ExamsKey

Microsoft

EXAM - 70-341

Core Solutions of Microsoft Exchange Server 2013

Buy Full Product

http://www.examskey.com/70-341.html

Examskey Microsoft 70-341 exam demo product is here for you to test the quality of the product. This Microsoft 70-341 demo also ensures that we have this product ready unlike most companies, which arrange the product for you as you order These 70-341 exam questions are prepared by Microsoft subject matter specialists. Hence these are most accurate version of the 70-341 exam questions that you can get in the market.

We also offer bundle discount packages for every Microsoft certification track, so you can buy all related exam questions in one convenient bundle. And for corporate clients we also offer bundles for Microsoft certification exams at huge discount.

Check out our 70-341 Exam Page and Microsoft Certification Page for more details of these bundle packages.

Case Study: 1
Fabrikam, Inc

Overview

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

The company has offices in Paris and Amsterdam.

Existing Environment Active Directory Environment

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

Network Infrastructure

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

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

Client computers run either Windows 7 or Windows 8 and have Microsoft Office 2010 installed. The Paris office uses the 192.168.1.0/24 IP range. The Amsterdam office uses the 192.168.2.0/24 IP range.

The offices connect to each other by using a high-speed, low-latency WAN link. Each office has a 10-Mbps connection to the Internet.

Planned Exchange Infrastructure

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

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

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

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

DAG1 will use FS1 as a file share witness. DAG2 will use FS3 as a file share witness.
You plan to create the following networks on each DAG:
A dedicated replication network named DAGNET1 A MAPI network named DAGNET2
All replication traffic will run on DAGNET1.
All client connections will run on DAGNET2. Client connections must never occur on DAGNET1. Replication traffic must only occur on DAGNET2 if DAGNET1 is unavailable.
Each Exchange Server 2013 Mailbox server will be configured to have two network adapters.
The following two mailbox databases will not be replicated as part of the DAGs:
A mailbox database named AccountingDB that is hosted on EX1 A mailbox database named TempStaffDB that is hosted on EX4
EDGE1 will have an Edge Subscription configured, with both EX1 and EX2 as targets.

Requirements Planned Changes

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

Technical Requirements

Fabrikam must meet the following technical requirements:
Email must be evaluated for SPAM before the email enters the internal network. Production system patching must minimize downtime to achieve the highest possible service to users. Users must be able to use the Exchange Control Panel to autonomously join and disjoin their department's distribution lists. Users must be able to access all Internet-facing Exchange Server services by using the names of mail.fabrikam.com and autodiscover.fabrikam.com.
The company establishes a partnership with another company named A, Datum Corporation. A, Datum uses the SMTP suffix adatum.com for all email addresses. Fabrikam plans to exchange sensitive information with A, Datum and requires that the email messages sent between the two companies be encrypted. The solution must use Domain Security.
Users in the research and development (R&D) department must be able to view only the mailboxes of the users in their department from Microsoft Outlook. The users in all of the other departments must be prevented from viewing the mailboxes of the R&D users from Outlook.

Administrators plan to produce HTML reports that contain information about recent status changes to the mailbox databases.
Fabrikam is evaluating whether to abort its plan to implement an Exchange Server 2010 Edge Transport server and to implement a Client Access server in the Paris office instead. The Client Access server will have anti-spam agents installed.

Question: 1

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.

Network Name	ReplicationEnabled	MapiAccessEnabled
DAGNET1	☐	☐
DAGNET2	☐	☐

Answer:

Network Name	ReplicationEnabled	MapiAccessEnabled
DAGNET1	☑	☐
DAGNET2	☐	☑

Question: 2

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

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

Answer: A

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

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

Question: 3

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

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

Answer: B

Explanation:
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: 4

You need to recommend a design that meets the technical requirements for communication between Fabrikam and A, Datum.
Which three actions should you perform in fabrikam.com? (Each correct answer presents part of the solution. Choose three.)

