70-341 Q&As

Core Solutions of Microsoft Exchange Server

Pass Microsoft 70-341 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.geekcert.com/70-341.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Microsoft Official Exam Center

- **Instant Download** After Purchase
- **100% Money Back** