client certificates is performed in Exchange Admin Center.

NOT D
IIS is configured on the Client Access Server not the Mailbox Server

B
After you've installed the Exchange 2013 Client Access server, there are a variety of configuration tasks that you can perform.

Although the Client Access server in Exchange 2013 doesn't handle processing for the client protocols, several settings need to be applied to the Client Access server, including virtual directory settings and certificate settings.


Exchange Server 2013 automatically configures multiple Internet Information Services (IIS) virtual directories during installation.

This topic contains information about the default IIS authentication settings and default Secure Sockets Layer (SSL) settings for the Client Access and Mailbox servers.

The following table lists the default settings on a stand-alone Exchange 2013 Client Access server.

<table>
<thead>
<tr>
<th>Default Client Access server IIS authentication and SSL settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual directory Authentication method SSL settings</td>
</tr>
<tr>
<td>Management method</td>
</tr>
<tr>
<td>Microsoft-Server-ActiveSync Basic authentication SSL required</td>
</tr>
<tr>
<td>Requires Requires 128-bit encryption EAC or Shell</td>
</tr>
</tbody>
</table>

C
Configure certificate-based authentication for Exchange ActiveSync


Client Access Server Configuration
To configure the Client Access server to enforce certificate based authentication:
1. Verify if Certificate Mapping Authentication is installed on the server.
2. Right-click on Computer in the start menu and choose Manage.
3. Expand Roles and click on Web Server (IIS)
Scroll down to the Role Services section. Under the Security section you should see Client Certificate Mapping Authentication installed.

If you don’t see Client Certificate Mapping Authentication installed, click add Role Services > (scroll) Security and select Client Certificate Mapping Authentication and then click Install.

Reboot your server.

Question 121
In which order should you perform the actions?

Your network contains four servers. The servers are configured as shown in the following table.

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.

Select and Place:

Correct Answer:

Explanation/Reference:

CONSENSUS OF AGREEMENT WITH THE ORDER OF:
Run the New-ManagementRole -Parent MyContactInformation -Name Role1
Run the Remove-ManagementRoleEntry Role1 Set-User command
Run the Add-ManagementRoleEntry Role1Set-User-Parameters Office, Homephone
Run the New-RoleAssignmentPolicy -Name Policy1-Roles MyBaseOptions, Role1, MyVoiceMail, MyTextMessages, MyTeamMailboxes, MyMarketPlaceApps, MyDistributionGroupMembership
Run the New-Mailbox cmdlet

First or last place

Question 122
Which three actions should you recommend performing on EX6 in sequence?

Your network contains an internal network and a perimeter network.
Your 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.)

Select and Place:

Correct Answer:

Explanation/Reference:

(step 1) You must install the Mailbox role and onto that role you install the Anti-spam Agents.
(step 2) Run the following command to install the Anti-Spam Agents
& $env:ExchangeInstallPath\Scripts\Install-All-AntiSpamAgents.ps1
(step 3) Run the Restart-Send-MSExchange Transport service command
Need to run this command
Once the Install-AntiSpamAgents.ps1 script has run, if the anti-spam agents were successfully installed then exchange will ask you to restart the Microsoft Exchange Transport service.
Use the Restart-Service MSExchange Transport command to do this.

Question 123
Which command should you run?

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

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

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.
Implicit scopes are defined on management roles. Implicit scopes apply to both built-in management roles and also to custom management roles.

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 regular scope 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.

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 management roles, specified as a predefined relative scope on a management role assignment, or created using custom filters and added to a management role assignment.

To view the properties of a database, you must run a Set-MailboxDatabase cmdlet and specify a management role scope.

When you apply a scope, the role assignee assigned to the role can only modify the objects contained within that scope. 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.

The database is replicated to database copies in multiple Active Directory sites. Set-MailboxDatabaseCopy -Identity DB1MBX2 -ActivationPreference 3

The 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 DB2MBX1 -ReplayLagTime 3.00:0:0

This example configures an activation preference of 3 for the copy of the database DB1 hosted on the Mailbox server MBX2.

Set-MailboxDatabaseCopy -Identity DB1MBX2 -ActivationPreference 3

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

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

SECTION 1
Explanation/Reference:
Explanation:
SECTION 1
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 DB2MBX1 -ReplayLagTime 3.00:0:0

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 DB1MBX2 -ActivationPreference 3

NOT Set-MailboxDatabaseAvailabilityGroup
Use the Set-MailboxDatabaseAvailabilityGroup cmdlet to configure some of the properties of a database availability group (DAG). The Set-MailboxDatabaseAvailabilityGroup 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 activated co-partition (DAC) mode.

SECTION 2
Need to identify the name of the mailbox database. (DB1)

SECTION 3
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.

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 to eliminate SecondCopy. Unsure of why – AllDatacenters is the final choice but there are 3 Active Directory sites in this scenario.

Set-MailboxDatabase: Exchange 2013 Help

Question 124
Which RBAC scopes should you identify?
DRAG DROP
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.)

Select and Place:

Correct Answer:

Explanation/Reference:
Explanation:
Understanding Management Role Scopes: Exchange 2013 Help

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 assignment 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 objects 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. The 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 explicit scopes 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.

TheRecipientFilter 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.

**Question 125**

Which two new policies should you create?

You have an Exchange Server 2013 organization that contains a server named EX1.

Your network contains a non-critical internal application that regularly connects to the POP3 Service on EX1.

Users report that Outlook Web App performs more slowly than usual.

You discover that EX1 frequently has a CPU utilization that is greater than 85 percent.

You need to configure EX1 temporarily to allocate more processor resources to Outlook Web App and to allocate less processor resources to POP3.

Which two new policies should you create? (Each correct answer presents part of the solution. Choose two.)

A. a throttling policy that sets OFWAMaxConcurrency to 25
B. a workload policy for POP3 that sets the WorkloadClassification to Discretionary
C. a workload policy for Outlook Web App that sets the WorkloadClassification to Discretionary
D. a throttling policy that sets POP3MaxConcurrency to 25
E. a workload policy for POP3 that sets the WorkloadClassification to CustomerExpectation
F. a workload policy for Outlook Web App that sets the WorkloadClassification to CustomerExpectation

Correct Answer: A, F

Explanation: Description:

A workload policy 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.

Workload classifications

Each Exchange workload (for example, the Calendar Synchronization Assistant workload), is assigned a classification.

Workload policy settings are used to group each workload into a class. Classification is used to control both priority and target resource usage.

Exchange workloads can be assigned one of the following classifications:

- Urgent
- Customer Expectation
- Internal Maintenance
- Discretionary

Workloads in a higher classification group are given preference as resource health shows signs of degrading. For example, when a resource such as local server CPU reaches high usage, workloads classified as Internal Maintenance may continue to run, while workloads classified as Discretionary may be stopped.

A throttling policy is related to Exchange 2010. Do not need to allocate less priority to Outlook Web App, but more POP3 is allocated too much resources with a WorkloadClassification of CustomerExpectation.

Need to allocate less priority to POP3. Outlook Web App is allocated the appropriate amount of resources with a WorkloadClassification of CustomerExpectation. New-WorkloadPolicy: Exchange 2013 Help.

**Question 126**

Which management roles should you identify?

**HOTSPOT**

Your company has an Exchange Server 2013 organization. The company hires 200 temporary employees. You create a mailbox for each temporary employee. You create a new management role named CustomBaseOptions that uses MyBaseOptions as a parent. You create a new management role named CustomContactInfo that uses MyContactInfo as a parent. You plan to apply the new management roles to the temporary employees. You need to identify which management roles must be modified to prevent the temporary employees from performing the following task:

- Adding a user photo
- Viewing delivery reports
- Viewing the Install Apps feature
- Changing the value of the office location

Which management roles should you identify?

To answer, select the appropriate management role for each task in the answer area.

**Hot Area:**

*Correct Answer:*

**Explanation/Reference:**

*Explanation:* View and modify the basic configuration of their own mailbox and associated settings.

**VIEWING DELIVERY REPORTS**

MyBaseOptions includes the following delivery reports information:

- Delivery Success
- Delivery Failure

**Email submission from the senders mailbox**

**Message was read etc...**

**VIEWING THE INSTALL APPS FEATURE**

MyBaseOptions View and modify the basic configuration of their own mailbox and associated settings.

**CHANGING THE VALUE OF THE OFFICE LOCATION**

The MyContactInformation management role enables individual users to modify their contact information, including address and phone numbers.


**Question 127**

Which design should you identify?

**HOTSPOT**

Your company has two offices. The offices are configured as shown in the following table.

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.

**Hot Area:**

*Correct Answer:*

**Explanation/Reference:**

*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.
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.

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 logged 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 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 be 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.

PICTURE2

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.

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

1 DAG 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 128
Which three commands should you run from Server1?

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.

Select and Place:

- Correct Answer:

Correct Answer:

Explanation/Reference:

Note:
- Before you install Microsoft Exchange Server 2013 on any servers in your organization, you must prepare Active Directory and domains.
- Prepare Active Directory and domains
1. From a Command Prompt window, run the following command.
   setup /PrepareSchema
   setup /ps
2. From a Command Prompt window, run the following command.
   setup /PrepareAD /OrganizationName: <organization name>
   setup /p /on: <organization name>
3. From a Command Prompt window, run one of the following commands:
   . Run setup /PrepareDomain or setup /pd to prepare the local domain. You don’t need to run this in the domain where you ran Step 2. Running setup /PrepareAD prepares the local domain.
   . Run setup /PrepareDomain: <FQDN of domain you want to prepare> to prepare a specific domain.
   . Run setup /PrepareAllDomains or setup /pad to prepare all domains in your organization.

Reference:
Exchange 2013 Prerequisites: Exchange 2013 Help
Exchange 2013, Prepare Active Directory and Domains

Question 129
Which cmdlet should you use in a scheduled task?

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

Correct Answer: C

Explanation/Reference:

New-AdminAuditLogSearch: Exchange 2013 Help

Question 130
What should you do?

You have an Exchange Server 2013 organization named for Contoso. A user named Admin1 is a member of the Domain Admins group. Admin1 fails to synchronize a new Windows Phone device by using Exchange ActiveSync and receives an HTTP 500 error message. Admin1 successfully logs on to Outlook Web App and Outlook Anywhere. You need to ensure that Admin1 can synchronize the new Windows Phone device by using Exchange ActiveSync.

What should you do?
A. Install a trusted root certificate on the Windows Phone device.
B. Create a new mobile device mailbox policy.
C. Enable permission inheritance on the Admin1 user account.
D. Disable permission inheritance on the Admin1 user account.

Correct Answer: C

Explanation/Reference:

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.

NOT A
It is possible to save a digital certificate to a file and install a digital certificate on a Windows Mobile phone. Microsoft Exchange ActiveSync enables a variety of mobile phones to synchronize with an Exchange mailbox.

A digital certificate might need to be installed on a user’s mobile phone if Exchange ActiveSync is required to use Secure Sockets Layer (SSL) and your organization uses a certificate that isn’t from a trusted commercial certification authority (CA).

No mention of SSL in this question

NOT B
This is a permission inheritance issue.

NOT D
Need to enable permission inheritance not disable it or leave it as disabled.

C
Question 131
What should you recommend doing first?
You plan to deploy an Exchange Server 2013 organization.
You need to recommend a solution to ensure that a user named User1 can access email messages by using Exchange ActiveSync on an Android device.
The solution must prevent all other users from using Android devices to access email by using Exchange ActiveSync.
What should you recommend doing first?
A. Run the Set-CasMailbox cmdlet.
B. Create a device access rule.
C. Modify the Quarantine Notification settings.
D. Create a mobile device mailbox policy.
Correct Answer: B
Explanation/Reference:
Explanation:
Access the Allow/Block/Quarantine rules
NOT A
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.
Need to create a rule to allow a particular user to use Exchange ActiveSync on an Android device.
NOT C
Can allow or block access for all users.
Quarantine all users and then selectively allow the users access.
A new device rule is a better way of managing the problem.

Question 132
What should you do?
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-Mailbox 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-CasMailbox cmdlet.
D. Create a new device access rule, and then run the Set-CasMailbox cmdlet.
Correct Answer: A
Explanation/Reference:
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 B C
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 133
What should you configure for each requirement?
DRAG DROP
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:
1. Messages sent to adatum.com must NOT include the disclaimer.
2. 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. Select and Place:

Correct Answer:

Explanation/Reference:
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

Technical Overview of Policy Tips in Exchange Online and Exchange 2013

Question 134
Which three actions should you perform next?
DRAG DROP
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.
Select and Place:

Correct Answer:

Explanation/Reference:
Note: Use Setup /m:RecoverServer to recover a server
1. Retrieve any replay log or truncation log settings for any mailbox database copies that exist on the server being recovered by using the Get-MailboxDatabase cmdlet.
2. (Box 1) Remove any mailbox database copies that exist on the server being recovered by using the Remove-MailboxDatabaseCopy cmdlet.
3. (Box 1) Remove the failed server’s configuration from the DAG by using the Remove-DatabaseAvailabilityGroupServer cmdlet.
4. Reset the server’s computer account in Active Directory. For detailed steps, see Reset a Computer Account.
5. (Box 2) Open a Command Prompt window. Using the original Setup media, run the following command:
Setup /m:RecoverServer
6. (Box 3) When the Setup recovery process is complete, add the recovered server to the DAG by using the Add-DatabaseAvailabilityGroupServer cmdlet.
7. (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 setup 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

Recorver a Database Availability Group Member Server: Exchange 2013 Help

Question 135
Which cmdlets should you use?
DRAG DROP
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 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.
Several employees must be able to open only the Inbox of a user named User1.

You need to configure access to Outlook to meet the following requirements:
Several employees plan to use Microsoft Outlook to collaborate on some projects.
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 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.
Several employees must be able to open only the Inbox of a user named User1.

Which cmdlets should you use?
To answer, move the three appropriate actions from the list of actions to the answer area and arrange them in the correct order.
Select and Place:

Correct Answer:

Explanation/Reference:
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 [email protected]:Marketing -User [email protected] -AccessRights Owner
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).

Public folders can 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, users can access the public folder to retrieve archived messages. 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.

Question 136

Which actions should you perform?

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 users in the Singapore office connect to their local server to retrieve the public folder hierarchy.
- Ensure that the public folders are available if a single Mailbox server fails.

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.

Correct Answer: ACD

Explanation/Reference:

Explanation:

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

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 help organize content in a deep hierarchy that’s easy to manage. 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 automatically calculates the per-user hierarchy mailbox.

NOT E


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 automatically 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 hierarchy.

