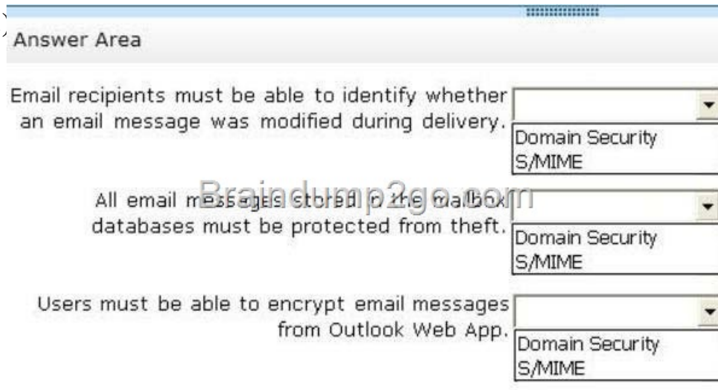
2014 Latest Microsoft 70-342 Dump Free Download(41-50)!

QUESTION 41You are evaluating the deployment of two additional Client Access servers and a hardware load balancer in the London office.You need to recommend changes to the Client Access namespace design to meet the site resiliency requirements. Which three actions should you recommend? (Each correct answer presents part of the solution. Choose three.) A. In the London office, set mail.proseware.com as the external host name for Outlook Anywhere. In the New York office, set mail.proseware.com as the external host name for Outlook Anywhere.B. In the London office, set ionmail.proseware.com as the internal host name for Outlook Anywhere. In the New York office, set nycmail.proseware.com as the internal host name for Outlook Anywhere.C. Use DNS round robin for the external host name for Outlook Anywhere.D. Use DNS round robin for the internal host name for Outlook Anywhere.E. In the London office, set nycmail.proseware.com as the external host name for Outlook Anywhere. In the New York office, set ionmail.proseware.com as the external host name for Outlook Anywhere.F. In the London office, set mail.proseware.com as the internal host name for Outlook Anywhere. In the New York office, set mail.proseware.com as the internal host name for Outlook Anywhere. Answer: ABCExplanation:A: Use mail.proseware.com as the external host name for Outlook Anywhere at both locations.B: Use internal names (lonmail.proseware.com and nycmail.proseware.com) as the internal host name for Outlook Anywhere in London and New York respectively.C: To meet the resiliency requirement use the external host name (mail.proseware.com) for DNS round robin for Outlook anywhere.* From scenario:/ Users connect to mail.proseware.com for Microsoft Outlook and Outlook Web App services. Mail.proseware.com resolves to an IP address on a hardware load balancer./ All Outlook Anywhere users are enabled for Cached Exchange Mode./ Proseware has two main offices located in New York and London./Site Resiliency Requirements- All mailboxes must be available if a single site becomes unavailable. The solution must not require administrator intervention.- User traffic on the WAN links must be minimized.* Split DNS for Exchange Server 2013Split DNS allows your internal clients to receive a different answer to their DNS lookups than an external client would receive. In effect you have your Exchange namespace hosted on your internal DNS server, with records configured to point to internal IP addresses. QUESTION 42You need to recommend a solution to meet the technical requirements for redundancy during email delivery.Which cmdlet should you include in the recommendation? A. Set-FrontendTransportServiceB. Set-TransportConfigC. Set-MailboxTransportServiceD. Set-TransportService Answer: BExplanation: QUESTION 43Hotspot QuestionYou need to recommend which technology can be used to meet each email security requirement.What should you recommend? (To answer, select the appropriate technology for each requirement in the answer area.)



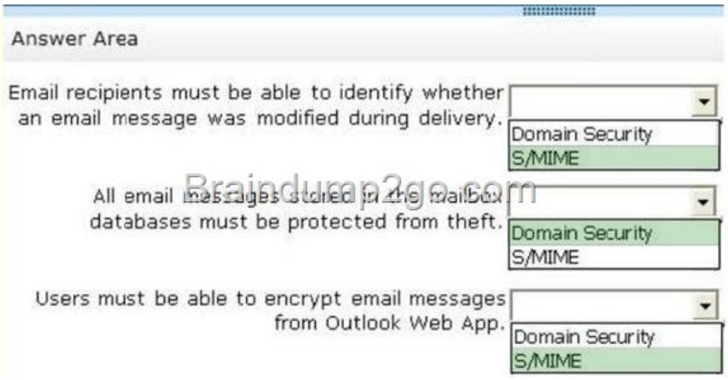
Answer Area

Email recipients must be able to identify whether an email message was modified during delivery.
Domain Security
S/MIME

All email messages stored in the mailbox databases must be protected from theft.
Domain Security
S/MIME

Users must be able to encrypt email messages from Outlook Web App.
Domain Security
S/MIME

Answer:



Answer Area

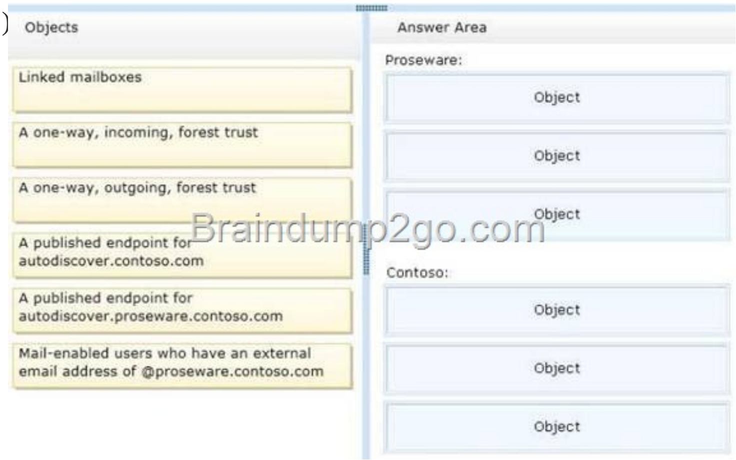
Email recipients must be able to identify whether an email message was modified during delivery.
Domain Security
[✓ S/MIME]

All email messages stored in the mailbox databases must be protected from theft.
[✓ Domain Security]
S/MIME

Users must be able to encrypt email messages from Outlook Web App.
Domain Security
[✓ S/MIME]

QUESTION 44Drag and Drop QuestionYou need to recommend a solution to support the planned changes for the integration of the

Exchange Server organizations of Contoso and Proseware.What should you configure in each organization? (To answer, drag the appropriate objects to the correct forests. 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.)



Objects

- Linked mailboxes
- A one-way, incoming, forest trust
- A one-way, outgoing, forest trust
- A published endpoint for autodiscover.contoso.com
- A published endpoint for autodiscover.proseware.contoso.com
- Mail-enabled users who have an external email address of @proseware.contoso.com

Answer Area

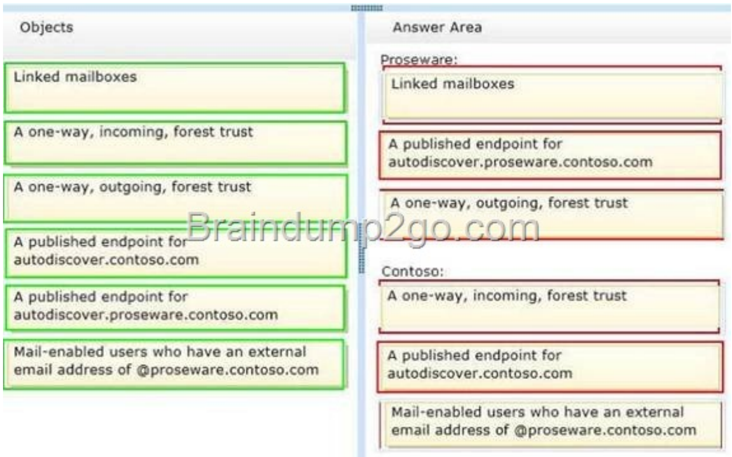
Proseware:

- Object
- Object
- Object

Contoso:

- Object
- Object
- Object

Answer:



Objects

- Linked mailboxes
- A one-way, incoming, forest trust
- A one-way, outgoing, forest trust
- A published endpoint for autodiscover.contoso.com
- A published endpoint for autodiscover.proseware.contoso.com
- Mail-enabled users who have an external email address of @proseware.contoso.com

Answer Area

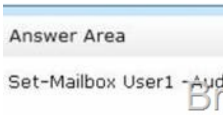
Proseware:

- Linked mailboxes
- A published endpoint for autodiscover.proseware.contoso.com
- A one-way, outgoing, forest trust

Contoso:

- A one-way, incoming, forest trust
- A published endpoint for autodiscover.contoso.com
- Mail-enabled users who have an external email address of @proseware.contoso.com

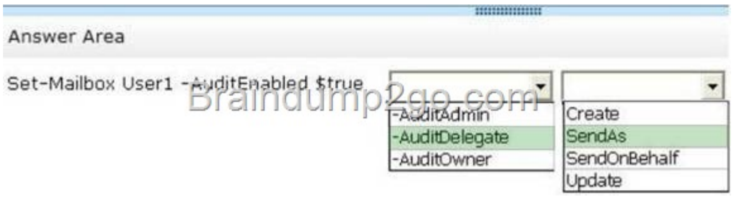
QUESTION 45You need to resolve the content filtering issue for the Office 365 pilot users.What should you do? A. Run the Set-Mailbox cmdlet and specify the -MaxBiockedSenders and the -MicrosoftOnlineServicesID parameters.B. Run the Microsoft Online Services Directory Synchronization Configuration Wizard and select Enable Exchange hybrid deployment.C. Modify the default content filter policy from the Office 365 portal.D. Run the Set-Mailbox cmdlet and specify the -MaxSafeSenders and the -MicrosoftOnlineServicesIDparameters. Answer: B QUESTION 46Hotspot QuestionYou need to recommend a solution to audit the issue of User1.Which command should you recommend? (To answer, select the appropriate options in the answer area.)



Answer Area

Set-Mailbox User1 -Aud

Answer:



Answer Area

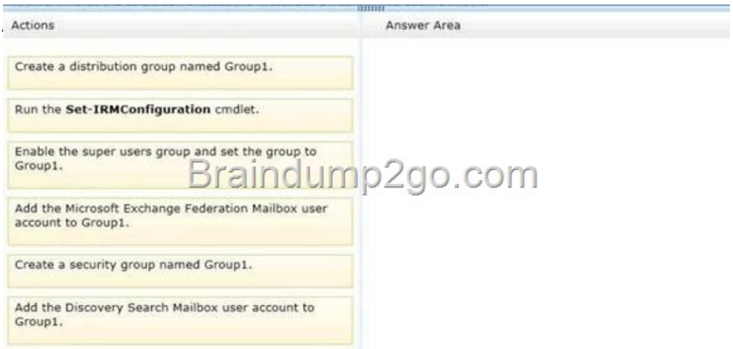
Set-Mailbox User1 -AuditEnabled $true

-AuditAdmin
[✓ -AuditDelegate]
-AuditOwner

Create
[✓ SendAs]
SendOnBehalf
Update

Explanation:http://technet.microsoft.com/en-us/library/bb123981(v=exchg.150).aspx http://technet.microsoft.com/en-us/library/bb676368(v=exchg.141).aspx QUESTION 47You discover that the Large Audience MailTip is not displayed when users compose an email message to the 20 new distribution groups.You need to ensure that the Large Audience MailTip is displayed for the new distribution groups immediately.Which cmdlet should you use? A.

Set-DistributionGroupB. Set-MailboxServerC. Set-ClientAccessServerD. Start-ManagedFolderAssistant Answer: B Explanation:http://technet.microsoft.com/en-us/library/jj674302(v=exchg.150).aspx QUESTION 48Drag and Drop QuestionYou have an Exchange Server 2013 organization that has Information Rights Management (IRM) configured.Users report that they cannot apply IRM protection to email messages from Outlook Web App.You verify that the users can protect the messages by using IRM from Microsoft Outlook. You need to recommend a solution to ensure that the users can protect email messages by using IRM from Outlook Web App.Which four actions should you recommend? To answer, move the four appropriate actions from the list of actions to the answer area and arrange them in the correct order.

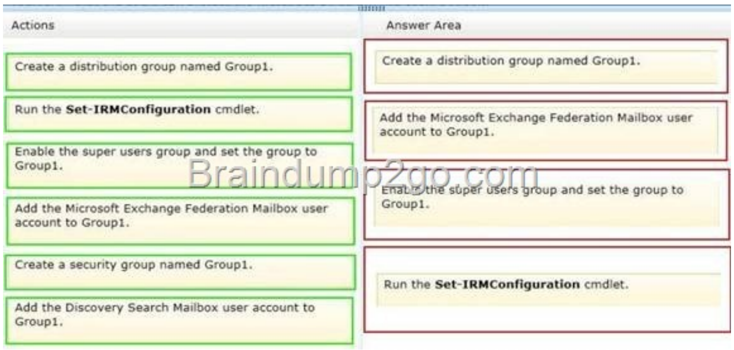


Actions

Answer Area

- Create a distribution group named Group1.
- Run the **Set-IRMConfiguration** cmdlet.
- Enable the super users group and set the group to Group1.
- Add the Microsoft Exchange Federation Mailbox user account to Group1.
- Create a security group named Group1.
- Add the Discovery Search Mailbox user account to Group1.

Answer:



Actions

- Create a distribution group named Group1.
- Run the **Set-IRMConfiguration** cmdlet.
- Enable the super users group and set the group to Group1.
- Add the Microsoft Exchange Federation Mailbox user account to Group1.
- Create a security group named Group1.
- Add the Discovery Search Mailbox user account to Group1.

Answer Area

- Create a distribution group named Group1.
- Add the Microsoft Exchange Federation Mailbox user account to Group1.
- Enable the super users group and set the group to Group1.
- Run the **Set-IRMConfiguration** cmdlet.

Explanation:Box 1: Create a distribution group named Group1.Box 2: Add the Microsoft Exchange Federation Mailbox user account to Group1. Box 3: Enable the super users group and set the group to Group1.Box 4: Run the Set-IRMConfiguration cmdlet.Note:* To enable IRM in Outlook Web App, you must add the Federation mailbox, a system mailbox created by Exchange 2013 Setup, to the super users group in AD RMS.*Step 1: Use the Shell to add the Federation mailbox to a distribution group If a distribution group has been created and configured as a super users group in the AD RMS cluster, you can add the Exchange 2013 Federation mailbox as a member of that group. If a super users group isn't configured, you must create a distribution group and add the Federation mailbox as a member.1.Create a distribution group dedicated for use as an AD RMS super users group.2. Add the user FederatedEmail.4c1f4d8b-8179-4148-93bf-00a95fa1e042 to the new distribution group.Step 2: Use AD RMS to set up a super users groupPerform the following procedure on an AD RMS cluster. The account used to perform this procedure must be a member of the AD RMS Enterprise Administrators local group on the AD RMS server.1. Open the Active Directory Rights Management Services console and expand the AD RMS cluster.2. In the console tree, expand Security Policies, and then click Super Users.3. In the action pane, click Enable Super Users.4. In the result pane, click Change Super User Group to open the Super Users property sheet.5. In the Super user group box, type the email address of the distribution group you created in the previous procedure, or click Browse to select a distribution group.* Information workers increasingly use e-mail to exchange sensitive information. To help secure this information, organizations can use Information Rights Management (IRM) to apply persistent protection to messaging content. Prior to Microsoft Exchange Server 2010, effective use of IRM protection was limited to Outlook clients. In Exchange Server 2007, Microsoft Outlook Web Access users were required to download the Rights Management add-in for Microsoft Internet Explorer so they could access IRM-protected content.In Exchange 2013, IRM in Outlook Web App allows your users to access the rich IRM functionality offered by Exchange to apply persistent IRM-protection to messaging content. Reference: Information Rights Management in Outlook Web App Reference: Add the Federation Mailbox to the AD RMS Super Users Group QUESTION 49You plan to deploy 20 Client Access servers that will have Exchange Server 2013 installed.You need to prepare the certificate required for the planned deployment. The solution must ensure that the same certificate can be used on all of the Client Access servers.What should you do first? A. On one of the Client Access servers, run the New-ExchangeCertificate cmdlet and specify the privatekey exportable parameter.B. On all of the Client Access servers, run the Get-ExchangeCertificate cmdiet.C. On one of the Client Access servers, run the New-ExchangeCertificate cmdiet and specify the binaryencoded parameter.D. On one of the Client Access servers, start the Certificates console and run the Certificate Import Wizard. Answer: AExplanation: http://technet.microsoft.com/en-us/library/aa998327%28v=exchg.150%29.aspx QUESTION 50Contoso, Ltd., and Fabnkam, Inc., are partner companies.Each company has an Exchange Server 2013 organization in a data center that is connected to the Internet. All of the Exchange servers in both of the organizations have the Client Access server role and the Mailbox role installed.The data centers connect to each other by using a redundant high-speed WAN link.The following mail exchanger (MX) records are configured:- Contoso.com MX 10 mail.contoso.com- Fabrikam.com MX 10 mail.fabrikam.comYou need to recommend a solution for inbound mail flow.The solution must meet the following requirements:- Users in both companies must receive email from the Internet if either of the Internet links fails. - Mail from the Internet to contoso.com must be received by mail.contoso.com if the Internet link at the Contoso data center is available.- Mail from the Internet to fabrikam.com must be received by mail.fabrikam.com if the Internet link at the Fabrikam data center is available.Which two actions should you recommend? (Each correct answer presents part of the solution. Choose two.) A. Create the following DNS records:Contoso.com MX 20 mail.fabrikam.comFabrikam.com MX 20 mail.contoso.comB. Create the following DNS records:Contoso.com MX 10 mail.fabrikam.comFabrikam.com MX 10 mail.contoso.comC. For each organization, configure an internal relay domain and a Send connector.D. For each organization, configure an external relay domain and a Receive connector.E. Create the following DNS records:Contoso.com MX 5 mail.fabrikam.comFabrikam.com MX 5 mail.contoso.com Answer: ACExplanation: A: Use a priority above 10.C:* 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.* 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.Incorrect:D: 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. If you want to 100% pass the Microsoft 70-342 Exam sucessfully, recommend to read latest Microsoft 70-342 Dump full version.