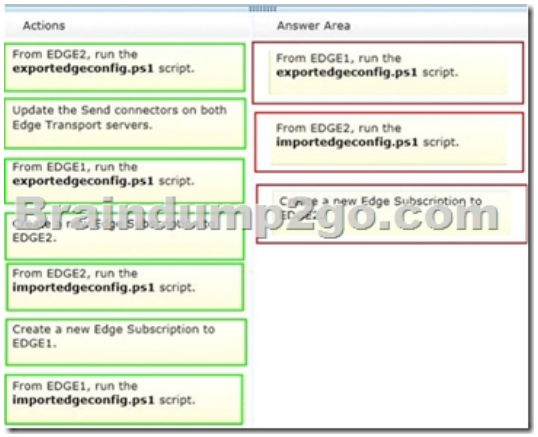
[Jun-2016-NEWLatest Exam 70-341 Study Guides VCE 226q Free Downloading in the Braindump2go[NQ61-NQ70

2016 June New Updated Microsoft 70-341 Exam Questions Released by Braindump2go.com for Free Instant Download Today! NEW QUESTION 61 - NEW QUESTION 70: QUESTION 61You have an Exchange Server 2013 organization that contains multiple Hub Transport servers.You need to recommend a message hygiene solution to meet the following requirements:- Block servers that are known to send spam- Minimize administrative effortWhat should you recommend? A. an IP Block listB. IP Block list providersC. recipient filteringD. sender filtering Answer: B QUESTION 62Your company has a Exchange Server 2013 organization.You plan to deploy Microsoft Office Outlook and mobile devices for remote users.You need to plan the deployment of Client Access servers to support the automatic configuration of Outlook profiles and --------.What should you include in the plan? A. AutodiscoverB. MailTipsC. Remote Access ServerD. Unified Messaging auto attendant Answer: A QUESTION 63You 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.comD. Run the Set-TransportConfigcmdlet.E. Run the Set-TransportServercmdlet.F. From a Mailbox server, create a Send connector that has an address space for adatum.com. Answer: BDFExplanation:NOT AApplies to: Exchange Server 2013, Exchange OnlineRemote domains are SMTP domains that are external to your Microsoft Exchange organization. You can create remote domain entries to define the settings for message transferred between your Exchange organization and specific external domains. The settings in the remote domain entry for a specific external domain override the settings in the default remote domain that normally apply to all external recipients. The remote domain settings are global for the Exchange organization.You can create remote domain entries to define the settings for message transfers between your Exchange Online organization and external domains. When you create a remote domain entry, you control the types of messages that are sent to that domain. You can also apply message format policies and acceptable character sets for messages that are sent from users in your organization to the remote domain.NOT CEdge1 is in the perimeter network and the send connector needs to be created on a mailbox serverNOT ESet-TransportServercmdlet.Use the Set-TransportServer cmdlet to set the transport configuration options for the Transport service on Mailbox servers or for Edge Transport servers. This example sets the DelayNotificationTimeout parameter to 13 hours on server named Mailbox01. Set-TransportServer Mailbox01 -DelayNotificationTimeout 13:00:00 Need Set-TransportConfig and the TLSReceiveDomainSecureList parameter to specify the domains from which you want to receive domain secured email by using mutual Transport Layer Security (TLS) authentication.BTo 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 certificatesOne key difference between Exchange 2010 and Exchange 2013 is that the certificates that are used on the Exchange 2013 Mailbox server are self-signed certificates. Because all clients connect to an Exchange 2013 Mailbox server through an Exchange 2013 Client Access server, the only certificates that you need to manage are those on the Client Access server. The Client Access server automatically trusts the self-signed certificate on the Mailbox server, so clients will not receive warnings about a self-signed certificate not being trusted, provided that the Client Access server has a non-self-signed certificate from either a Windows certification authority (CA) or a trusted third party. There are no tools or cmdlets available to manage self-signed certificates on the Mailbox server. After the server has been properly installed, you should never need to worry about the certificates on the Mailbox server.DSet-TransportConfig.Use the Set-TransportConfig cmdlet to modify the transport configuration settings for the wholeExchange organization.EXAMPLE 1This example configures the Exchange organization to forward all DSN messages that have the DSN codes5.7.1, 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.FIf you want to ensure secure, encrypted communication with a partner, you can create a Send connector that is configured to enforce Transport Layer Security (TLS) for messages sent to a partner domain. TLS provides secure communication over the Internet. Use the EAC to create a Send connector to send email to a partner, with TLS applied To create a Send connector for this scenario, log in to the EAC and perform the following steps:In the EAC, navigate to Mail flow > Send connectors, and then click Add . In the New send connector wizard, specify a name for the send connector and then select Partner for the Type.When you select Partner, the connector is configured to allow connections only to servers that authenticate with TLS certificates. Click Next. Verify that MX record associated with