A

Need to create a public folder mailbox in the Singapore office.

C

Use the Add-MailboxDatabaseCopy cmdlet to create a passive copy of an existing active mailbox database.

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 137

Which three actions should you perform?

DRAG DROP

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

 answered
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. Select and Place:

Correct Answer:

Explanation/Reference:

* 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.
* You can specify a name for the DAG and the witness server that you want to use, and leave the Witness directory field empty. In this scenario, the task will create the default witness directory on the specified server.
* If the witness server you specify isn't an Exchange 2013 or Exchange 2010 server, you must add the Exchange Trusted Subsystem universal security group to the local Administrators group on the witness server. These security permissions are necessary to ensure that Exchange can create a directory and share on the witness server as needed.


Question 138
What should you do?
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.

Correct Answer: B

Explanation/Reference:

* 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

Question 139
Which two actions should you perform?
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.

Correct Answer: AD

Explanation/Reference:

* 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.

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
B
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 140**
Which three cmdlets should you run?
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 [email protected]
- Email messages sent from the Internet to a distribution list named Executives must be rejected.
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 [email protected]
- Email messages sent from the Internet to a distribution list named Executives must be rejected.

**Correct Answer:** ABE
Explanation/Reference:
A. Add ContentFilterPhrase
B. Set-ContentFilterConfig
C. Set-TransportConfig
D. Set-SenderReputationConfig
E. Set-RecipientFilterConfig

**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

**EXAMPLE 2**
This example modifies the Recipient Filter agent configuration so that recipient validation is enabled.
Set-RecipientFilterConfig -RecipientValidationEnabled $true

**Syntax**

**Set-ContentFilterConfig**
Use the Set-ContentFilterConfig cmdlet to modify the content filter configuration on a Mailbox server or an Edge Transport server.

**Set-RecipientFilterConfig**
Use the Set-RecipientFilterConfig cmdlet to modify the recipient filter configuration on a Mailbox server.

**Set-TransportConfig**
Use the Set-TransportConfig cmdlet to modify the transport configuration for the whole Exchange organization.

**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 16 hours.

Set-SenderReputationConfig -SenderBlockingEnabled $true -SrlBlockThreshold 6 -SenderBlockingPeriod 36

Add-ContentFilterPhrase: Exchange 2013 Help
Set-ContentFilterConfig: Exchange 2013 Help
Set-RecipientFilterConfig: Exchange 2013 Help

Question 141
Which action or actions should you recommend performing?
You need to recommend a solution to resolve the load balancing issue.
Which action or actions should you recommend performing? (Each correct answer presents part of the solution. Choose all that apply.)
A. From Exchange Management Shell, import a certificate and assign the certificate to the IIS service.
B. From the settings of the hardware load balancer, enable cookie-based persistence.
C. From Exchange Admin Center, configure the Exchange Server 2013 virtual directories.
D. From DNS Manager, create new DNS records in the public DNS zone.
E. From the settings of the hardware load balancer, disable the source NAT (SNAT).
F. From EX3, generate a new certificate.

Correct Answer: ACD
Explanation/Reference:

NOT B: The hardware load balancer is a Layer 4 device which supports IP-Address affinity, not cookie-based persistence which is a Layer 7 feature.

NOT E: Source NAT (SNAT) is a Layer 7 feature.

NOT F: A self-signed certificate will not suffice in this instance.

Question 142
Which commands should you run?
HOTSPOT
You create a workload management policy named EX4.
You need to create a new workload policy to resolve the hardware resources issue on EX4.
Which commands should you run? (To answer, select the appropriate options in the answer area.)

Hot Area:

Correct Answer: New-WorkloadPolicy
Explanation/Reference:
Explanation:
New-WorkloadPolicy
Workload Management Reference
Change Workload Management Policy Settings for a Specific Server
Change Workload Management Policy Settings for All Servers in Your Organization

Question 143
What should you do?
You need to ensure that users can create new public folders when EX4 is unavailable.
What should you do?
A. Run the New-PublicFolderMoveRequest cmdlet.
B. Add EX4 to DAG1.
C. Create a new public folder database.
D. Run the New-MoveRequest cmdlet.

Correct Answer: B
Explanation/Reference:
The Public Folder hierarchy is homed on DB3. DB3 is mounted on EX4.
Currently EX4 is not part of a DAG.
Exchange 2013 public folders are built on mailbox infrastructure and use the same mechanisms for availability and redundancy. Every public folder mailbox can have multiple redundant copies with automatic failover, just like regular mailboxes.

Question 144
What authentication and permission group should you configure for the Receive Connector?
HOTSPOT
You need to ensure that the help desk application can use EX4 as an SMTP relay to send email messages. The solution must ensure that the sender of the email messages is displayed as Help Desk.
What authentication and permission group should you configure for the Receive Connector? (To answer, configure the appropriate options in the answer area.)

Hot Area:
Question 145
Which actions should you recommend performing in each forest?

DRAG DROP
You are evaluating the implementation of the address rewrite feature in the Fabrikam forest.
You need to recommend a solution for the Trey Research forest and the Fabrikam forest to share the SMTP domain name of treyresearch.com. Which actions should you recommend performing in each forest? (To answer, drag the appropriate actions to the correct forests. Each action 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)

Select and Place:

Correct Answer:

Explanation/Reference:
Receive Connector Authentication Mechanisms: Exchange 2013 Help

Question 146
Which cmdlet should you include in the recommendation? You need to recommend a solution to resolve the issue of domain controller overuse. Which cmdlet should you include in the recommendation?
A. Set-ExchangeServer
B. Set-OrganizationConfig
C. Set-ADServerSettings
D. Set-AuthConfig

Correct Answer: A
Explanation/Reference:

Hard code specific DC’s for a particular Exchange server:
Set-ExchangeServer -identity Exch01 -DomainController dc01.domain.com -StaticDomainControllers 'dc01.domain.com', 'dc02.domain.com'- StaticGlobalCatalogs 'dc01.domain.com', 'dc02.domain.com'- StaticConfigDomainController 'dc01.domain.com', 'dc02.domain.com' Remove the configuration above:
Set-ExchangeServer -identity Exch01 -staticDomainControllers $NULL -staticGlobalCatalogs $NULL -staticConfigDomainController $NULL

Question 147
Which value should you set for each SCL option? You need to implement the SCL configurations to support the planned changes. Which value should you set for each SCL option? (To answer, configure the appropriate options in the dialog box in the answer area.)

Hot Area:

Correct Answer:

Explanation/Reference:
Spam Confidence Level Threshold: Exchange 2013 Help

Question 148
Which command should you include in the recommendation? You need to recommend a solution to resolve the issue for the finance department users. Which command should you include in the recommendation? (To answer, select the appropriate options in the answer area.)

Hot Area:

Correct Answer:

Explanation/Reference:
Get-CASMailbox: Exchange 2013 Help
Set-CASMailbox: Exchange 2013 Help

Question 149
Which four cmdlets should you use? You need to configure the address books to meet the business goal for the finance department. Which four cmdlets should you use?
A. Set-MailUser, New-OfflineAddressBook, New-AddressBookPolicy, and New-GlobalAddressList
B. Set-MailUser, New-OfflineAddressBook, New-GlobalAddressList, and New-AddressList
C. Set-Mailbox, New-DistributionGroup, New-AddressBookPolicy, and New-AddressList
D. Set-Mailbox, New-AddressBookPolicy, New-GlobalAddressList, and New-AddressList

Correct Answer: D
Explanation/Reference:
Set-Mailbox must be used to assign the Address Book Policy, therefore D is correct
In creating the ABP, you will create multiple address lists based on how you want your users to view the address lists in Outlook or Outlook Web App. This organization has four address lists:

- **AL_FAB_Users_DGs**
- **AL_FAB_Contacts**
- **AL_FAB_Users_DGs**
- **AL_FAB_Contacts**

This example creates the address list **AL_FAB_Users_DGs**. The address list contains all users and distribution groups where CustomAttribute15 equals FAB.

```powershell
New-AddressList -Name "AL_FAB_Users_DGs" -RecipientFilter {((RecipientType -eq 'UserMailbox') -or (RecipientType -eq 'MailUniversalDistributionGroup') -or (RecipientType -eq 'MailDistributionGroup')) -and (CustomAttribute15 -eq "FAB")}
```

For more information about creating address lists by using recipient filters, see Create an Address List By Using Recipient Filters.

This organization has four address lists:

- **AL_TAIL_Users_DGs**
- **AL_TAIL_Contacts**
- **AL_BlankRoom**
- **AL_FAB_Contacts**

In creating the ABP, you will create multiple address lists based on how you want your users to view the address lists in Outlook or Outlook Web App. This organization has four address lists:

- **AL_TAIL_Users_DGs**
- **AL_TAIL_Contacts**
- **AL_BlankRoom**
- **AL_FAB_Contacts**

This example creates the address list **AL_TAIL_Users_DGs**. The address list contains all users and distribution groups where CustomAttribute15 equals TAIL.

```powershell
New-AddressList -Name "AL_TAIL_Users_DGs" -RecipientFilter {((RecipientType -eq 'UserMailbox') -or (RecipientType -eq 'MailUniversalDistributionGroup') -or (RecipientType -eq 'MailDistributionGroup') -or (RecipientType -eq 'ConferenceRoomMailbox') -or (RecipientType -eq 'MailDistributionGroup')) -and (CustomAttribute15 -eq "TAIL")}
```

For more information about creating address lists by using recipient filters, see Create an Address List By Using Recipient Filters.

In order to create an ABP, you have to provide a room address list. If your organization doesn’t have resource mailboxes such as room or equipment mailboxes, we suggest that you create a blank room address list. The following example creates a blank room address list because there are no room mailboxes in the organization.

```powershell
New-AddressList -Name "AL_BlankRoom" -RecipientFilter {((RecipientDisplayType -eq 'ConferenceRoomMailbox') -or (RecipientDisplayType -eq 'MailDistributionGroup') -or (RecipientDisplayType -eq 'MailDistributionGroup')) -and (CustomAttribute15 -eq "TAIL")}
```

However, in this scenario, Fabrikam and Contoso both have room mailboxes. This example creates room list for Fabrikam by using a recipient filter where CustomAttribute15 equals FAB.

```powershell
New-AddressList -Name "AL_FAB_Room" -RecipientFilter {((Alias -ne $null) -and (CustomAttribute15 -eq "FAB") -and (RecipientType -eq "MailUniversalDistributionGroup") -and (CustomAttribute15 -eq "TAIL"))}
```

This example creates the OAB for Fabrikam named **OAB_FAB**.

```powershell
New-OfflineAddressBook -Name "OAB_FAB" -AddressLists "GAL_FAB"
```

For more information, see Create an Offline Address Book.

Step 4: Create the ABPs.

After you’ve created all of the required objects you can then create the ABP. This example creates the ABP named **ABP_TAIL**.

```powershell
New-AddressBookPolicy -Name "ABP_TAIL" -AddressLists "AL_TAIL_Users_DGs","AL_TAIL_Contacts" -OfflineAddressBook "OAB_TAIL" -GlobalAddressList "GAL_TAIL"; -RoomList "AL_TAIL_Rooms"
```

For more information, see Create an Address Book Policy.

Step 5: Assign the ABPs to the mailboxes

Assigning the ABP to the user is the last step in the process. ABPs take effect when a user application connects to the Microsoft Exchange Address Book service on the Client Access server. If the user is already connected to Outlook or Outlook Web App when the ABP is applied to their account, they will need to close and restart the client application before they can see their new address lists and GAL.

This example assigns **ABP_FAB** to all mailboxes where CustomAttribute15 equals **FAB**.

```powershell
Get-Mailbox | Set-Mailbox -AddressBookPolicy "ABP_TAIL"
```

### Question 150

Which command should you run?

You need to ensure that if a volume fails on EX2 again, a mailbox database copy is recreated automatically on a different volume.

Which command should you run?

A. Set-MailboxAutoRecovery
B. Set-MailboxDatabase
C. Set-MailboxDatabaseCopy
D. Set-MailboxAutoReplayConfig

Correct Answer: C

Explanation/Reference: Exchange 2013 includes a great new high availability feature that is part of the Database Availability Group. This feature will reseed a database in case of disk failure from a “pool” of volumes that were pre-configured for this purpose. In case that the failed drive contained an active database, Exchange will failover to one of the other passive copies and reseed the database. In case that the failed drive contained one of the passive copies, Exchange will reseed the database on the same drive.

### Question 151

Which three actions should you recommend performing in sequence?

**DRAG DROP**

You need to recommend to a solution to deploy the Outlook app.

Which three actions should you recommend performing 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.)

Select and Place:

Correct Answer: 

Explanation/Reference: 

References:
Install or Remove Apps for Outlook for Your Organization
Get-App: Exchange 2013 Help
Set-App: Exchange 2013 Help

Question 152
Which command should you include in the recommendation?
HOTSPOT
You need to recommend a solution to meet the technical requirement for message recovery.
Which command should you include in the recommendation? (To answer, configure the appropriate options in the answer area.)
Hot Area:

Correct Answer:

Explanation/Reference:
References:

Question 153
Which cmdlets should you recommend using on EX1 and EX2?
DRAG DROP
You need to recommend a solution to resolve the user access issues that occur during the installation of updates on the Exchange Server 2013 servers.
Which cmdlets should you recommend using on EX1 and EX2? (To answer, drag the appropriate cmdlet 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.)
Select and Place:

Correct Answer:

Explanation/Reference:
The process for putting an Exchange 2013 server into maintenance mode is relatively straightforward. To enable the Maintenance Mode, you must run the commands below.
1. If the server is a Mailbox server and before you can disable the transport service, all active queues need to be drained first. To help clearing out the queues, existing messages on the server will be moved to another server.
2. Please note that the TargetServer value has to be a FQDN:
   - Set-ServerComponentState -Component HubTransport -State Draining -Requester Maintenance -Redirect-Message -Server -Target <server_fqdn>
   - If the server is part of a DAG, you must also run these commands:
     - Suspend-ClusterNode
     - Set-MailboxServer -DatabaseCopyActivationDisabledAndMoveNow True
   - Once all queues are empty, you can disable all components:
     - Set-MailboxServer -DatabaseCopyAutoActivationPolicy Blocked

   Taking the server out of Maintenance Mode is a matter of simply reversing the actions we took to put it into Maintenance Mode. First, we reactive all components:
   - Set-ServerComponentState -Identity -Component HubTransport -State Active -Requester Maintenance
   - If the server is part of a DAG, you need to reactive it in the cluster (by resuming the cluster node):
     - Resume-ClusterNode
   - Set-MailboxServer -DatabaseCopyAutoActivationPolicy Unrestricted
   - If the server is a Mailbox Server, the transport queues need to be resumed as well:

   This ensures they 'pick up' the changed component states immediately rather than having to wait for Managed Availability (Health Service) to take action.