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

Answer: B,D,F

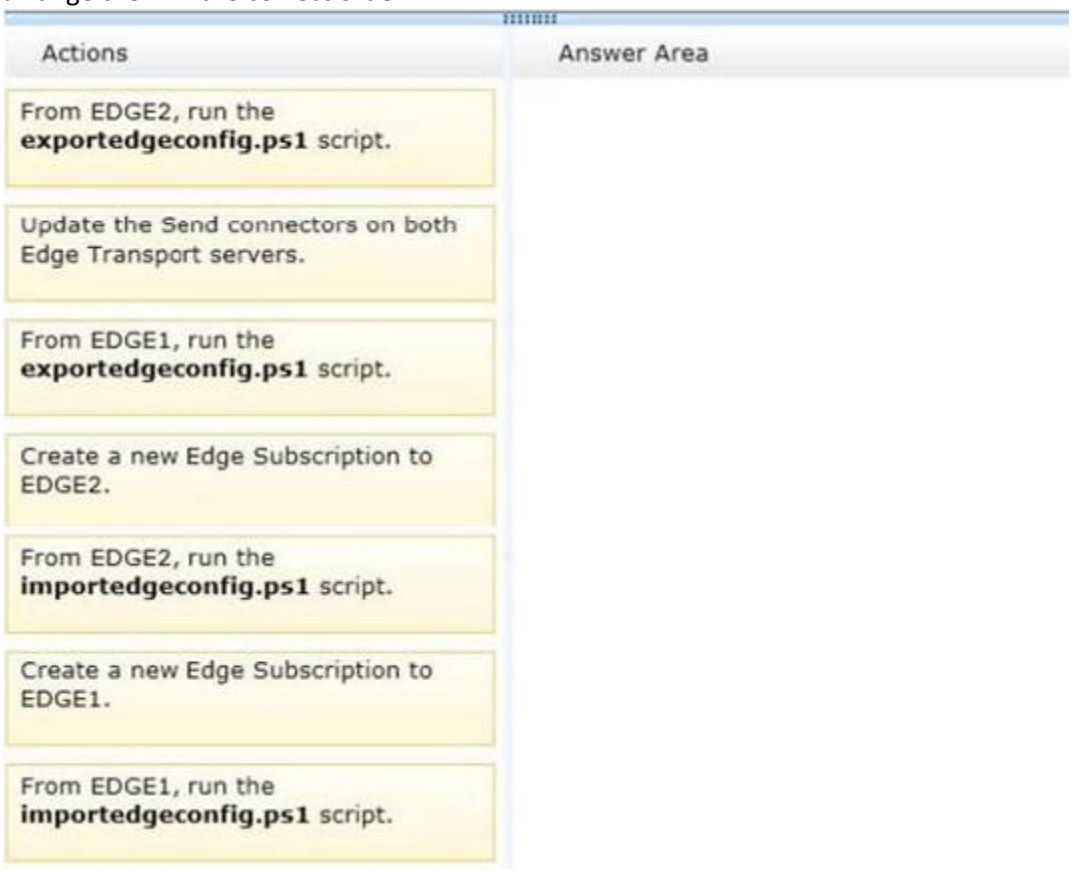
Explanation:
NOT A Applies to: Exchange Server 2013, Exchange Online Remote domains are SMTP domains that are external to your Microsoft Exchange organization. You can create remote domain entries to define the settings for message transferred between your Exchange organization and specific external domains. The settings in the remote domain entry for a specific external domain override the settings in the default remote domain that normally apply to all external recipients. The remote domain settings are global for the Exchange organization.
You can create remote domain entries to define the settings for message transfers between your Exchange Online organization and external domains. When you create a remote domain entry, you control the types of messages that are sent to that domain. You can also apply message format policies and acceptable character sets for messages that are sent from users in your organization to the remote domain.
NOT C Edge1 is in the perimeter network and the send connector needs to be created on a mailbox server
NOT E Set-TransportServercmdlet. Use the Set-TransportServer cmdlet to set the transport configuration options for the Transport service on Mailbox servers or for Edge Transport servers. This example sets the DelayNotificationTimeout parameter to 13 hours on server named Mailbox01. Set-TransportServer Mailbox01 -DelayNotificationTimeout 13:00:00 Need Set-TransportConfig and the TLSReceiveDomainSecureList parameter to specify the domains from which you want to receive domain secured email by using mutual Transport Layer Security (TLS) authentication.
B To activate SSL encryption on an Exchange server, you need a server certificate on the Client Access Server in each company. The client access server is the internet facing server in an organization.
An SSL certificate is a digital certificate that authenticates the identity of the exchange server and encrypts information that is sent to the server using Secure Sockets Layer (SSL) technology Mailbox server certificates One key difference between Exchange 2010 and Exchange 2013 is that the certificates that are used on the Exchange 2013 Mailbox server are self-signed certificates. Because

all clients connect to an Exchange 2013 Mailbox server through an Exchange 2013 Client Access server, the only certificates that you need to manage are those on the Client Access server.
The Client Access server automatically trusts the self-signed certificate on the Mailbox server, so clients will not receive warnings about a self-signed certificate not being trusted, provided that the Client Access server has a non-self-signed certificate from either a Windows certification authority (CA) or a trusted third party. There are no tools or cmdlets available to manage self-signed certificates on the Mailbox server. After the server has been properly installed, you should never need to worry about the certificates on the Mailbox server.
D Set-TransportConfig. Use the Set-TransportConfig cmdlet to modify the transport configuration settings for the whole Exchange organization. EXAMPLE 1 This example configures the Exchange organization to forward all DSN messages that have the DSN codes 5.7.1, 5.7.2, and 5.7.3 to the postmaster email account. Set-TransportConfig -GenerateCopyOfDSNFor 5.7.1,5.7.2,5.7.3 The TLSReceiveDomainSecureList parameter specifies the domains from which you want to receive domain secured email by using mutual Transport Layer Security (TLS) authentication.
F If you want to ensure secure, encrypted communication with a partner, you can create a Send connector that is configured to enforce Transport Layer Security (TLS) for messages sent to a partner domain. TLS provides secure communication over the Internet. Use the EAC to create a Send connector to send email to a partner, with TLS applied To create a Send connector for this scenario, log in to the EAC and perform the following steps:
In the EAC, navigate to Mail flow > Send connectors, and then click Add . In the New send connector wizard, specify a name for the send connector and then select Partner for the Type. When you select Partner, the connector is configured to allow connections only to servers that authenticate with TLS certificates. Click Next. Verify that MX record associated with recipient domain is selected, which specifies that the connector uses the domain name system (DNS) to route mail. Click Next. Under Address space, click Add . In the Add domain window, make sure SMTP is listed as the Type. For Fully Qualified Domain Name (FQDN), enter the name of your partner domain. Click Save. For Source server, click Add . In the Select a server window, select a Mailbox server that will be used to send mail to the Internet via the Client Access server and click Add . After you've selected the server, click Add .
Click OK. Click Finish. Once you have created the Send connector, it appears in the Send connector list. Send Connector In Microsoft Exchange Server 2013, a Send connector controls the flow of outbound messages to the receiving server. They are configured on Mailbox servers running the Transport service. Most commonly, you configure a Send connector to send outbound email messages to a smart host or directly to their recipient, using DNS. Exchange 2013 Mailbox servers running the Transport service require Send connectors to deliver messages to the next hop on the way to their destination. Send connectors that are created on Mailbox servers are stored in Active Directory and are available to all Mailbox servers running the Transport service in the organization. Send Connectors: Exchange 2013 Help

Question: 5

DRAG DROP
You are evaluating the implementation of a second Edge Transport server named EDGE2 in the Amsterdam office.
You need to recommend which tasks must be performed to ensure that email messages can be sent by the organization if a single Edge Transport server fails.
Which three actions should you include in the recommendation?

To answer, move the three appropriate actions from the list of actions to the answer area and arrange them in the correct order.