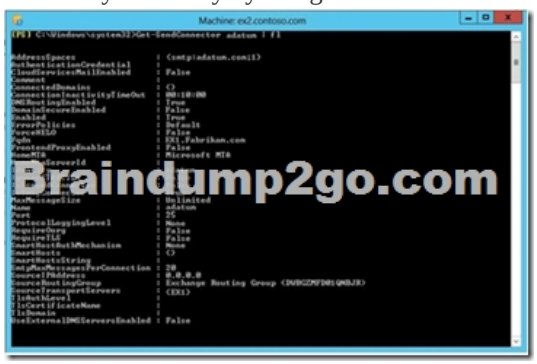
recipient domain is selected, which specifies that the connector uses the domain name system (DNS) to route mail. Click Next. Under Address space, click Add . In the Add domain window, make sure SMTP is listed as the Type. For Fully Qualified Domain Name (FQDN), enter the name of your partner domain. Click Save.For Source server, click Add . In the Select a server window, select a Mailbox server that will be used to send mail to the Internet via the Client Access server and click Add . After you've selected the server, click Add .Click OK.Click Finish.Once you have created the Send connector, it appears in the Send connector list.Send ConnectorIn Microsoft Exchange Server 2013, a Send connector controls the flow of outbound messages to the receiving server.They are configured on Mailbox servers running the Transport service. Most commonly, you configure a Send connector to send outbound email messages to a smart host or directly to their recipient, using DNS.Exchange 2013 Mailbox servers running the Transport service require Send connectors to deliver messages to the next hop on the way to their destination. Send connectors that are created on Mailbox servers are stored in Active Directory and are available to all Mailbox servers running the Transport service in the organization. QUESTION 64Drag and Drop QuestionYou are evaluating the implementation of a second Edge Transport server named EDGE2 in the Amsterdam office. You need to recommend which tasks must be performed to ensure that email messages can be sent by the organization if a single Edge Transport server fails. Which three actions should you include in the recommendation? To answer, move the three appropriate actions from the list of actions to the answer area and arrange them in the correct order.

Answer:



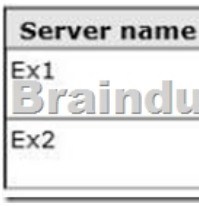
QUESTION 65You need to recommend which type of group must be used to create the planned department lists.Which type of group should you recommend? A. Universal DistributionB. Dynamic DistributionC. Global SecurityD. Universal Security Answer: AExplanation:AUniversal DistributionMail-enabled universal distribution groups (also called distribution groups) can be used only to distribute messages.NOT BA dynamic distribution group is a distribution group that uses recipient filters and conditions to derive its membership at the time messages are sent.http://technet.microsoft.com/en-us/library/bb123722(v=exchg.150).aspxUse the EAC to create a dynamic distribution groupAs ExamTester from Netherlands commented belowBut the Fabrikam case asks that users must be able to add and remove themselves from the distribution group. This is not possible using a dynamic group since membership is dynamically calculated based on attributesUse this explanation for NOT B http://technet.microsoft.com/en-us/library/bb201680(v=exchg.150).aspxYou can't use Exchange Server 2013 to create non-universal distribution groups.Mail-enabled non-universal groups were discontinued in Exchange Server 2007 and can exist only if they were migrated from Exchange 2003 or earlier versions of Exchange. Seems to contradict the above.NOT C DIn Exchange, all