Question 154
What should you include in the recommendation?
You need to recommend a solution to resolve the issue of the human resources department manager.
What should you include in the recommendation?
A. Run Set-ADServerSettings -ConfigurationDomainController dcl.proseware.com on all of the Exchange servers in the London site.
B. Move the PDC emulator to the New York office.
C. Modify the replication interval on the Active Directory site link.
D. Schedule a task that runs the Update-AddressList command to run once per hour.

Correct Answer: C

Explanation/Reference:
Set-ADServerSettings
Use the Set-ADServerSettings cmdlet to manage the Active Directory Domain Services (AD DS) environment in the current Exchange Management Shell session. The Set-ADServerSettings cmdlet replaces the AdminSessionADSettings session variable that was used in Microsoft Exchange Server 2007.

The ConfigurationDomainController parameter specifies the fully qualified domain name (FQDN) of the configuration domain controller to be used for reading Exchange configuration information in this session.

Not B
Issue is related to AD Site replication

Not D
Will not improve the site replication

You can use the Shell to update a global address list (GAL). A GAL is a directory that contains entries for every group, user, and contact within an organization’s implementation of Microsoft Exchange.

C
You must set the site link replication interval property to indicate how frequently you want replication to occur during the times when the schedule allows replication. For example, if the schedule allows replication between 02:00 hours and 04:00 hours, and the replication interval is set for 30 minutes, replication can occur up to four times during the scheduled time. The default replication interval is 180 minutes, or 3 hours.

Consider the following criteria to determine how often replication occurs within the schedule window:

- A small interval decreases latency but increases the amount of WAN traffic.
- To keep domain directory partitions up to date, low latency is preferred.


**Question 155**

What should you do?
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.

Correct Answer: D
Explanation/Reference:
Explanation:

A. Would not resolve the issue.
B. Would not resolve the issue.
C. Would not resolve the issue.
D. Recommend to create a new arbitration mailbox.


**Question 156**

Which three actions should you recommend?
Running above command will force Outlook client “Only connect to proxy servers that have this principal name in their certificate” to be enabled and value set to msstd:mail.contoso.com.
If client connects to a proxy server, which does not have mail.contoso.com in subject name field in the certificate, the connection will fail.

You need to recommend which actions must be performed to meet the technical requirements for the new Contoso users.
Which three actions should you recommend? (Each correct answer presents part of the solution. Choose three.)
A. Configure UPN suffix routing.
B. Configure Contoso to trust Proseware.
C. Configure Proseware to trust Contoso.
D. Run the New-Mailbox cmdlet and specify the LinkedMasterAccount parameter.
E. Run the New-Mailbox cmdlet and specify the LinkedMasterAccount parameter.
F. Create a linked role group.

Correct Answer: D
Explanation/Reference:
Explanation:

A. Would not resolve the issue.
B. Would not resolve the issue.
C. Would not resolve the issue.
D. Recommend to create a new arbitration mailbox.
E. Recommend to create a new arbitration mailbox.
F. Recommend to create a new arbitration mailbox.


**Explanation:**

The LinkedMasterAccount parameter specifies the master account in the forest where the user account resides. The master account grants access to the mailbox. This parameter is required only if you're creating a linked mailbox.

A linked mailbox is a mailbox that's associated with an external account. The resource forest scenario is an example of a situation in which you would want to associate a mailbox with an external account. In a resource forest scenario, user objects in the Exchange forest have mailboxes, but the user objects are disabled for logon. You must associate these mailbox objects in the Exchange forest with enabled user objects in the external accounts forest.

Several components in a hybrid deployment are required to enable the shared free/busy feature in a Microsoft Exchange Server 2013 deployment:

Sharing free/busy (calendar availability) information between users located on-premises and in the Exchange Online organization is one of the primary benefits of a hybrid deployment. Users in both organizations can view each other’s calendars just as if they were located in the same physical organization. This makes scheduling meetings and resources easy and efficient.

Several components in a hybrid deployment are required to enable the shared free/busy feature in a Microsoft Exchange Server 2013 deployment:

NOT Set-AutodiscoverVirtualDirectory
Changing the Autodiscover virtual directory will not address the issues.
Use the Set-AutodiscoverVirtualDirectory cmdlet to configure settings on the Autodiscover virtual directory on a server running Microsoft Exchange Server 2013. You can run this cmdlet on the local Client Access server or from another Exchange 2013 server.

EXAMPLE 1
This example sets the authentication method to Digest authentication for the Autodiscover virtual directory.
Set-AutodiscoverVirtualDirectory -Identity 'autodiscover(default Web Site)' -BasicAuthentication $false -DigestAuthentication Strue
NOT Set-AvailabilityConfig
The Set-AvailabilityConfig cmdlet defines two accounts or security groups: a per-user free/busy proxy account or group, and an organization-wide free/busy proxy account or group.
These accounts and groups are trusted by all availability services in the current organization for availability proxy requests.
For cross-forest availability services to retrieve free/busy information in the current forest, they must be using one of the specified accounts, belong to one of the specified security groups, or have a user name and password for one of the specified accounts or security groups.

You can use a linked management role group to enable members of a universal security group (USG) in a foreign Active Directory forest to manage a Microsoft Exchange Server 2013 organization in a resource Active Directory forest.
By associating a USG in a foreign forest with a linked role group, the members of that USG are granted the permissions provided by the management roles assigned to the linked role group.

For more information about linked role groups, see Understanding Management Role Groups.

Question 157
Which command should you include in the recommendation?
HOTSPOT
You need to recommend a solution to resolve the Autodiscover and the free/busy information issues.
Which command should you include in the recommendation? (To answer, configure the appropriate options in the answer area.)
Hot Area:

Correct Answer:

Explanation/Reference:
Explanation:
Free/busy information issues
Sharing free/busy (calendar availability) information between users located on-premises and in the Exchange Online organization is one of the primary benefits of a hybrid deployment. Users in both organizations can view each other’s calendars just as if they were located in the same physical organization. This makes scheduling meetings and resources easy and efficient.
Several components in a hybrid deployment are required to enable the shared free/busy feature in a Microsoft Exchange Server 2013 deployment:

NOT Set-AutodiscoverVirtualDirectory
Changing the Autodiscover virtual directory will not address the issues.
Use the Set-AutodiscoverVirtualDirectory cmdlet to configure settings on the Autodiscover virtual directory on a server running Microsoft Exchange Server 2013. You can run this cmdlet on the local Client Access server or from another Exchange 2013 server.

EXAMPLE 1
This example sets the authentication method to Digest authentication for the Autodiscover virtual directory.
Set-AutodiscoverVirtualDirectory -Identity 'autodiscover(default Web Site)' -BasicAuthentication $false -DigestAuthentication Strue
NOT Set-AvailabilityConfig
The Set-AvailabilityConfig cmdlet defines two accounts or security groups: a per-user free/busy proxy account or group, and an organization-wide free/busy proxy account or group.
These accounts and groups are trusted by all availability services in the current organization for availability proxy requests.
For cross-forest availability services to retrieve free/busy information in the current forest, they must be using one of the specified accounts, belong to one of the specified security groups, or have a user name and password for one of the specified accounts or security groups.

Set-ClientAccessServer
Use the Set-ClientAccessServer cmdlet to set properties on specified Client Access server objects.

EXAMPLE 1
This example sets two properties on the Client Access server CAS-01.
-AutoDiscoverSiteScope “Mail”
The AutoDiscoverServiceDefaultUri parameter specifies the default URL of the Autodiscover service.
NOT -External
Parameter not related to Set-ClientAccessServer
Parameter not related to Set-AvailabilityConfig
Parameter not related to Set-AutodiscoverVirtualDirectory
NOT -Internal
Parameter not related to Set-ClientAccessServer
Parameter not related to Set-AvailabilityConfig
Parameter not related to Set-AutodiscoverVirtualDirectory


Question 158
Which two commands should you run?
You are implementing a solution to meet the security requirements for Outlook authentication.
You purchase a new certificate that has a subject name of mail.proseware.com and SANs of autodiscover.proseware.com and oa.proseware.com.
You create a host (A) record for oa.proseware.com in the public DNS zone.
Remote users report that they fail to connect to their mailbox by using Outlook.
You need to ensure that the remote users can connect to their mailbox from Outlook. The solution must meet the security requirements.
Which two commands should you run? (Each correct answer presents part of the solution. Choose two.)
A. Set-OutlookProvider EXPR -CertPrincipalName msstd:mail.proseware.com
B. Set-OutlookAnywhere -ExternalHostName mail.proseware.com -ExternalClientAuthenticationMethod Basic -ExternalClientsRequireSsl Strue – InternalHostName mail.proseware.com -InternalClientAuthenticationMethodMethod NTLM -InternalClientsRequireSsl Strue
C. Set-OutlookProvider EXPR -CertPrincipalName msstd:oa.proseware.com
D. Set-OutlookAnywhere -ExternalHostName mail.proseware.com -ExternalClientAuthenticationMethod Basic -ExternalClientsRequireSsl Strue – InternalHostName mail.proseware.com -InternalClientAuthenticationMethodMethod NTLM -InternalClientsRequireSsl Strue

Correct Answer: AB

Explanation/Reference:
Explanation:
Set-OutlookProvider EXPR
The common benefit of enabling Outlook Provider, is to assure Outlook client connecting to a specific server, which has a specific name in subject name field on the certificate.
Set-OutlookProvider EXPR -CertPrincipalName msstd:mail.contoso.com
Running above command will force Outlook client “Only connect to proxy servers that have this principal name in their certificate” to be enabled and value set to
If client connects to a proxy server, which does not have mail.contoso.com in subject name field in the certificate, the connection will fail.

Set-OutlookAnywhere

Use the Set-OutlookAnywhere cmdlet to modify the properties on a computer running Microsoft Exchange Server 2013 enabled for Microsoft Outlook Anywhere.

The ExternalHostname parameter specifies the external host name to use in the Microsoft Outlook profiles for users enabled for Outlook Anywhere.

A
Subject name of the certificate is mail.proseware.com not oa.proseware.com
NOT C
Subject name of the certificate is mail.proseware.com not oa.proseware.com
B
ExternalHostName mail.proseware.com is correct as oa.proseware.com is a host (A) record in the public DNS zone.
NOT D
ExternalHostName mail.proseware.com is NOT correct as oa.proseware.com is a host (A) record in the public DNS zone.


Question 159
Which command should you use?
HOTSPOT
You are attempting to resolve the database activation issue. You need to identify why the database copies are activated on EX3 instead of EX2.
Which command should you use? (To answer, select the appropriate options in the answer area.)

Hot Area:

Correct Answer:

Explanation/Reference:
Exchange 2013 Managed Availability

In Exchange 2013, native, built-in monitoring and recovery actions are included in a feature called Managed Availability. Managed Availability is the integration of built-in, active monitoring and the Exchange 2013 high availability platform, allowing Exchange to make a determination on when to fail over a database based on service health.

To view the health of a server, you use the cmdlets Get-ServerHealth to retrieve the raw health data and Get-HealthReport that operates on the raw health data and provides a snapshot of the health.

This example returns the server health for server MBX1:

Get-ServerHealth Server01

The following examples return a report on the health of the server. The second cmdlet narrows the report to the Store process:


Get-AvailabilityReportOutage

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.

EXAMPLE 1
This example returns all outages that occurred the previous day. This cmdlet always returns outages for one day.

Get-AvailabilityReportOutage

EXAMPLE 2
This example returns all outages reported for Microsoft Outlook services at all sites on the selected day.

Get-AvailabilityReportOutage -ReportDate:"2011-12-05" -Identity:"Outlook*"

Get-HealthReport

Use the Get-HealthReport cmdlet to return health information related to the server you specify. You can use the health values to determine the state of the server. The cmdlet also returns an alert value that provides the specific state of your server.

This example retrieves health information about a server running Microsoft Exchange Server 2013.

Get-HealthReport -RollupGroup

The following list contains the health values that are returned:

Online
Partially Online
Offline
Sidelined
Functional
Unavailable
Get-ServerHealth

Use the Get-ServerHealth cmdlet to return health information related to the server you specify.

This example returns the server health for server Server01.

Get-ServerHealth -Identity Server01

The cmdlet also returns an alert value that provides the specific state of your server. The following values may be returned:

Degraded
Unhealthy
Repairing
Disabled
Unavailable
UnInitialized


Question 160
Which commands should you run?
DRAG DROP

You need to identify which commands must be run to perform the maintenance window tasks.

Which commands should you run? (To answer, drag the appropriate commands to the correct tasks. Each command 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.)

Select and Place:
Performing maintenance on DAG members

- Start-DatabaseAvailabilityGroup
  - Identity DAG1
  - MailboxServer MBX2

Draining the transport queue refers to emptying the transport queue.

- Run Set-ServerComponentState -Component HubTransport -State Draining -Requester Maintenance

- Run Suspend-ClusterNode <ServerName> to pause the cluster node, which prevents the node from becoming the PAM.

- Run Set-MailboxServer <ServerName> – DatabaseCopyAutoActivationPolicy Blocked to prevent the server from hosting active database copies.

Draining the transport queue refers to emptying the transport queue.