Answer:

Question: 6

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

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

Answer: A

Explanation:
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 or not.
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: 7

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

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

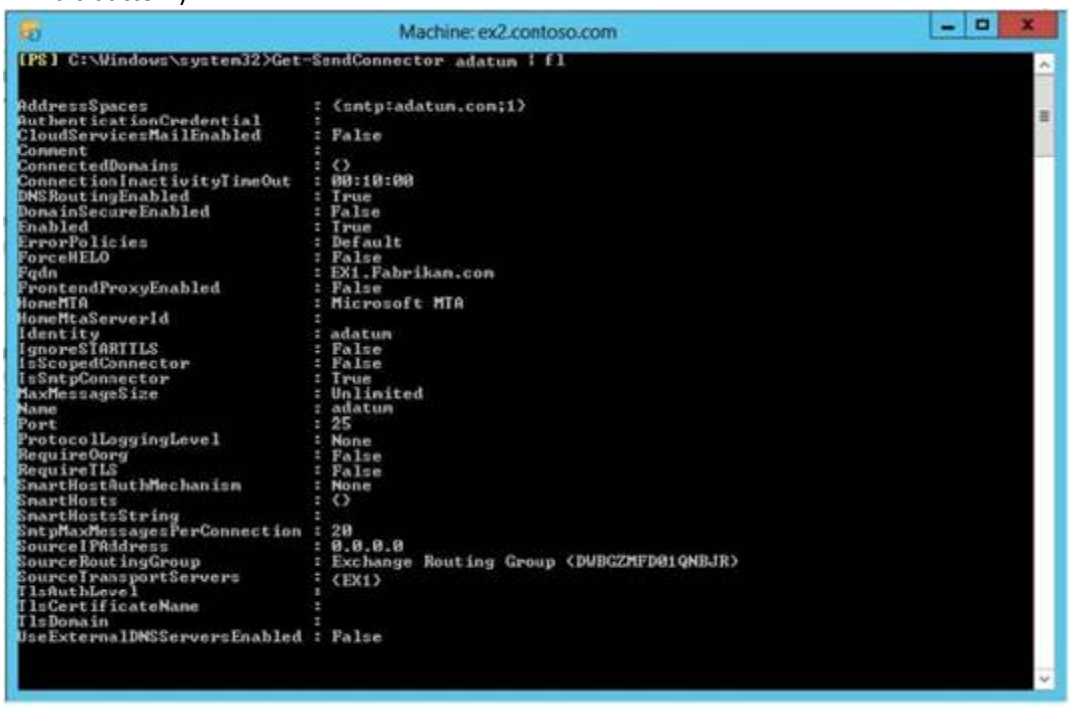
Answer: A,D

Explanation:
NOT B Need an address book policy

NOT C
Update AddressList cmdlet Use the Update-AddressList cmdlet to update the recipients included in the address list that you specify.
EXAMPLE 1 This example updates the recipients of the address list building4 and under the container All Users\Sales. Update-AddressList -Identity "All Users\Sales\building4"
NOT E Will not resolve the issue Need an address book policy and to assign this policy to users.
A Address book policies (ABPs) allow you to segment users into specific groups to provide customized views of your organization's global address list (GAL). When creating an ABP, you assign a GAL, an offline address book (OAB), a room list, and one or more address lists to the policy. You can then assign the ABP to mailbox users, providing them with access to a customized GAL in Outlook and Outlook Web App. The goal is to provide a simpler mechanism to accomplish GAL segmentation for on-premises organizations that require multiple GALs.
D After you create an address book policy (ABP), you must assign it to mailbox users. Users aren't assigned a default ABP when their user account is created. If you don't assign an ABP to a user, the global address list (GAL) for your entire organization will be accessible to the user through Outlook and Outlook Web App. This example assigns the ABP All Fabrikam to the existing mailbox user joe@fabrikam.com. Set-Mailbox -Identity joe@fabrikam.com -AddressBookPolicy "All Fabrikam" Address Book Policies: Exchange Online Help Set-Mailbox: Exchange 2013 Help

Question: 8

You are testing the planned implementation of Domain Security. You discover that users fail to exchange domain-secured email messages.
You open the Exchange Management Shell and discover the output shown in the exhibit. (Click the Exhibit button.)



You need to ensure that users can exchange email messages by using Domain Security.
Which two parameters should you modify by using the Set-SendConnector cmdlet? (Each correct answer presents part of the solution. Choose two.)

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

Answer: B,E

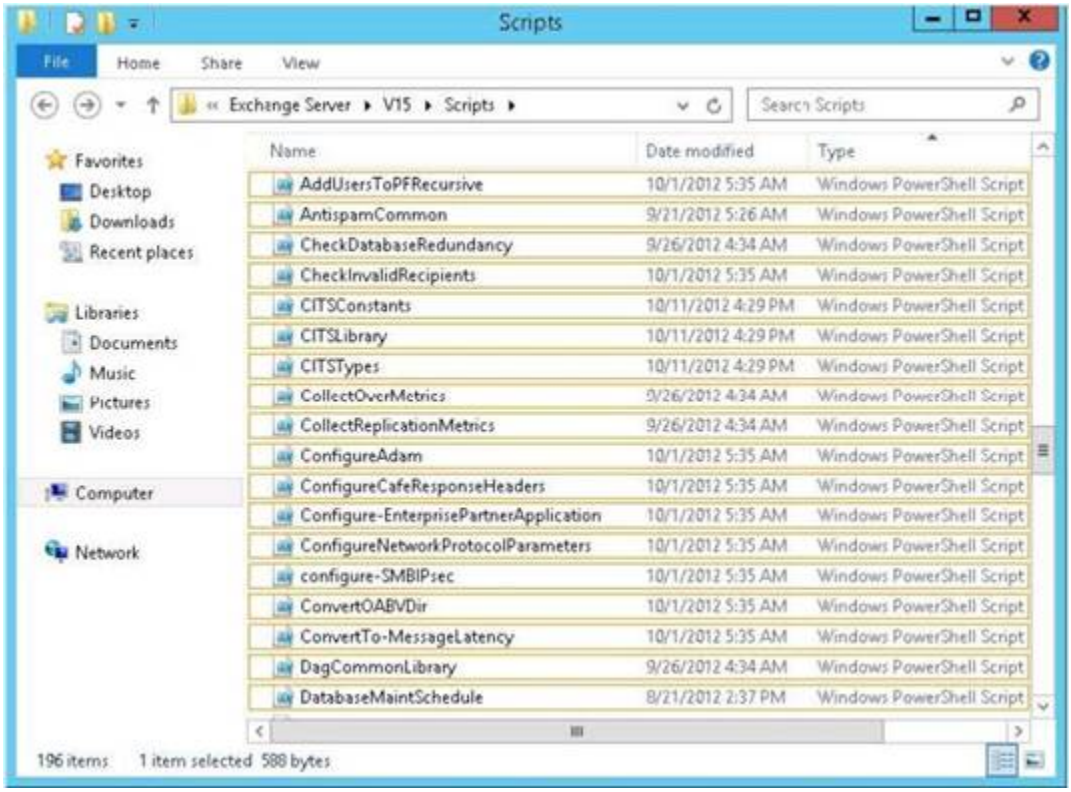
Explanation:
Domain Security Domain Security is a feature of Exchange Server (both 2010 and 2013) that can secure SMTP traffic between two Exchange organizations. It is implemented on server level, and it works without configuring any options on user
(sender or recipient) side. Domain Security uses mutual TLS authentication to provide session-based authentication and encryption. Mutual TLS authentication is different from TLS as it's usually implemented. Usually, when you implement TLS, client will verify the server certificate, and authenticate the server, before establishing a connection. With mutual TLS authentication, each server verifies the connection with the other server by validating a certificate that's provided by that other server, so clients are not included at all. We establish secure SMTP channel between two Exchange Servers, usually over the Internet. Clients, Outlook and Outlook Web App, will be aware that Domain Security is established. Green icon with check mark will be shown on each messages exchanged between servers on which Domain
Security is implemented. Set-SendConnector Use the Set-SendConnector cmdlet to modify a Send connector. EXAMPLE 1 This example makes the following configuration changes to the Send connector named Contoso.com Send Connector: Sets the maximum message size limit to 10 MB. Changes the connection inactivity time-out to 15 minutes. Set-SendConnector "Contoso.com Send Connector" -MaxMessageSize 10MB -ConnectionInactivityTimeOut
00:15:00 PARAMETERS Requiretls The RequireTLS parameter specifies whether all messages sent through this connector must be transmitted using TLS. The default value is $false. Domainsecureenabled The DomainSecureEnabled parameter is part of the process to enable mutual Transport Layer Security (TLS) authentication for the domains serviced by this Send connector. Mutual TLS authentication functions correctly only when the following conditions are met: The value of the DomainSecureEnabled parameter must be $true. The value of the DNSRoutingEnabled parameter must be $true. The value of the IgnoreStartTLS parameter must be $false. The wildcard character (*) is not supported in domains that are configured for mutual TLS authentication. The same domain must also be defined on the corresponding Receive connector and in the TLSReceiveDomainSecureList attribute of the transport configuration. The default value for the DomainSecureEnabled parameter is $false for the following types of Send connectors:
All Send connectors defined in the Transport service on a Mailbox server. User-created Send connectors defined on an Edge server. The default value for the DomainSecureEnabled parameter is $true for default Send connectors defined on an Edge server.
NOT TLSAUTHLEVEL The TlsAuthLevel parameter specifies the TLS authentication level that is used for outbound TLS connections established by this Send connector. Valid values are: EncryptionOnly: TLS is used only to encrypt the communication channel. No certificate authentication is performed. CertificateValidation: TLS is used to encrypt the channel and certificate chain validation and revocation lists checks are performed. DomainValidation: In addition to channel encryption and certificate validation, the Send connector also verifies that the FQDN of the target certificate

matches the domain specified in the TlsDomain parameter. If no domain is specified in the TlsDomain parameter, the FQDN on the certificate is compared with the recipient's domain. You can't specify a value for this parameter if the IgnoreSTARTTLS parameter is set to $true, or if the RequireTLS parameter is set to $false.
NOT ignorestarttls The IgnoreSTARTTLS parameter specifies whether to ignore the StartTLS option offered by a remote sending server. This parameter is used with remote domains. This parameter must be set to $false if the RequireTLS parameter is set to $true. Valid values for this parameter are $true or $false.
NOT tlsdomain The TlsDomain parameter specifies the domain name that the Send connector uses to verify the FQDN of the target certificate when establishing a TLS secured connection. This parameter is used only if the TlsAuthLevel parameter is set to DomainValidation. A value for this parameter is required if: The TLSAuthLevel parameter is set to DomainValidation. The DNSRoutingEnabled parameter is set to $false (smart host Send connector).
NOT smarthostauthmechanism The SmartHostAuthMechanism parameter specifies the smart host authentication mechanism to use for authentication with a remote server. Use this parameter only when a smart host is configured and the DNSRoutingEnabled parameter is set to $false. Valid values are None, BasicAuth, BasicAuthRequireTLS, ExchangeServer, and
ExternalAuthoritative. All values are mutually exclusive. If you select BasicAuth or BasicAuthRequireTLS, you must use the AuthenticationCredential parameter to specify the authentication credential. TLS Functionality and Related Terminology: Exchange 2013 Help

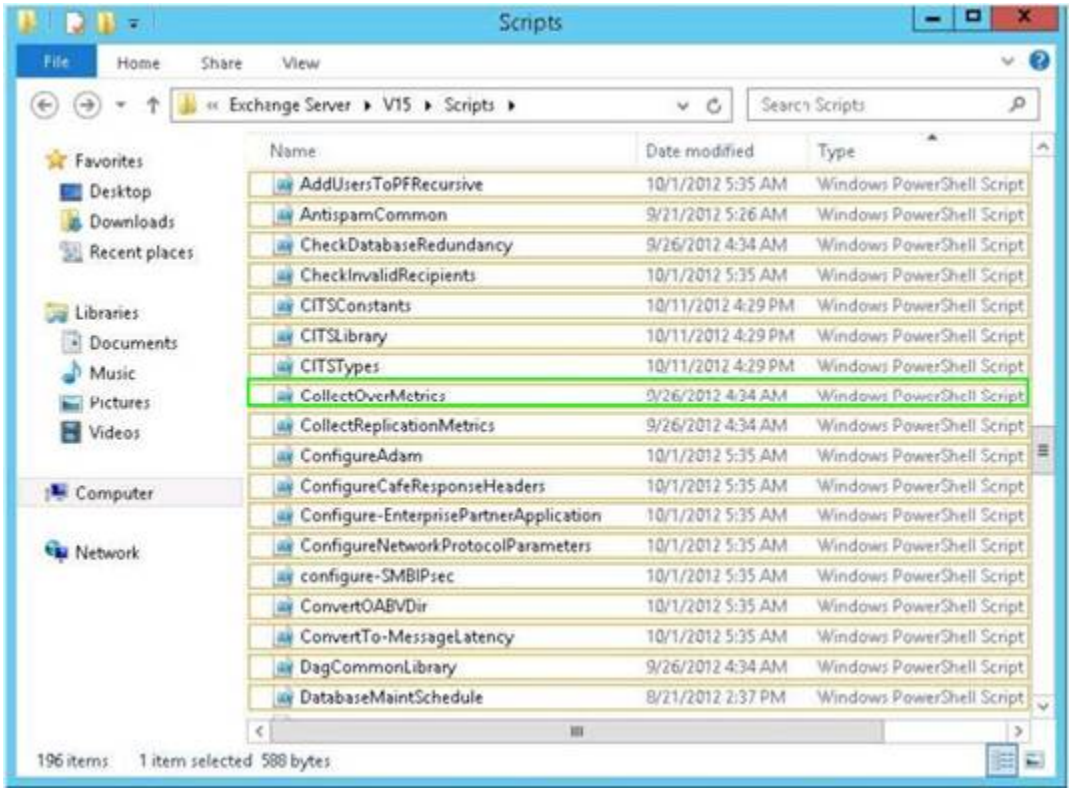
Question: 9

HOTSPOT

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.


Scripts
File
Home
Share
View
Exchange Server ▸ V15 ▸ Scripts ▸
Search Scripts
Favorites
Desktop
Downloads
Recent places
Libraries
Documents
Music
Pictures
Videos
Computer
Network
Name
Date modified
Type
AddUsersToPFRecursive 10/1/2012 5:35 AM Windows PowerShell Script
AntispamCommon 9/21/2012 5:26 AM Windows PowerShell Script
CheckDatabaseRedundancy 9/26/2012 4:34 AM Windows PowerShell Script
CheckInvalidRecipients 10/1/2012 5:35 AM Windows PowerShell Script
CITSConstants 10/11/2012 4:29 PM Windows PowerShell Script
CITSLibrary 10/11/2012 4:29 PM Windows PowerShell Script
CITSTypes 10/11/2012 4:29 PM Windows PowerShell Script
CollectOverMetrics 9/26/2012 4:34 AM Windows PowerShell Script
CollectReplicationMetrics 9/26/2012 4:34 AM Windows PowerShell Script
ConfigureAdam 10/1/2012 5:35 AM Windows PowerShell Script
ConfigureCafeResponseHeaders 10/1/2012 5:35 AM Windows PowerShell Script
Configure-EnterprisePartnerApplication 10/1/2012 5:35 AM Windows PowerShell Script
ConfigureNetworkProtocolParameters 10/1/2012 5:35 AM Windows PowerShell Script
configure-SMBIPsec 10/1/2012 5:35 AM Windows PowerShell Script
ConvertOABVDir 10/1/2012 5:35 AM Windows PowerShell Script
ConvertTo-MessageLatency 10/1/2012 5:35 AM Windows PowerShell Script
DagCommonLibrary 9/26/2012 4:34 AM Windows PowerShell Script
DatabaseMaintSchedule 8/21/2012 2:37 PM Windows PowerShell Script
196 items
1 item selected 588 bytes

Answer:



Question: 10

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

A. On EX2, create a new mailbox database. Restore the database files, and then mount the database. Run the New-MailboxRestoreRequest cmdlet for all of the mailboxes in the database.

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

Answer: A

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

Question: 11

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

Answer:


Answer Area
Run the $Data=Get-Content -Path "C:\Apps\SocialMediaApp.xml" -Encoding Byte -ReadCount 0 command.
Run the New-App -FileData $Data command.
Run the Set-App cmdlet.
Run the Get-App cmdlet.
Install the Outlook app.
Install the Outlook app.
Run the Get-App cmdlet.
Run the Set-App cmdlet.

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 70-341 Exam Questions With Answers.

http://www.examskey.com/70-341.html

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Download Free Product Demo From:

http://www.examskey.com/70-341.html

Money Back Guarantee

Check Out Our Customer Testimonials

http://vimeo.com/102521210