mail-enabled groups are referred to as distribution groups, whether they have a security context or not. QUESTION 66You need to recommend which tasks must be performed to meet the technical requirements of the research and development (R&D) department. Which two tasks should you recommend? (Each correct answer presents part of the solution. Choose two.) A. Create a new global address list (GAL) and a new address book policy.B. Modify the permissions of the default global address list (GAL), and then create a new GAL.C. Run the Update AddressList cmdlet.D. Run the Set-Mailbox cmdlet.E. Create an OAB virtual directory. Answer: ADExplanation:NOT BNeed an address book policyNOT CUpdate AddressList cmdletUse the Update-AddressList cmdlet to update the recipients included in the address list that you specify.EXAMPLE 1This example updates the recipients of the address list building4 and under the container All UsersSales.Update-AddressList -Identity "All UsersSalesbuilding4"NOT EWill not resolve the issueNeed an address book policy and to assign this policy to users.AAddress 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.DAfter you create an address book policy (ABP), you must assign it to mailbox users. Users aren't assigned a default ABP when their user account is created. If you don't assign an ABP to a user, the global address list (GAL) for your entire organization will be accessible to the user through Outlook and Outlook Web App. This example assigns the ABP All Fabrikam to the existing mailbox user joe@fabrikam.com.Set-Mailbox -Identity joe@fabrikam.com -AddressBookPolicy "All Fabrikam" Address Book Policies: Exchange Online Help QUESTION 67You 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.)

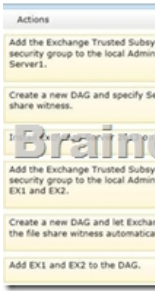


A. tlsauthlevelB. requiretlsC. ignorestarttlsD. tlsdomainE. domainsecureenabledF. smarthostauthmechanism Answer: BEExplanation:Domain SecurityDomain Security is a feature of Exchange Server (both 2010 and 2013) that can secure SMTP traffic between two Exchange organizations.It is implemented on server 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 DomainSecurity is implemented.Set-SendConnectorUse the Set-SendConnector cmdlet to modify a Send connector.EXAMPLE 1This 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 -ConnectionInactivityTimeOut00:15:00 PARAMETERSRequiretlsThe RequireTLS parameter specifies whether all messages sent through this connector must be transmitted using TLS. The default value is $false.DomainsecureenabledThe DomainSecureEnabled parameter is part of the process to enable mutual Transport Layer Security (TLS) authentication for the domains serviced by this Send connector. Mutual TLS authentication functions correctly only when the following conditions are met:The value of the DomainSecureEnabled parameter must be $true. The value of the DNSRoutingEnabled parameter must be $true. The value of the IgnoreStartTLS parameter must be

$false. The wildcard character (*) is not supported in domains that are configured for mutual TLS authentication. The same domain must also be defined on the corresponding Receive connector and in the TLSReceiveDomainSecureList attribute of the transport configuration. The default value for the DomainSecureEnabled parameter is $false for the following types of Send connectors:All Send connectors defined in the Transport service on a Mailbox server. User-created Send connectors defined on an Edge server. The default value for the DomainSecureEnabled parameter is $true for default Send connectors defined on an Edge server.NOT TLSAUTHLEVELThe TlsAuthLevel parameter specifies the TLS authentication level that is used for outbound TLS connections established by this Send connector. Valid values are:EncryptionOnly: TLS is used only to encrypt the communication channel. No certificate authentication is performed.CertificateValidation: TLS is used to encrypt the channel and certificate chain validation and revocation lists checks are performed.DomainValidation: In addition to channel encryption and certificate validation, the Send connector also verifies that the FQDN of the target certificate matches the domain specified in the TlsDomain parameter. If no domain is specified in the TlsDomain parameter, the FQDN on the certificate is compared with the recipient's domain. You can't specify a value for this parameter if the IgnoreSTARTTLS parameter is set to $true, or if the RequireTLS parameter is set to $false. NOT ignorestarttlsThe 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 smarthostauthmechanismThe SmartHostAuthMechanism parameter specifies the smart host authentication mechanism to use for authentication with a remote server. Use this parameter only when a smart host is configured and the DNSRoutingEnabled parameter is set to $false.Valid values are None, BasicAuth, BasicAuthRequireTLS, ExchangeServer, andExternalAuthoritative.All values are mutually exclusive. If you select BasicAuth or BasicAuthRequireTLS, you must use the AuthenticationCredential parameter to specify the authentication credential. QUESTION 68You need to recommend which recovery solution will restore access to all of the mailboxes in AccountingDB if EX1 fails. The solution must restore access to email messages as quickly as possible.Which recovery solution should you recommend? A. On EX2, create a new mailbox database. Restore the database files, and then mount the database.Run the New-MailboxRestoreRequest cmdlet for all of the mailboxes in the database.B. On EX2, create a new mailbox database. Restore the database files, and then mount the database.Run the Set-Mailbox cmdlet for all of the mailboxes in the database.C. On replacement hardware, run setup /mode:recoverserver. Restore the database files, and then mount the database. Run the Set-Mailbox cmdlet.D. On replacement hardware, run setup /mode:recoverserver. Restore the database files, and then mount the database. Run the New-MailboxRestoreRequest cmdlet for all of the mailboxes in the database. Answer: A Explanation:Restore Data Using a Recovery DatabaseCreate a Recovery Database http://technet.microsoft.com/en-us/library/ee332351%28v=exchg.150%29.aspx QUESTION 69Drag and Drop QuestionYou have an Exchange Server 2013 organization that contains two servers. The servers are configured as shown in the following table.