- Run Set-MailboxServer <ServerName> – DatabaseCopyActivationDisabledAndMoveNow $True

The question is asking you to failover the databases.
To verify that a server is ready for maintenance, perform the following tasks:

1. Run `Get-MailboxServer <ServerName> | ft DatabaseCopy* -AutoSize` to verify the server has been placed into maintenance mode.
2. Run `Get-TransportService` to view the transport configuration information for the Transport service on Mailbox servers or for Edge Transport servers.
   - Example 1
     - This example provides different results depending on the server role on which it’s run. When you run this command on an Edge Transport server, it provides a configuration summary for the local server. Otherwise, it displays a list of all Mailbox servers in your organization.
     - Get-TransportService
     - Example 2
     - This example retrieves the detailed transport configuration information for the Transport service on the Mailbox server named Mailbox1.
     - Get-TransportService Mailbox1 | Format-List
     - Get-Message
     - Related to message queue
     - Use the Get-Message cmdlet to view the details of one or more messages in queues on Mailbox servers or Edge Transport servers.
     - EXAMPLE 1
     - This example displays detailed information about all messages queued on the local server and received from any sender at the contoso.com domain.
     - Get-Message -Filter {FromAddress -like "contoso.com"} -Format-List
     - Get Queue
     - Use the Get-Queue cmdlet to view configuration information for queues on Mailbox servers or Edge Transport servers.
     - EXAMPLE 1
     - This example displays detailed information about all queues on the Mailbox server on which the command is run.
     - Get-Queue | Format-List
     - EXAMPLE 2
     - This example lists the queues that contain more than 100 messages.
     - Get-Queue -Filter {MessageCount -gt 100}
     - Remove-Message
     - Use the Remove-Message cmdlet to delete messages from a queue on a Mailbox server or an Edge Transport server.
     - EXAMPLE 1
     - This example removes all messages that meet the following criteria without generating NDRs:
       - Messages sent by the sender [email protected]
       - The messages are queued on the server Server1
     - Remove-Message -Server Server1 -Filter {FromAddress -eq [email protected]} -WithNDR $false
     - NOT Resend-Message, Suspend-Message
     - Need to remove the email notifications from all of the servers if App1 malfunctions again.
     - Related to message queue
     - Use the Get-Queue cmdlet to view information about the amount of mailboxes in this organization.
     - Example 1
     - This example returns information about all queues in the DAG named DAG01.
     - Get-QueueDigest DAG01
     - NOT SUSPEND-QUEUE
     - Not needed in this scenario
     - The Suspend-Queue cmdlet stops processing on a queue that has a status of Active or Retry
     - NOT GET-MESSAGETRACKINGLOG
     - Not needed in this scenario
     - Use the Get-MessageTrackingLog cmdlet to search for message delivery information stored in the message tracking log.
     - EXAMPLE 1
     - This example searches the message tracking logs on the Mailbox server named Mailbox01 for information about all messages sent from March 13, 2013, 09:00 to March 15, 2013, 17:00.
     - Get-MessageTrackingLog -Server Mailbox01 -Start "03/13/2013 09:00:00" -End "03/15/2013 17:00:00" –

Question 161

Which command should you recommend?

Hotspot

You need to recommend which command must be run to remove the email notifications from all of the servers if App1 malfunctions again.

Which command should you recommend? (To answer, configure the appropriate options in the answer area.)

Hot Area:

Correct Answer:

Explanation/Reference:

Powershell Commands and Piping

The output of the initial command is an input into the next command in the sequence.

The ResultSize parameter specifies the maximum number of results to return. If you want to return all results that match the query, use unlimited for the value of this parameter.

Get-TransportService

Can you this command to obtain a listing of mailbox servers in the organization.

Use the Get-TransportService cmdlet to view the transport configuration information for the Transport service on Mailbox servers or for Edge Transport servers.

Example 1

This example provides different results depending on the server role on which it’s run. When you run this command on an Edge Transport server, it provides a configuration summary for the local server. Otherwise, it displays a list of all Mailbox servers in your organization.

Get-TransportService

Example 2

This example retrieves the detailed transport configuration information for the Transport service on the Mailbox server named Mailbox1.

Get-TransportService Mailbox1 | Format-List

Get-Message

Related to message queue

Use the Get-Message cmdlet to view the details of one or more messages in queues on Mailbox servers or Edge Transport servers.

EXAMPLE 1

This example displays detailed information about all messages queued on the local server and received from any sender at the contoso.com domain.

Get-Message -Filter {FromAddress -like "contoso.com"} -Format-List

Get Queue

Use the Get-Queue cmdlet to view configuration information for queues on Mailbox servers or Edge Transport servers.

EXAMPLE 1

This example displays detailed information about all queues on the Mailbox server on which the command is run.

Get-Queue | Format-List

EXAMPLE 2

This example lists the queues that contain more than 100 messages.

Get-Queue -Filter {MessageCount -gt 100}

Remove-Message

Use the Remove-Message cmdlet to delete messages from a queue on a Mailbox server or an Edge Transport server.

EXAMPLE 1

This example removes all messages that meet the following criteria without generating NDRs:

- The messages are sent by the sender [email protected]
- The messages are queued on the server Server1

Remove-Message -Server Server1 -Filter {FromAddress -eq [email protected]} -WithNDR $false

NOT Resend-Message, Suspend-Message

Need to remove the email notifications from all of the servers if App1 malfunctions again.

Related to message queue

Use the Get-Queue cmdlet to view information about the amount of mailboxes in this organization.

Example 1

This example returns information about all queues in the DAG named DAG01.

Get-QueueDigest DAG01

NOT SUSPEND-QUEUE

Not needed in this scenario

The Suspend-Queue cmdlet stops processing on a queue that has a status of Active or Retry

NOT GET-MESSAGETRACKINGLOG

Not needed in this scenario

Use the Get-MessageTrackingLog cmdlet to search for message delivery information stored in the message tracking log.

EXAMPLE 1

This example searches the message tracking logs on the Mailbox server named Mailbox01 for information about all messages sent from March 13, 2013, 09:00 to March 15, 2013, 17:00.

Get-MessageTrackingLog -Server Mailbox01 -Start "03/13/2013 09:00:00" -End "03/15/2013 17:00:00" –

In Microsoft Exchange Server 2013, the message tracking log is a detailed record of all message activity as messages are transferred to and from the Transport service on Mailbox servers, mailboxes on Mailbox servers, and Edge Transport servers. You can use the Get-MessageTrackingLog cmdlet in the Exchange Management Shell to search for entries in the message tracking log by using specific search criteria.

Correct Answer:

Explanation/Reference:

Anti-Spam Agents


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

You can then pass this message tracking report ID to the Get-MessageTrackingReport cmdlet to get full message tracking information. For more information, see Get-MessageTrackingReport. The message tracking report cmdlets are used by the delivery reports feature.

Steps

1. Get-TransportService obtains a listing of all mail servers in the exchange organization
2. Get-Queue displays detailed information of the queue on these mail servers
3. Get-Message displays details of the messages in these queues on these mail servers
4. -ResultSize unlimited | Where {$_ Subject -eq “System Alert: Sales Database Reaching Capacity” } 

This statement returns an unlimited listing of emails with a subject of “System Alert: Sales Database Reaching Capacity” and removes the ones that do not have a No Delivery Notification attached to them.


NDR – non-delivery report (NDR) delivery status notification (DSN) messages in Microsoft Exchange Server 2013.

You are evaluating the planned deployment of the additional Exchange Server 2013 servers.

You need to meet the technical requirement for installing all of the anti-spam agents and for enabling antimalware filtering.

What should you do? (To answer, drag the appropriate servers to the correct locations. 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.)

Select and Place:

Correct Answer:

Explanation/Reference:

Anti-Spam Agents


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

However, you can install these anti-spam agents on a Mailbox server running a script in the Exchange Management Shell. Typically, you would install the anti-spam agents on a Mailbox server only when your organization accepts all incoming mail without any prior anti-spam filtering.

What happens if you install the available anti-spam agents on a Transport service on a Mailbox server, but you also have other Exchange anti-spam agents operating on the messages before they reach the Mailbox server?

For example, what if you have a Microsoft Exchange 2007 or Exchange 2010 Edge Transport server in the perimeter network that delivers incoming mail directly to the Transport service on the Mailbox server?

The anti-spam agents on the Mailbox server recognize the anti-spam X-header values that are added to messages by other Exchange anti-spam agents, and messages that contain these X-headers pass through without being scanned again. However, recipient look-ups performed by the Recipient Filter agent will occur again on the Mailbox server.

Anti-malware filtering

By default, malware filtering is enabled in Microsoft Exchange Server 2013. The default anti-malware policy controls your company-wide malware filtering settings.

As an administrator, you can view and edit, but not delete, the default anti-malware policy so that it is tailored to best meet the needs of your organization.

For greater granularity, you can also create custom malware filter policies and apply them to specified users, groups, or domains in your organization. Custom policies always take precedence over the default policy, but you can change the priority (that is, the running order) of your custom policies.

Client Access Servers

The Client Access Server role is simplified to be a stateless server that accepts and authenticates client connections and acts as a proxy between the clients and the Mailbox servers, ensuring that clients can locate the Mailbox server with the required data. No data or session state is stored on the Client Access server, and clients can connect to any Client Access server and even switch Client Access servers during a session (previous clients using some protocols had to stay connected to the same server for an entire session), thereby reducing load-balancing complexity. Client Access servers can be located in different sites from Mailbox servers, which provides flexibility for deployments.

Steps

1. ANY OF EX1-EX4
2. EXCLUDE EX5
3. STEPS

SERVORS ON WHICH TO INSTALL ALL OF THE ANTI-SPAM AGENTS
(NOT INSTALLED BY DEFAULT)

1. ANY OF EX1-EX4
2. EXCLUDE EX5
3. STEPS

SERVORS ON WHICH TO ENABLE ANTIMALWARE FILTERING

1. ANY OF EX1-EX4
2. EXCLUDE EX5
3. STEPS


Malware protection settings, Exchange 2013 includes a brand-new enhanced feature for malware protection, by default this feature is enabled on Exchange Mailbox Servers, but if you want you can also disable it.

Anti-Spam Protection: Exchange 2013 Help

Set-OwaVirtualDirectory
Use the Set-OwaVirtualDirectory cmdlet to set attributes related to client access for Microsoft Exchange ActiveSync, Microsoft Office Outlook Web App, POP3, and IMAP4 for a specified user.

EXAMPLE 1
This example enables Outlook Web App and enables POP3 for the user [email protected]
Set-CASMailbox -Identity [email protected] -OWAEnabled -StrStrm -PopEnabled -Strue

Set-ClientAccessArray
Appears to be an Exchange 2010 command
Use the Set-ClientAccessArray cmdlet to specify an object that represents a load-balanced array of Client Access servers within a single Active Directory site.

Detailed Description
The Set-ClientAccessArray cmdlet configures a load-balanced array of Client Access servers within an Active Directory site.

Set-OutlookProvider
Use the Set-OutlookProvider cmdlet to set specific global settings using the msExchOutlookProvider attribute on the msExchAutoDiscoverConfig object in Active Directory.

EXAMPLE 1
This example changes the duration that the Autodiscover service settings are valid for the Microsoft Outlook web provider msExchAutoDiscoverConfig.
Set-OutlookProvider -Identity msExchAutoDiscoverConfig -TTL 2

Set-OVAVirtualDirectory
Use the Set-OvaVirtualDirectory cmdlet to modify the properties of Microsoft Office Outlook Web App virtual directories on a server running Microsoft Exchange Server 2013 that has the Client Access server role installed.

EXAMPLE 1
This example sets the DirectFileAccessOnPublicComputersEnabled parameter to $false on the Outlook Web App virtual directory owa on the default Internet Information Services (IIS) website on the Exchange server Contoso.

DirectFileAccessOnPrivateComputersEnabled
Parameter of Set-OVAVirtualDirectory
The DirectFileAccessOnPrivateComputersEnabled parameter specifies the left-click options on attachments when the user has chosen to log on using the Private option.

If this parameter is set to Strue, Open is an available option. If it’s set to $false, the Open option is disabled.

OrganizationEnabled
Parameter of Set-OVAVirtualDirectory
When the OrganizationEnabled parameter is set to Strue, the Automatic Reply option doesn’t include external and internal options, the address book doesn’t show the organization hierarchy, and the Resources tab in Calendar forms is disabled.

WSSAccessOnPrivateComputersEnabled
Parameter of Set-OVAVirtualDirectory
The WSSAccessOnPrivateComputersEnabled parameter isn’t available in this release of Exchange 2013.

LogonPagePublicPrivateSelectionEnabled
Parameter of Set-OVAVirtualDirectory
The LogonPagePublicPrivateSelectionEnabled parameter specifies whether the Outlook Web App sign-in page includes the private computer or public computer sign-in option.

PlacesEnabled
Parameter of Set-OVAVirtualDirectory
This parameter is reserved for internal Microsoft use.

PremiumClientEnabled
Parameter of Set-OVAVirtualDirectory
The PremiumClientEnabled parameter is no longer used and will be deprecated.

PublicFoldersEnabled
Parameter of Set-OVAVirtualDirectory
The PublicFoldersEnabled parameter specifies whether a user can browse or read items in public folders using Outlook Web App.

By default, the PublicFoldersEnabled parameter is set to Strue. If the PublicFoldersEnabled parameter is set to $false, users can only access their private mailboxes in Outlook Web App.

STEPS
1. Set-OVAVirtualDirectory Offline mode is concerned with the virtual directory settings of OWA.

   - AllowOfflineOn

   The AllowOfflineOn parameter specifies which computers can use Outlook Web App in offline mode. The possible values are PrivateComputersOnly, NoComputers, or AllComputers

   3. LogonPagePublicPrivateSelectionEnabled

   The LogonPagePublicPrivateSelectionEnabled parameter specifies whether the Outlook Web App sign-in page includes the private computer or public computer sign-in option.

Set-OvaVirtualDirectory: Exchange 2013 Help
Question 164
What should you include in the recommendation?
You are evaluating the deployment of the additional Exchange Server 2013 servers.
You need to recommend changes to the transport configurations to ensure that all email messages sent from the Detroit office are routed through EX2.
What should you include in the recommendation?
A. Increase the cost of the CHI-NY site link to 15.
B. Specify an Exchange-specific cost of 20 for the CHI-DET site link.
C. Decrease the cost of the CHI-NY and the DET-NY site links to 4.
D. Increase the cost of the DET-NY site link to 15.
Correct Answer: B
Explanation/Reference:
Route Mail Between Active Directory Sites: Exchange 2013 Help
N O T A C D
Need to introduce an exchange specific cost not change and AD cost
B
You need to recommend changes to the transport configurations to ensure that all email messages sent from the Detroit office are routed through EX2.
All of the Detroit Users have a mailbox hosted on EX2 currently (New York)
After the planned changes all of Detroit mailboxes would be shifted to EX3 (Detroit)
The office in New York and Detroit connect to the internet directly.
In order to change the transport configuration to ensure that all email messages sent from the Detroit office are routed through EX2 an exchange specific cost has to be implemented.
B is the only answer option which achieves this.

Question 165
What should you include in the solution?
You need to recommend a solution to resolve the issue of email messages not being received on the Internet.
What should you include in the solution?
A. Modify the CNAME record.
B. Add an MX record.
C. Modify the TXT record.
D. Add a pointer (PTR) record.
Correct Answer: D
Explanation/Reference:
A Canonical Name or CNAME record is a type of DNS record that links an alias name to another canonical domain name.
You’ll need to configure DNS CNAME records if you want to use URL forwarding to create a custom web address, forward a URL to Google Sites, or forward a naked domain URL, as well as verify your site with your domain name provider.
Lastly, you may need to use CNAME records to reset the administrator password if you can’t access the Google Apps control panel because you’ve forgotten the administrator password.
Your CNAME record logs are stored in the DNS Zone File as pairs of key values.
The value of an A CNAME record is always a domain name. CNAME records are often used to create subdomains. CNAME records are useful because they allow you to set up an alias to a server without using its IP address, through an intermediary standard domain name.
MX Records
MX Records are DNS settings associated with your domain that direct its mail to the servers hosting your users’ email accounts.
These settings are managed by your domain host, not by Google. To make sure mail always gets delivered, you typically create records for multiple servers, all of which can deliver mail to users.
That way, if one server is down, mail can be routed to another server, instead. You determine which servers get tried first by assigning priorities, using values like 10, 20, 30, and so on. The lowest value gets highest priority.

CTR Record
A DNS PTR record – for those of you who are wondering – is a special entry in the Domain Name System (DNS) that basically maps an IP address (like 65.33.12.249) to a domain name (like www.c2zip.microsoft.com). Having a DNS PTR record for your IP address is (somewhat) a sign of reliability in the Internet, since only the owner of a specific network zone has the ability to create and edit these DNS records.
Today, most mail exchangers will check this record for each incoming connection and may abort the communication if they find your IP address does not have an associated DNS PTR entry; because of this reason, always suggest to make sure your public servers IP addresses have DNS PTR records configured properly. While EmailVerify.NET can validate email addresses even without a DNS PTR entry configured, the quality of the validation results in this event may be suboptimal.

TXT Record
A TXT record is an entry within the Domain Name System (DNS) that provides supplemental information about your domain.
A TXT (text) record is used to hold some test information. You can put virtually any free text you want within a TXT record.
A TXT record has a hostname so that you can assign the free text to a particular hostname/zone.
The most common use for TXT records is to store SPF (sender policy framework) records and to prevent emails being faked to appear to have been sent from you. The name field of the SPF record should be left blank unless mail is sent from a subdomain such as [email protected] If this was the case “mail” would be entered in the name field of the record.
Alternatively, if email is sent from [email protected], the name field is left blank. The data field of the record is populated with the list of hosts that are permitted to send email for the domain in SPF format.

There are wizards which can assist in generating an SPF record available. The data field of the record must be enclosed in quotations so servers will read the value as a single string. Below is a default SPF record example-1.com.

```
 not a
```

### Question 166
What should you include in the recommendation?

You need to recommend a solution for the New York office that meets the technical requirements for client access.

What should you include in the recommendation? (Each correct answer presents a complete solution. Choose all that apply.)

A. DNS round robin
B. A Layer 4 hardware load balancer
C. A Layer 7 hardware load balancer
D. The Network Load Balancing (NLB) feature
E. A Client Access server array

Correct Answer: CE

Explanation/Reference:
Load Balancing: Exchange 2013 Help

### Question 167
Which three actions should you recommend performing in sequence?

**DRAG DROP**

You need to recommend a solution to meet the mailbox creation requirements.

Which three actions should you recommend performing 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.)

Select and Place:

Correct Answer:

Explanation/Reference:

Explanation:
Cmdlet Extension Agents: Exchange 2013 Help

Cmdlet Extension Agents

Cmdlet extension agents are components in Microsoft Exchange Server 2013 invoked by Exchange 2013 cmdlets when the cmdlets run. As the name implies, cmdlet extension agents extend the capabilities of the cmdlets that invoke them by assisting in processing data or performing additional actions based on the requirements of the cmdlet. Cmdlet extension agents are available on any server role.

Agents can modify, replace, or extend functionality of Exchange Management Shell cmdlets. An agent can provide a value for a required parameter that isn’t provided on a command, override a value provided by a user, perform other actions outside of the cmdlet workflow while a cmdlet runs, and more.

You can use the Scripting agent cmdlet extension agent in Exchange 2013 to insert your own scripting logic into the execution of Exchange cmdlets. Using the Scripting agent, you can add conditions, override values, and set up reporting.

Every time an Exchange cmdlet is run, the cmdlet invokes the Scripting agent cmdlet extension agent. When this agent is invoked, the cmdlet checks whether any scripts are configured to be invoked by the cmdlet. If a script should be run for a cmdlet, the cmdlet tries to invoke any APIs defined in the script.

The Scripting agent configuration file contains all the scripts that you want the Scripting agent to run. Scripts in the configuration file are contained within XML tags that define the beginning and end of the script and various input parameters required to pass data to the script. Scripts are written using Windows PowerShell syntax.

The configuration file is an XML file that uses the elements or attributes in the following table.

Every Exchange 2013 server includes the file ScriptingAgentConfig.xml.sample in the <installation path>\V15\Bin\CmdletExtensionAgents folder. This file must be renamed as ScriptingAgentConfig.xml on every Exchange 2013 server if you enable the Scripting Agent cmdlet extension agent. The sample configuration file contains example scripts that you can use to help you understand how to add scripts to the configuration file.

After you add a script to the config file, if you make a change to the configuration file, you must update the file on every Exchange 2013 server in your organization. This must be done to make sure that each server contains an up-to-date version of the scripts that the Scripting agent cmdlet extension agent runs.

ScriptingAgentConfig.xml

- **Renamed from:** ScriptingAgentConfig.xml sample on every Exchange 2013 server if you enable the Scripting Agent cmdlet extension agent.

- **ScriptingAgentConfig.xml sample**

Every Exchange 2013 server includes the file ScriptingAgentConfig.xml sample in the <installation path>\V15\Bin\CmdletExtensionAgents folder.

This file must be renamed to ScriptingAgentConfig.xml on every Exchange 2013 server if you enable the Scripting Agent cmdlet extension agent.

The sample configuration file contains sample scripts that you can use to help you understand how to add scripts to the configuration file.

Enable-CmdletExtensionAgent "Scripting Agent" command

Use the Enable-CmdletExtensionAgent cmdlet on a server running Microsoft Exchange Server 2013 to enable a cmdlet extension agent.

**EXAMPLE 1**

This example enables the Scripting Agent cmdlet extension agent. Before you enable the Scripting Agent, you need to make sure that you’ve first deployed the ScriptingAgentConfig.xml configuration file to all the servers in your organization. If you don’t deploy the configuration file first and you enable the Scripting Agent, all non-Get cmdlets fail when they’re run.

Enable-CmdletExtensionAgent "Scripting Agent" command

Run the Set-CmdletExtensionAgent "Scripting Agent" command

Use the Set-CmdletExtensionAgent cmdlet on a server running Microsoft Exchange Server 2013 to modify a cmdlet extension agent.

**EXAMPLE 1**

This example enables the Scripting Agent cmdlet extension agent. Before you enable the Scripting Agent, you need to make sure that you’ve first deployed the ScriptingAgentConfig.xml configuration file to all the servers in your organization. If you don’t deploy the configuration file first and you enable the Scripting Agent, all non-Get cmdlets fail when they’re run.

Enable-CmdletExtensionAgent "Scripting Agent" command

Run the Set-CmdletExtensionAgent "Scripting Agent" command

Use the Set-CmdletExtensionAgent cmdlet on a server running Microsoft Exchange Server 2013 to modify a cmdlet extension agent.

**EXAMPLE 1**
This example changes the priority of the fictitious "Validation Agent" cmdlet extension agent to 9.

Set-CmdletExtensionAgent "Validation Agent" -Priority 9

Steps
1. Edit the ScriptingAgentConfig.xml.sample file, and then rename the file as ScriptingAgentConfig.xml
2. Copy the ScriptingAgentConfig.xml file to all of the Mailbox Servers

The question refers to mailbox creation requirements but according to the above information –
After you add a script to the configuration file, or if you make a change to the configuration file, you must update the file on every Exchange 2013 server in your organization. In the absence of further information, accept updating the mailbox servers over the client access servers 3.Enable-CmdletExtensionAgent "Scripting Agent" command Have to enable the cmdlet extension agent.

Question 168
Which external namespaces should you identify for each office?

Drag & Drop
You need to identify which external namespaces must be used for the Exchange servers in each office.
Which external namespaces should you identify for each office?

To answer, drag the appropriate namespace to the correct office in the answer area. Each namespace 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.
Select and Place:

Correct Answer:

Explanation/Reference:
This configuration ensures that the Client Access server does not redirect the connection to the target Client Access server, but instead proxies it. Installing Exchange 2013 into a mixed Exchange 2007 and Exchange 2010 organization
If so, then you first need to follow the steps in Install Exchange 2013 in an Existing Exchange 2007 Organization to create a new legacy namespace to coexist with Exchange 2013.
You need to create a legacy domain name system (DNS) host name so your legacy Exchange environment (Exchange 2007 and Exchange 2013) can coexist.
For example, if your domain name is currently contoso.com, you're likely using a host name of mail.contoso.com or www.contoso.com for external client access to Exchange.
During coexistence, we recommend creating and using, for example, a host name of legacy.contoso.com. This host name should be configured the same way your primary host name is configured. You'll associate the legacy host name with your existing Exchange servers and associate your current host name (for example, mail.contoso.com) with your Exchange 2013 Client Access server. Your end users will not see or use the legacy host name. It will be used by Autodiscover and Client Access servers when redirecting legacy users to a legacy server.
All client connections will be proxied, including Exchange ActiveSync, Outlook Web App, POP/IMAP, and IMAP4.
After the legacy host name has been configured, users will be able to access their mailbox regardless of whether it's on Exchange 2007 or Exchange 2013. If you're upgrading from Exchange 2007 to Exchange 2013, Availability service requests will also be redirected.
You will need a legacy namespace because Exchange 2013 uses a contiguous namespace.

Small Single Namespace with Proxy Sites
This model is based on the consolidated data center model but proxies the requests to the physical Mailbox server located at another site. One of the sites has one or more Internet-facing Client Access servers that proxy the requests.
This scenario has the following advantages:
Only one or very few DNS records need to be managed
Only one or very few certificates are required for your Exchange organization
All users use the same URL to access Exchange server.
The disadvantage of this model is that most users will access their mailboxes using proxying, thus accessing their data might be slower across latent WAN links.
To configure this namespace model, you need to configure the ExternalURL option of the Client Access server(s) at one site, and make sure that the ExternalURL settings on all the other sites are configured to $null. This configuration ensures that the Client Access server does not redirect the connection to the target Client Access server, but instead proxies it. Redirect means that the Client Access server forwards the connection to the target Client Access server; proxy means that the Client Access server contacts the target Client Access server and retrieves the data for the connection.
Autodiscover domain name
In order for Exchange 2007/2010/2013 and Outlook 2007/2010/2013 to function properly, you must have a special DNS record set up for your domain name which points to the Intermediate Autodiscover server.
You need to set up the Autodiscover record for your domain name to have the following features:
Outlook 2007/2010/2013 setup using Autodiscovery
Outlook 2011 for Mac and Entourage EWS setup using Autodiscovery
Free/Busy information in your Calendar
Out of Office automated response messages setup in Outlook
Note: Without the Autodiscover record you can use Outlook Web Access to set up automatic replies.
Proper syncing of Offline Address Book
Folder Sharing by sending out the Sharing invitation. Read the Knowledge Base article on How Do I Share (Let Others See) My Outlook Folders? for more information.
Load Balancing (Hardware and Virtual Load Balancing)
You need to have an understanding of how the load balancer fits in your environment. Typically clients will connect to it for web services, like OWA, and also through Outlook via MAPI, using a Client Access Array as illustrated by this simplified diagram:
In addition to planning your environment, you’ll also need some other information for the load balancer setup:
IP address for management
IP address for the virtual load balancer interface, in the same subnet
DNS and NTP server addresses
Client Access Server IP addresses
Network Access from the virtual load balancer interface to the following TCP ports on the Client Access Servers:
80 and 443 for HTTP/HTTPS
135, 139, 6001-6004,60000 and 60001 for RPC Client Access
Note that if you’re testing this in a perimeter network, you only need ports 80 and 443 open for external access to Exchange servers.

Exchange 2013 Client Access server configuration: Exchange 2013 Help
Set-AutodiscoverVirtualDirectory: Exchange 2013 Help

Question 169
Which command should you include in the recommendation?
HOTSPOT
You need to recommend a solution to meet the technical requirements for mailbox size restrictions.

Which command should you include in the recommendation? (To answer, select the appropriate options in the answer area.)

Hot Area:

Correct Answer:

Explanation/Reference:

Get-Mailbox
Use the Get-Mailbox cmdlet to view mailbox objects and attributes, populate property pages, or supply mailbox information to other tasks.

EXAMPLE 1
This example returns a list of all the mailboxes in your organization.
Get-Mailbox -ResultSize unlimited
Get-MailboxDatabase
Use the Get-MailboxDatabase cmdlet to retrieve one or more mailbox database objects from a server or organization.

EXAMPLE 1
This example retrieves information about all the mailbox databases in the Exchange organization, including the mailbox databases that reside on computers running Exchange 2013 and earlier versions of Exchange.
Get-MailboxDatabase -IncludePreExchange2013
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 (email protected) mailbox.
Set-Mailbox -Identity John -DeliverToMailboxAndForward True -ForwardingSMTPAddress [email protected]
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

-IssueWarningQuota Parameter of SetMailbox
The IssueWarningQuota parameter specifies the mailbox size at which a warning message is sent to the user. This attribute applies to all mailboxes in this mailbox database that don’t have their own warning quota attribute set. You must specify either an integer or unlimited.
The default value is 1.9 gigabytes (GB).
-ProhibitSendQuota Parameter of SetMailbox
The ProhibitSendQuota parameter specifies the mailbox size at which users associated with mailboxes in this mailbox database can no longer send messages. This attribute applies to all mailboxes in this mailbox database that don’t have their own prohibit send quota attributes set. You must specify either an integer or unlimited.
-ProhibitSendReceiveQuota Parameter of SetMailbox
The ProhibitSendReceiveQuota parameter specifies the mailbox size at which the user associated with this mailbox can no longer send or receive messages. This attribute applies to all mailboxes in this mailbox database that don’t have their own prohibit send receive quota attributes set. You must specify either an integer or unlimited.

STEPS
1. Get-MailboxDatabase to retrieve a listing of all the mailbox databases.
2. Set-MailboxDatabase to configure a variety of properties for a mailbox database.
3. -ProhibitSendReceiveQuota to limit the size of the mailbox to the specified level of 5 GB.

Get-MailboxDatabase: Exchange 2013 Help
Set-MailboxDatabase: Exchange 2013 Help

Question 170
Which command should you include in the recommendation?

HOTSPOT
You need to recommend a solution to meet the technical requirements for email message recovery.

Which command should you include in the recommendation? (To answer, configure the appropriate options in the answer area.)

Hot Area:

Correct Answer:

Explanation/Reference:

Get-Mailbox
Use the Get-Mailbox cmdlet to view mailbox objects and attributes, populate property pages, or supply mailbox information to other tasks.

EXAMPLE 1
This example returns a list of all the mailboxes in your organization.
Get-Mailbox -ResultSize unlimited
Get-MailboxDatabase
Use the Get-MailboxDatabase cmdlet to retrieve one or more mailbox database objects from a server or organization.

EXAMPLE 1
This example retrieves information about all the mailbox databases in the Exchange organization, including the mailbox databases that reside on computers running Exchange 2013 and earlier versions of Exchange.
Get-MailboxDatabase -IncludePreExchange2013
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 (email protected) mailbox.
Set-Mailbox -Identity John -DeliverToMailboxAndForward True -ForwardingSMTPAddress [email protected]
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

-IssueWarningQuota Parameter of SetMailbox
The IssueWarningQuota parameter specifies the mailbox size at which a warning message is sent to the user. This attribute applies to all mailboxes in this mailbox database that don’t have their own warning quota attribute set. You must specify either an integer or unlimited.
The default value is 1.9 gigabytes (GB).
-ProhibitSendQuota Parameter of SetMailbox
The ProhibitSendQuota parameter specifies the mailbox size at which users associated with mailboxes in this mailbox database can no longer send messages. This attribute applies to all mailboxes in this mailbox database that don’t have their own prohibit send quota attributes set. You must specify either an integer or unlimited.
-ProhibitSendReceiveQuota Parameter of SetMailbox
The ProhibitSendReceiveQuota parameter specifies the mailbox size at which the user associated with this mailbox can no longer send or receive messages. This attribute applies to all mailboxes in this mailbox database that don’t have their own prohibit send receive quota attributes set. You must specify either an integer or unlimited.

STEPS
1. Get-MailboxDatabase to retrieve a listing of all the mailbox databases.
2. Set-MailboxDatabase to configure a variety of properties for a mailbox database.
3. -ProhibitSendReceiveQuota to limit the size of the mailbox to the specified level of 5 GB.

Get-MailboxDatabase: Exchange 2013 Help
Set-MailboxDatabase: Exchange 2013 Help

Question 170
Which command should you include in the recommendation?

HOTSPOT
You need to recommend a solution to meet the technical requirements for mailbox size restrictions.

Which command should you include in the recommendation? (To answer, select the appropriate options in the answer area.)

Hot Area:
Use the Set-TransportService cmdlet to set the transport configuration options for the Transport service on Mailbox servers or for Edge Transport service.

**EXAMPLE 1**
This example sets the DelayNotificationTimeout parameter to 13 hours for the Transport service on a Mailbox server named Mailbox01.

```
Set-TransportService Mailbox01 -DelayNotificationTimeout 13:00:00
-MaxDumpsterTime
```

This parameter isn’t used by Microsoft Exchange Server 2013. It’s only used by Microsoft Exchange 2010 servers in a coexistence environment.

`-MessageExpirationTimeout`

Not a parameter of Set-TransportConfig

**SafetyNetHoldTime**

Parameter of Set-TransportConfig

The SafetyNetHoldTime parameter specifies how long a copy of a successfully processed message is retained in Safety Net. Unacknowledged shadow copies of messages auto-expire from Safety Net based on adding the values of the SafetyNetHoldTime parameter and the MessageExpirationTimeout parameter on the Set-TransportService cmdlet.

To specify a value, enter it as a time span: dd.hh:mm:ss where d = days, h = hours, m = minutes, and s = seconds.

The default value is 2.00:00:00 or 2 days.

The ShadowMessageAutoDiscardInterval parameter specifies how long a server retains discarded events for shadow messages. A primary server queues discarded events until queried by the shadow server. However, if the shadow server doesn’t query the primary server for the duration specified in this parameter, the primary server deletes the queued discard events.

To specify a value, enter it as a time span: dd.hh:mm:ss where d = days, h = hours, m = minutes, and s = seconds.

Valid input for this parameter is 00:00:05 to 90.00:00:00. The default value is 2.00:00:00 or 2 days.

**STEPS**

1. Set-TransportConfig. Need to use Safety Net and this is a parameter of Set-TransportConfig

2. SafetyNetHoldTime Need to configure Safety Net

How Safety Net Works

Safety Net can be considered to be having two parts- Shadow Redundancy and Safety Net Redundancy.

While the safety net keeps a redundant copy of a message after it is successfully processed, shadow redundancy keeps a redundant copy of the message which is in transit. All features of shadow redundancy like transport high availability boundary, primary messages, primary servers, shadow messages and shadow servers will be applicable to Safety Net.

The Primary Safety Net is applicable for a Mailbox server that holds the primary message before the Transport service completely processes the message. Once the processing of the message is over, the primary server moves the message to the Primary Safety Net from the active queue on the same server.

The Shadow Safety Net is applicable to the Mailbox server which holds the shadow message. Once the shadow server receives the information that the primary server has successfully processed the primary message, the shadow message is moved to the shadow safety net from the shadow queue on the server. For the Shadow Safety Net operation, shadow redundancy should be enabled, and shadow redundancy is enabled by default in Exchange 2013.

**Set-TransportConfig. Exchange 2013 Help**

**Question 171**

What should you recommend adding?

You are evaluating the planned deployment of the additional Exchange Server 2013 servers.

You need to recommend changes to the DNS records to ensure that email messages are routed to the Detroit site if the servers in the New York site are unavailable.

What should you recommend adding?

A. An MX record that has a preference value of 10 that points to EX4

B. An MX record that has a preference value of 20 that points to EX4

C. An MX record that has a preference value of 10 that points to EX3

D. An MX record that has a preference value of 20 that points to EX3

Correct Answer: B

**Explanation/Reference:**
Configure Exchange to Accept Mail for Multiple Authoritative Domains, Exchange 2013 Help

**DX (mail exchange)** Specifies a mail exchange server for the domain, which allows mail to be delivered to the correct mail servers in the domain.

**Managing DNS Records**

**Question 172**

Which property should you modify by using the Set-OutlookAnywhere cmdlet?

You are testing the planned implementation of Exchange Server 2013. After you begin moving several mailboxes to Exchange Server 2013, you discover that users on the internal network that have been moved are prompted repeatedly for their credentials when they run Microsoft Outlook.

You run the Get-OutlookAnywhere cmdlet on CH-EX4, and receive the following output:

```
CCH-EX4: ~ > Get-OutlookAnywhere
Identity: CAS01rpc (Default Web Site)
-ExternalClientAuthenticationMethod: Ntlm
-InternalClientAuthenticationMethod:NTLM
-InternalHostname:CH-EX4
-IISAuthenticationMethods:
-InternalClientAuthenticationMethod:
-ExternalClientAuthenticationMethod:
-InternalClientAuthenticationMethod:
```

You need to prevent the internal users from being prompted for their credentials when they connect to their mailbox by using Outlook.

Which property should you modify by using the Set-OutlookAnywhere cmdlet?

A. IISAuthenticationMethods

B. InternalHostname

C. ExternalHostname

D. ExternalClientAuthenticationMethod

E. InternalClientAuthenticationMethod

Correct Answer: A

**Explanation/Reference:**

The `IISAuthenticationMethods` parameter specifies the authentication method enabled on the /rpc virtual directory in Internet Information Services (IIS).

Windows Challenge/Response (NTLM) is the authentication protocol used on networks that include systems running the Windows operating system and on stand-alone systems.

**NEED TO CONVERT THE INTERNAL/CLIENTAUTHENTICATIONMETHOD TO BASIS NOT NTLM IN ORDER TO FIX THE ISSUE.**

**USE IISAUTHENTICATIONMETHODS PARAMETER IN ORDER TO ACHIEVE THIS.**

Set-OutlookAnywhere

Use the Set-OutlookAnywhere cmdlet to modify the properties on a computer running Microsoft Exchange Server 2013 enabled for Microsoft Outlook Anywhere.

**EXAMPLE 1**
This example sets the client authentication method to NTLM for the /rpc virtual directory on the Client Access server CAS01.

```
Set-OutlookAnywhere -Identity: CAS01rpc (Default Web Site) -ExternalClientAuthenticationMethod:Ntlm
```

**PARAMETERS**

The `IISAuthenticationMethods` parameter specifies the authentication method enabled on the /rpc virtual directory in Internet Information Services (IIS).

You can set the virtual directory to allow Basic authentication or NTLM authentication.
Alternatively, you can also set the virtual directory to allow both Basic and NTLM authentication. All other authentication methods are disabled.

You may want to enable both Basic and NTLM authentication if you’re using the IIS virtual directory with multiple applications that require different authentication methods.

The InternalHostname parameter specifies the internal hostname for the Outlook Anywhere virtual directory.

The ExternalHostname parameter specifies the external host name to use in the Microsoft Outlook profiles for users enabled for Outlook Anywhere.

The ExternalClientAuthenticationMethod parameter specifies the authentication method used for external client authentication. Possible values include:

- Basic
- Digest
- Ntlm
- Fba
- WindowsIntegrated
- LiveIdFba
- LiveIdBasic
- LiveIdNegotiate
- WSSecurity
- Certificate
- NegoEx
- OAuth
- Adfs
- Kerberos
- Negotiate
- Misconfigured

The InternalClientAuthenticationMethod parameter specifies the authentication method used for internal client authentication. Possible values include:

- Basic
- Digest
- Ntlm
- Fba
- WindowsIntegrated
- LiveIdFba
- LiveIdBasic
- LiveIdNegotiate
- WSSecurity
- Certificate
- NegoEx
- OAuth
- Adfs
- Kerberos
- Negotiate
- Misconfigured

Set-OutlookAnywhere: Exchange 2013 Help

Question 173

Which two tasks should you recommend?

You need to recommend which tasks must be performed to deliver email messages to the Internet if CH-EX2 and CH-EX3 fail to connect to the Internet. The solution must ensure that all queued email is sent.

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

A. Run the retry-queue ch-to-internet command.
B. Create a new Send connector on a server in the Baltimore office.
C. Modify the cost of the CH-to-Internet Send connector.
D. Run the set-sendconnector -identity ch-to-internet -frontendproxyenabled Strue command.
E. Disable the CH-to-Internet Send connector.

Correct Answer: BE

Explanation/Reference:

Explanation:

The Baltimore and Chicago offices have independent Internet connections. Internet connectivity for the Los Angeles office is provided through Chicago. Currently no mail servers in Chicago. Only in Baltimore and Los Angeles.

Once the transition to Exchange Server 2013 in the Chicago office is complete, all mail flow to and from the Internet will be managed centrally through that office by using a Send connector that has the following configurations:

- Connector name: CH-to-Internet
- Address space *

Source servers: CH-EX2, CH-EX3

Cost: 10

When you deploy Exchange 2013, outbound mail flow cannot occur until you configure a Send connector to route outbound mail to the Internet.

NOT A

Use the Retry-Queue cmdlet to force a connection attempt for a queue on a Mailbox server or an Edge Transport server. Will not resolve the issue.

EXAMPLE 1

This example forces a connection attempt for all queues that meet the following criteria:
The queues are holding messages for the domain contoso.com.
The queues have a status of Retry.
The queues are located on the server on which the command is executed.

Retry-Queue -Filter {NextHopDomain -eq "contoso.com" -and Status -eq "Retry"}

NOT C

Modifying the cost will not fix the issue of CH-EX2 and CH-EX3 failing to connect to the Internet.

Cost is used to set the priority of this connector, used when two or more connectors are configured for the same address space. The lower the cost higher the priority.

NOT D

Modifying the send connector will not fix the internet connection from Chicago mail server to the internet.

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

The FrontendProxyEnabled parameter routes outbound messages through the CAS server, where destination specific routing, such as DNS or IP address, is set.
when the parameter is set to $true.

Need to disable the send connector from Chicago to the internet so that when a new send connector on the Baltimore server is created, email can be sent to the internet.

**Send Connectors:** Exchange 2013 Help

**Question 174**

Which three actions should you perform?

**DRAG DROP**

You need to create and configure a hierarchical address book (HAB) named Litware to reflect the company’s organizational chart.

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.

Select and Place:

Correct Answer:

Explanation/Reference:

(Note: Example:

For this example, an OU called HAB will be created for the HAB. The name of the domain for the Exchange 2013 organization is Contoso.com, and Contoso,Ltd will be the name of the top-level organization in the hierarchy (the root organization).

Create an OU named HAB in the Contoso organization. You can use Active Directory Users and Computers or type the following at a command prompt.

Alternatively, you can use an existing OU in your Exchange forest.

(Box 1) Create the root distribution group Contoso,Ltd for the HAB.

(Box 2) Designate Contoso,Ltd as the root organization for the HAB.

Set-OrganizationConfig -HierarchicalAddressBookRoot "Contoso,Ltd"

Create distribution groups for the other tiers in the HAB.

Designate each of the groups as members of the HAB. For this example, you would designate the following groups as being hierarchical groups: Contoso,Ltd, Corporate Office, Product Support Organization, Sales & Marketing Organization, Human Resources, Accounting Group, and Administration Group. This example designates the distribution group Contoso,Ltd as a member of the HAB.

Set-Group -Identity "Contoso,Ltd" -IsHierarchicalGroup $true

Add each of the subordinate groups as members of the root organization.

Add each of the groups that are subordinate to the distribution group Corporate Office as members of the HAB.

Add users to the groups in the HAB.

(Box 1) Create a distribution group that will be used for the root organization (top-level tier). If desired, you can use an existing organizational unit in your Exchange forest for the distribution group.

(Box 2) Create a distribution group for the child tier and designate them as members of the HAB.

(Box 3) Add the groups as members of the HAB.

Set the SeniorityIndex parameter for users in the HAB.

Set the SeniorityIndex parameter for groups in the HAB.

Configure hierarchical address books

The general steps are as follows:

(Box 1, Box 2) Create a distribution group that will be used for the root organization (top-level tier). If desired, you can use an existing organizational unit in your Exchange forest for the distribution group.

Create distribution groups for the child tiers and designate them as members of the HAB.

Add organization members. Modify the SeniorityIndex parameter of these groups so they're listed in the proper hierarchical order within the root organization.

Add users to the groups in the HAB.

(Box 3) Set the SeniorityIndex parameter for users in the HAB.