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



Answer:

QUESTION 70You have an Exchange Server 2013 organization that contains one Client Access server. The Client Access server is accessible from the Internet by using a network address translation (NAT) device. You deploy an additional Client Access server. You also deploy an L4 hardware load balancer between the Client Access servers and the NAT device. After deploying the hardware load balancer, you discover that all of the Exchange Server traffic is directed to a single Client Access server. You need to ensure that the hardware load balancer distributes traffic evenly across both Client Access servers. What should you do? A. Change the default route of the Client Access servers to point to the hardware load balancer.B. Configure the NAT device to pass the original source IP address of all connections from the Internet.C. Configure the Client Access servers to have a second IP address and web site. Create the Exchange virtual directories in the new sites.D. Configure SSL offloading on the hardware load balancer and the Client Access servers. Answer: BExplanation:When using source NAT, the client IP address is not passed to the load balanced server. The insertion of the Client IP address into the header allows the exchange servers to see the IP that made the connection. Level 4 Load Balancer:A load balancer is a server computer with a very specialized operating system tuned to manage network traffic using user-created rules. Enterprises and hosting companies rely on load-balancing devices to distribute traffic to create highly available services L4 load balancing is fairly simple, two servers sharing the same IP address. You get redirected to the less-busy server.The most popular Layer 4 load balancing techniques are:- round-robin- weighted round-robin- least connections- weighted least connectionsNOT Ahttp://pdfs.loadbalancer.org/Microsoft_Exchange_2013_Deployment_Guide.pdf If there was no NAT device and the load balancer was completing the NAT translation then there maybe some merit in this answer option. B is a better answer given this scenario.NOT CNo need to configure the Client Access servers to have a second IP address.NOT DNot required in this scenarioSSL offloading relieves a Web server of the processing burden of encrypting and/or decrypting traffic sent via SSL, the security protocol that is implemented in every Web browser. The processing is offloaded to a separate device designed specifically to perform SSL acceleration or SSL termination.Correct Answer BWhen using source NAT, the client IP address is not passed to the load balanced server. The insertion of the Client IP address into the header allows the exchange servers to see the IP that made the connection.http://pdfs.loadbalancer.org/Microsoft_Exchange_2013_Deployment_Guide.pdf 2016 Valid Microsoft 70-341 Exam Study Materials: 1.| Latest 70-341 PDF and VCE Dumps 226Q&As from Braindump2go: http://www.braindump2go.com/70-341.html [100% Exam Pass Guaranteed!] 2.| New 70-341 Exam Questions and Answers ? Google Drive: https://drive.google.com/folderview?id=0B9YP8B9sF_gNTnZCU1FPNFRfZk0&usp=sharing 3.| More Valid 70-341 Practice Questions ? 2015 to 2016: https://drive.google.com/folderview?id=0B75b5xYLjSSNbTQ2eEI5ZkRZUVE&usp=sharing MORE Practice is the Most Important IF You want to PASS 70-341 Exam 100%!????? Braindump2go.com????? Pass All IT Exams at the first Try!