Set-Group -Identity "Contoso,Ltd" -IsHierarchicalGroup $true

Set-OrganizationConfig: Exchange 2013 Help

Set-Group: Exchange 2013 Help

**Question 175**

Which tools should you identify?

**DRAG DROP**

You are planning the upgrade to Exchange Server 2013.

You plan to perform the following tasks:

Identify the number of email messages sent and received by the users in the current Exchange Server organization.

Identify how many IOps are required to provide adequate access to mailboxes for all of the users in the planned organization.

Validate that all of the planned servers will meet the IOPS requirements of the planned organization.

You need to identify which tool must be used to achieve each task.

Which tools should you identify?

To answer, drag the appropriate tool to the correct task in the answer area. Each tool 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.

Select and Place:

Correct Answer:

Explanation/Reference:

Exchange Mailbox Server Role Requirements Calculator

Exchange 2010 Product


(Exchange 2013 Server Role Requirements Calculator

Yes, this is no longer a Mailbox server role calculator; this calculator includes recommendations on sizing Client Access servers too!

After you have determined the design you would like to implement, you can follow the steps in the Exchange 2010 Mailbox Server Role Design Example article within the Exchange 2010 Online Help to calculate your solution’s CPU, memory, and storage requirements, or you can leverage the Exchange 2010 Mailbox Server Role Requirements Calculator. The calculator is broken out into the following sections (worksheets):

Input

Role Requirements
Microsoft Exchange Server Jetstress 2010

Important:
Jetstress testing should be performed before you install Exchange on the server.

Microsoft Exchange Server Profile Analyzer

The Microsoft Exchange Server Profile Analyzer tool lets administrators collect estimated statistical information from a single mailbox store or across an Exchange organization. You can use the collected data to perform the following operations:
- Analyze the performance and health of a mailbox server.
- Improve capacity planning models.
- Improve testing methodologies and tools.
- Improve future client and server products.

STEPS
1. Microsoft Exchange Server Profile analyzer collects statistical information from a single mailbox store or across an Exchange organization.
2. Exchange Mailbox Server Role Requirements Calculator makes recommendations based on inputs provided.

Microsoft Exchange Server Jetstress 2010
Jetstress helps verify disk performance by simulating Exchange disk I/O load. You can use Jetstress 2010 to verify the performance and stability of a disk subsystem prior to putting an Exchange 2010 server into production.

You need to verify the performance and stability of a disk subsystem prior to putting an Exchange 2010 server into production.

Correct Answer: D

Explanation/Reference:

Question 176
What should you do next?
You have successfully completed Jetstress testing and verified that your Exchange 2010 disk subsystem is adequately sized to meet the performance criteria you establish.

Correct Answer: A

Explanation/Reference:
Correct Answer: BID
Explanation/Reference:
Explanation:
Internal Relay Domain
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.

When you configure an internal relay domain, some or all of the recipients in this domain don’t have mailboxes in this Exchange organization. Mail from the Internet is relayed for this domain through Transport servers in this Exchange organization. This configuration is used in the scenarios that are described in this section. An organization may have to share the same SMTP address space between two or more different messaging systems. For example, you may have to share the SMTP address space between Exchange and a third-party messaging system, or between Exchange environments that are configured in different Active Directory forests. In these scenarios, users in each email system have the same domain suffix as part of their email addresses.

To support these scenarios, you need to create an accepted domain that’s configured as an internal relay domain. You also need to add a Send connector that’s sourced on a Mailbox server and configured to send email to the shared address space. If an accepted domain is configured as authoritative and a recipient isn’t found in Active Directory, a non-delivery report (NDR) is returned to the sender. The accepted domain that’s configured as an internal relay domain first tries to deliver to a recipient in the Exchange organization. If the recipient isn’t found, the message is routed to the Send connector that has the closest address space match.

If an organization contains more than one forest and has configured global address list (GAL) synchronization, the SMTP domain for one forest may be configured as an internal relay domain in a second forest. Messages from the Internet that are addressed to recipients in internal relay domains are relayed to the Mailbox servers in the same organization. The receiving Mailbox servers then route the messages to the Mailbox servers in the recipient forest. You configure the SMTP domain as an internal relay domain to make sure that email that’s addressed to that domain is accepted by the Exchange organization. The connector configuration of your organization determines how messages are routed.

B
An accepted domain is any SMTP namespace for which a Microsoft Exchange Server 2013 organization sends or receives email. Accepted domains include those domains for which the Exchange organization is authoritative. An Exchange organization is authoritative where it handles mail delivery for recipients in the accepted domain. Accepted domains also include domains for which the Exchange organization receives mail and then relays it to an email server that’s outside the organization for delivery to the recipient.

D
2nd part of establishing an internal relay domain is to establish a Send Connector that is configured to point to the other organization’s mail servers (a datum)

EXAMPLE 1
This example creates a non-default user throttling policy that can be associated with specific users. Any parameters that you omit inherit the values from the default throttling policy GlobalThrottlingPolicy.

New-ThrottlingPolicy
Use the New-ThrottlingPolicy cmdlet to create a non-default user throttling policy.

EXAMPLE 1
This example creates a non-default user throttling policy that can be associated with specific users. Any parameters that you omit inherit the values from the default throttling policy GlobalThrottlingPolicy.

New-ThrottlingPolicy
-Name ITUserPolicy
-EwsMaxConcurrency 4
-ThrottlingPolicyScope Regular
-ThrottlingPolicyName ITStaffPolicy

Explanation:
Correct Answer: BD
Explanation/Reference:
Explanation:
New-ThrottlingPolicy
Use the New-ThrottlingPolicy cmdlet to create a non-default user throttling policy.

EXAMPLE 1
This example creates a non-default user throttling policy that can be associated with specific users. Any parameters that you omit inherit the values from the default throttling policy GlobalThrottlingPolicy.

After you create this policy, you can associate it with specific users.

New-ThrottlingPolicy
-Name ITUserPolicy
-EwsMaxConcurrency 4
-ThrottlingPolicyScope Regular

The ThrottlingPolicyScope parameter specifies the scope of the throttling policy. You can use the following values.

- Global
- Organization
- Regular

Organization Specifies a custom policy that applies to all users in your organization.

Regular Specifies a custom policy that applies to specific users.

Organization Specific The actual policy, which is generated by Exchange, applies to specific users.

Global Reserved for the default throttling policy.

C
Need to establish a New Throttling policy to limit the Exchange ActiveSync connections and that has a regular scope to associate with specific users.

D
Use the Set-ThrottlingPolicy cmdlet to associate a throttling policy with a specific object. The object can be a user with a mailbox, a user without a mailbox, a contact, or a computer account.

EXAMPLE 1
This example associates a user with a user name of tonymsmith to the throttling policy ITStaffPolicy that has higher limits.

Set-ThrottlingPolicy
-Identity tonymsmith
-ThrottlingPolicy ITStaffPolicy

Note A
Need a regular scope

Note B
Need a regular scope

Note E
Need to associate the new throttling policy with respective users.

Use the Set-ThrottlingPolicy cmdlet to modify the settings for a user throttling policy.

EXAMPLE 1
This example modifies a throttling policy so that users associated with this policy can have a maximum of four concurrent requests running in Exchange Web Services.

Sa = Get-ThrottlingPolicy RemoteSiteUserPolicy $a | Set-ThrottlingPolicy -EwsMaxConcurrency 4

Note F
Need to create a new throttling policy

Set-ThrottlingPolicy

Note A
Need a regular scope

Note B
Need a regular scope

Note E
Need to associate the new throttling policy with respective users.

Use the Set-ThrottlingPolicy cmdlet to modify the settings for a user throttling policy.

EXAMPLE 1
This example modifies a throttling policy so that users associated with this policy can have a maximum of four concurrent requests running in Exchange Web Services.
Question 179
What are three possible ways to achieve the goal?
You need to recommend a temporary solution to reroute all of the outbound email messages through the Miami mail appliance during the planned replacement of the New York mail appliance.

What are three possible ways to achieve the goal? (Each correct answer presents a complete solution. Choose three.)
A. Modify the value of the SmartHost of the Send connector in the New York office.
B. Decrease the cost of the Send connector in the Miami office.
C. Increase the cost of the Send connector in the New York office.
D. Increase the cost of the Send connector in the Miami office.
E. Modify the value of the SmartHost of the Send connector in the Miami office.
F. Disable the Send connector in the Miami office.

Correct Answer: ACF
Explanation/Reference:

Question 180
Which DAG design should you deploy?

You need to ensure that all of the users in the New York and Atlanta offices can access their mailbox if the WAN link fails.

Which DAG design should you deploy?
A. Modify the value of the SmartHost of the Send connector in the New York office.
B. Enhance the cost of the Send connector in the Miami office.
C. Increase the cost of the Send connector in the New York office.
D. Increase the cost of the Send connector in the Miami office.
E. Modify the value of the SmartHost of the Send connector in the Miami office.
F. Disable the Send connector in the New York office.

Correct Answer: CDF
Explanation/Reference:

Question 181
Which node should you install the root CA certificate?

You need to recommend a temporary solution to reroute all of the outbound email messages through the Miami mail appliance during the planned replacement of the New York mail appliance.

What are three possible ways to achieve the goal? (Each correct answer presents a complete solution. Choose three.)
A. Modify the value of the SmartHost of the Send connector in the New York office.
B. Decrease the cost of the Send connector in the Miami office.
C. Increase the cost of the Send connector in the New York office.
D. Increase the cost of the Send connector in the Miami office.
E.Modify the value of the SmartHost of the Send connector in the Miami office.
F. Disable the Send connector in the New York office.

Correct Answer: CDF
Explanation/Reference:
You discover that one of the Client Access servers in the New York office does not trust the standalone CA. You need to ensure that all of the users who have Windows Phone devices can connect successfully to their mailbox.

In which node should you install the root CA certificate?

To answer, select the appropriate node in the answer area.

Hot Area:

Correct Answer:

Explanation/Reference:

Explanation:

Root certificate
If you’re using a self-signed certificate or a certificate authority (CA)-issued certificate that is not preinstalled in the Trusted Root Certification Authorities store of your device, you’ll have to manually install it before your device can work with a Secure Sockets Layer (SSL)-enabled server.

Trusted Root Certification Authorities
Because the certificate is signed, Internet Explorer will automatically install it in the Trusted root Certificate Authority list.

If you use a certification authority (CA) to issue smart card login or domain controller certificates, you must add the root certificate to the Trusted Root Certification Authorities group policy in Active Directory.

If you’re using a self-signed certificate or a certificate authority (CA)-issued certificate that is not preinstalled in the Trusted Root Certification Authorities store of your device, you’ll have to manually install it with a Secure Sockets Layer (SSL)-enabled server.


Install a certificate on a Windows or a Windows Mobile device

Install a certificate on a Windows device

Steps:
Browse to the location where you have exported the certificate to, then double-click the certificate file.

The Certificate window appears, click Install Certificate.

The Certificate Import Wizard window appears, click Next, on the next page choose the Place all certificate in the following store option, and click Browse.

The Select Certificate Store window appears, select Trusted Root Certificate Authorities, and click OK.

Click Next and Finish in the next two screens to close the wizard and complete the process.

Click Yes on the security warning to install the certificate.

Click OK to dismiss the Certificate window.

One problem with self-signed and PKI-based certificates is that, because the certificate is not automatically trusted by the client computer or mobile device, you must make sure that you import the certificate into the trusted root certificate store on client computers and devices.

Digital Certificates and SSL, Exchange 2013 Help

Installing a root certificate

Question 182
What should you recommend?

What should you recommend?

You need to recommend changes to the network to ensure that you can deploy the planned Exchange Server 2013 infrastructure.

A. Transfer of the FSMO roles to a domain controller in the Chicago office.
B. Change the forest functional level.
C. Change the domain functional level.
D. Change the operating system on one of the domain controllers in the Chicago office.

Correct Answer: D

Explanation/Reference:

Explanation:

DIFFICULT QUESTION

FSMO (Flexible Single Master Operations)

In a forest, there are five FSMO roles that are assigned to one or more domain controllers. The five FSMO roles are:

Schema Master:
The schema master domain controller controls all updates and modifications to the schema. Once the Schema update is complete, it is replicated from the schema master to all other DCs in the directory.

To update the schema of a forest, you must have access to the schema master. There can be only one schema master in the whole forest.

Domain naming master:
The domain naming master domain controller controls the addition or removal of domains in the forest. This DC is the only one that can add or remove a domain from the directory. It can also self-propagate cross references to domains in external directories. There can be only one domain naming master in the whole forest.

Infrastructure Master:
When an object in one domain is referenced by another object in another domain, it represents the reference by the GUID, the SID (for references to security principals), and the DN of the object being referenced. The infrastructure FSMO role holder is the DC responsible for updating an object’s SID and distinguished name in a cross-domain object reference. At any one time, there can be only one domain controller acting as the infrastructure master in each domain.

Note: The Infrastructure Master (IM) role should be held by a domain controller that is not a Global Catalog server (GC). If the Infrastructure Master runs on a Global Catalog server, it will stop updating object information because it does not contain any references to objects that it does not hold. This is because a Global Catalog server maintains a partial replica of every object in the forest. As a result, cross-domain object references in that domain will not be updated and a warning to that effect will be logged on that DC’s event log. If all the domain controllers in a domain also host the global catalog, all the domain controllers have the current data, and it is not important which domain controller holds the infrastructure master role.

Relative ID (RID) Master:
The RID master is responsible for processing RID pool requests from all domain controllers in a particular domain. When a DC creates a security principal object such as a user or group, it attaches a unique Security ID (SID) to the object. This SID consists of a domain SID (the same for all SIDs created in a domain), and a relative ID (RID) that is unique for each security principal SID created in the domain. Each DC in a domain is allocated a pool of RIDs that it is allowed to assign to the security principals it creates. When a DC’s allocated RID pool falls below a threshold, that DC issues a request for additional RIDs to the domain’s RID master.

The domain RID master responds to the request by retrieving RIDs from the domain’s unallocated RID pool and assigns them to the pool of the requesting DC. At any one time, there can be only one domain controller acting as the RID master in the domain.

PDC Emulator:
The PDC emulator is necessary to synchronize time in an enterprise.

The PDC emulator of a domain is authoritative for the domain. The PDC emulator at the root of the forest becomes authoritative for the enterprise, and should be configured to gather the time from an external source.

All PDC FSMO role holders follow the hierarchy of domains in the selection of their in-bound time partner.

NOTA
All of the FSMO roles are located on a domain controller in the Baltimore Office. All of the domain controllers are configured as a global catalog server.

No need to transfer all of these roles to the Chicago domain controller as the question suggests.

NOTB
Apparently no need to change the forest functional level

Forest functional levels enable features across all the domains in your forest. The following table lists the forest functional levels and their corresponding supported domain controllers.

NOT C
Apparently no need to change the domain functional level
For all domain controllers to function accordingly in the domain the domain functional level would have to be set to Windows Server 2003
All domain controllers in the Chicago office run Windows Server 2003 Service Pack 1. (SP1)
All domain controllers in the Los Angeles office run Windows Server 2008 R2.
All domain controllers in the Baltimore office run Windows Server 2012
Domain functional levels
Domain functionality enables features that affect the entire domain and that domain only. The following table lists the domain functional levels and their corresponding supported domain controllers:

Mixture of exchange 2007,2010 and 2013 environment
Currently all of the chicago domain controllers are 2003 SP1
Need to upgrade a chicago domain controller which will house Exchange 2013
Exchange 2013 System Requirements: Exchange 2013 Help

Question 183
Which names should you identify?
HOTSPOT
You need to identify which names must be used as the URLs of each virtual directory on the planned Exchange Server 2013 servers.
Which names should you identify?
To answer, configure the appropriate name for each server in the answer area.
Hot Area:

Correct Answer:

Explanation/Reference:
Explanation:
CH-EX2 and CH-EX3
Domain name of litwareinc.com
Use CH-EX2.domain name and CH-EX3.domain name for the mailbox server virtual directories:
CH-EX4 and CH-EX5
Hardware load balancer connects to the various Client Access Servers. (CH-EX4 and CH-EX5)
Hence use client.litwareinc.com for the Client Access Servers as All client connections to the Exchange Server organization will be routed though a hardware load balancer.
The name client.litwareinc.com will point to the virtual IP address of the hardware load balancer.

Load Balancing: Exchange 2013 Help

Question 184
Which two parameters should you modify by using the Set-SendConnector cmdlet?
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

Correct Answer: BE

Explanation/Reference:
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" -AtMaxMessageSize 10MB -ConnectionInactivityTimeOut 0:00:15:00

PARAMETERS

Require tls
The Require-TLS 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 Exchange 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 TlDomain parameter. If no domain is specified in the TlDomain parameter, the FQDN on the certificate is compared against the recipient’s domain.
- Smarthostauthmechanism
  - 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 $true.
  - 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.

NOT TLSAUTHLEVEL
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.

TLS Functionality and Related Terminology: Exchange 2013 Help

Question 185
Which script should you recommend?
You need to recommend which script the administrators must run to create the reports required to meet the technical requirements.
Which script should you recommend?
To answer, select the appropriate script in the answer area.

Hot Area: ☑

Correct Answer:

Explanation/Reference:
Explanation:
CollectOverMetrics.ps1 script
CollectOverMetrics.ps1 is a script that is used to collect metrics related to database operations over a specific time period. Each operation by the script records the following information:
- Identity of the database.
- Time at which the operation began and ended.
- Servers on which the database was mounted at the start and finish of the operation.
- Reason for the operation.
- Whether the operation was successful, and if the operation failed, the error details.
- The script writes this information to a .csv file with one operation per row. It writes a separate .csv file for each DAG.
- The script supports parameters that allow you to customize the script’s behavior and output. For example, the results can be restricted to a specified subset by using the Database and DgnReportFilter parameters.
- Only the operations that match these filters will be included in the summary HTML report.

Monitoring Database Availability Groups: Exchange 2013 Help

Question 186
Which recovery solution should you recommend?
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.

Correct Answer: A
Explanation/Reference:
Restore Data Using a Recovery Database
Create a Recovery Database

Question 187
Which three actions should you recommend performing in sequence?
You need to recommend to a solution to deploy the Outlook app.
Which three actions should you recommend performing in sequence?
Select and Place:

Correct Answer:

Explanation/Reference:
Install or Remove Apps for Outlook for Your Organization
Get-App: Exchange 2013 Help
Set-App: Exchange 2013 Help

Question 188
Which business requirement should you identify?
You need to identify which business requirement will be met by implementing the planned hardware load balancer.
Which business requirement should you identify?
A. Minimize the hardware costs required for a load balancing solution.
B. Minimize the software costs required for a load balancing solution.
C. Minimize user interruptions if a service fails on a Client Access server.
D. Minimize user interruptions if a service fails on a Mailbox server.

Correct Answer: C
Explanation/Reference:
Explanation:
NOT A
Introducing a load balancing solution will not minimize hardware costs
NOT B
Introducing a hardware load balancing solution will not minimize software costs
NOT D
A hardware load balancer connects to the Client Access servers not the Mailbox servers.
C
A hardware load balancer connects to the Client Access servers not the Mailbox servers AND is designed to minimize user interruptions
Understanding Load Balancing in Exchange 2010: Exchange 2010 Help

Question 189
What should you recommend?
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.

Correct Answer: B
Explanation/Reference:
Explanation:
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 A C
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).
Prepare Active Directory and Domains: Exchange 2013 Help

Question 190
Which three actions should you perform in fabrikam.com?
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.
Correct Answer: BDF
Explanation/Reference:
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 transfers 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
Edge is in the perimeter network and the send connector needs to be created on a mailbox server
NOT E
Set-TransportServer cmdlet. 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 servers 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.
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 specified, 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 the 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.
Send Connector 1 Exchange 2013 Help

Question 191
Which three actions should you include in the recommendation?
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.
Select and Place:

Correct Answer:

Explanation/Reference:

Configure Edge Transport Server Using Cloned Configuration
You can use the provided Shell scripts to duplicate the configuration of a computer that has the Microsoft Exchange Server 2010 Edge Transport server role installed.

This process is referred to as cloned configuration. Cloned configuration is the practice of deploying new Edge Transport servers based on the configuration information from a previously configured source server. The configuration information from the previously configured source server is copied and exported to an XML file, which is then imported to the target server. Edge Transport server configuration information is stored in Active Directory Lightweight Directory Services (AD LDS) and isn’t replicated among multiple Edge Transport servers. By using cloned configuration, you can make sure that every Edge Transport server that’s deployed in the perimeter network is operating by using the same configuration.

These scripts are located in the scripts folder in your Exchange installation folder. The default location for this folder is C:\Program Files\Microsoft Exchange ServerScripts.

exportedgeconfig.ps1
This script 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 XML file to see whether the server-specific export settings are valid for the target server. If settings have to be modified, the script writes the invalid settings to an answer file that you modify to specify the target server information that’s used during the import configuration step.

During the import configuration step, the script imports all user-configured settings and data that’s stored in the intermediate XML file that was created by the ExportEdgeConfig.ps1 script.

Send Connectors 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.

Edge Subscription
The Edge Subscriptions management role enables administrators to manage edge synchronization and subscription configuration between Microsoft Exchange Server 2010 Edge Transport servers and Microsoft Exchange Server 2013 Mailbox servers in an organization.

Edge Transport servers deployed with Microsoft Exchange are deployed in an organization’s on-premises perimeter network. The Edge Subscription file is used in the EdgeSync process, and it contains information about the credentials that are used during the LDAP communication process. These credentials are used to authenticate and authorize the connection between Active Directory Lightweight Directory Service (AD LDS) and Active Directory during replication.

Although creating an Edge Subscription is optional, subscribing an Edge Transport server to the Exchange organization provides a simpler management experience for the administrator and enhances the available antispam features. You must create an Edge Subscription if you plan to use recipient lookup or safelist aggregation, or if you plan to help secure SMTP communications with partner domains by using mutual Transport Layer Security (TLS).

Edge2 is the new edge transport server therefore have to create a new edge subscription for Edge2.
Cloned configuration doesn’t duplicate the Edge Subscription settings of a server. The certificates used by the Microsoft Exchange EdgeSync service aren’t cloned. You must run the EdgeSync process separately for each Edge Transport server. The Microsoft Exchange EdgeSync service overwrites any settings included in both cloned configuration information and in EdgeSync replication information.

After an Edge Transport server has been subscribed to the Exchange organization, the Microsoft Exchange EdgeSync service replicates data from the Active Directory directory service to the Active Directory Application Mode (ADAM) directory service instance on the Edge Transport server. The replicated data lets you implement a wider range of anti-spam features and enables domain security functionality. The EdgeSync synchronization process also lets you configure Send connectors and configuration objects that are common to both the Exchange organization and the Edge Transport server on a Hub Transport server and then have that data automatically populated to ADAM. The EdgeSync synchronization process keeps the data up to date by performing scheduled synchronization.

However should it be created 1st or last in the answer selection.

The Microsoft Exchange EdgeSync service overwrites any settings included in both cloned configuration information and in EdgeSync replication information.

Therefore it should be last on the answer list.

Configure Edge Transport Server Using Cloned Configuration: Exchange 2013 Help

Question 192
Which type of group should you recommend?
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

Correct Answer: A

Explanation/Reference:
Explanation:
There are two types of groups that can be used to distribute messages:
Mail-enabled universal distribution groups (also called distribution groups) can be used only to distribute messages.

Mail-enabled universal security groups (also called security groups) can be used to distribute messages as well as to grant access permissions to resources in Active Directory. For more information, see Manage Mail-Enabled Security Groups. A mail-enabled security group is an Active Directory universal security group object that can be used to assign access permissions to resources in Active Directory and can also be used to distribute messages.

It’s important to note the terminology differences between Active Directory and Exchange. In Active Directory, a distribution group refers to any group that doesn’t have a security context, whether it’s mail-enabled or not. In contrast, in Exchange, all mail-enabled groups are referred to as distribution groups, whether they have a security context.

Dynamic Distribution Groups
Unlike regular distribution groups that contain a defined set of members, the membership list for dynamic distribution groups is calculated each time a message is sent to the group, based on the filters and conditions that you define. When an email message is sent to a dynamic distribution group, it’s delivered to all recipients in the organization that match the criteria defined for that group.

Manage Distribution Groups: Exchange Online Help

Question 193
Which two tasks should you recommend?
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.

Correct Answer: AD

An administrator recommends removing EDGE1 from the implementation plan and adding a new Client Access server named CAS-8 instead. Which anti-spam feature should you identify?

2. DAGNET2 must be MapiAccessEnabled to fulfill the requirements

1. DAGNET1 must be ReplicationEnabled

STEPS

- servers and not use a replication network for a server that is a member of the same DAG located across a WAN connection.

- creating a replication network since both networks would be sharing the same bandwidth.

- This often makes it difficult to use a replication network when building a DAG across multiple locations. The reason being that multiple WAN connections would be necessary in order to separate the MAPI traffic from the replication traffic. (After all, creating multiple VLANs within a single WAN connection defeats the purpose of creating a replication network since both networks would be sharing the same bandwidth.)

- Each server within a DAG must have the same number of replication networks. This means that you cannot use a replication network between two local Mailbox servers and route a replication network for a server that is a member of the same DAG located across a WAN connection.

- DAGNET1 must be ReplicationEnabled

- DAGNET2 must be MapiAccessEnabled to fulfill the requirements

Managing Database Availability Groups: Exchange 2013 Help

Question 194

Which configurations should you recommend?

HOTSPOT

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.

Hot Area:

Correct Answer:

Explanation/Reference:

Explanation:

DAG NETWORKS

A DAG network is a collection of one or more subnets used for either replication traffic or MAPI traffic. Each DAG contains a maximum of one MAPI network and zero or more replication networks.

In a single network adapter configuration, the network is used for both MAPI and replication traffic.

Although a single network adapter and path is supported, we recommend that each DAG have a minimum of two DAG networks. In a two-network configuration, one network is typically dedicated for replication traffic, and the other network is used primarily for MAPI traffic. You can also add network adapters to each DAG member and configure additional DAG networks as replication networks.

MAPI

Messaging Application Programming Interface (MAPI) is a messaging architecture and a Component Object Model based API for Microsoft Windows. MAPI allows client programs to become (e-mail) messaging-enabled, -aware, or -based by calling MAPI subsystem routines that interface with certain messaging servers. While MAPI is designed to be independent of the protocol, it is usually used with MAPI/RPC, the proprietary protocol that Microsoft Outlook uses to communicate with Microsoft Exchange.

Simple MAPI is a subset of 12 functions which enable developers to add basic messaging functionality. Extended MAPI allows complete control over the messaging system on the client computer, creation and management of messages, management of the client mailbox, service providers, and so forth. Simple MAPI ships with Microsoft Windows as part of Outlook Express/Windows Mail while the full Extended MAPI ships with Office Outlook and Exchange.

In addition to the Extended MAPI client interface, programming calls can be made indirectly through the Simple MAPI API client interface, through the Common Messaging Calls (CMC) API client interface, or by the object-based CDO Library Interface. These three methods are easier to use and designed for less complex messaging-enabled and -aware applications. (Simple MAPI and CMC were removed from Exchange 2003.)

CONFIGURING DAG NETWORKS

There are several items to keep in mind when configuring DAG networks:

- There must be one MAPI network. There is not going to be a replication network, the MAPI network will be used for replication.
- Replication networks are optional. There can be multiple replication networks.
- If the replication network fails, the DAG will fail back to the MAPI network for replication.
- If you want to create a replication network, it must reside on a different subnet than the MAPI network.
- This often makes it difficult to use a replication network when building a DAG across multiple locations. The reason being that multiple WAN connections would be necessary in order to separate the MAPI traffic from the replication traffic. (After all, creating multiple VLANs within a single WAN connection defeats the purpose of creating a replication network since both networks would be sharing the same bandwidth.)
- Each server within a DAG must have the same number of replication networks. This means that you cannot use a replication network between two local Mailbox servers and route a replication network for a server that is a member of the same DAG located across a WAN connection.

STEPS

1. DAGNET1 must be ReplicationEnabled
2. DAGNET2 must be MapiAccessEnabled to fulfill the requirements

Managing Database Availability Groups: Exchange 2013 Help

Question 195

Which anti-spam feature should you identify?

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

Correct Answer: A
Explanation/Reference:
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, see <fwlink to 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, see <fwlink to http://technet.microsoft.com/library/bb124399(v=exchg.141).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 wasn’t the only anti-spam agent that wasn’t available. In Exchange 2013, when you enable the anti-spam 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 found, the message isn’t permitted to enter the organization.
Recipient filtering compares the message recipients on the RCPT TO: SMTP command to an administrator defined Recipient Block list. If a match is inside the organization. For more information, Recipient Filter agent
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 B C D
Only need to identify 1 and this is connection filtering.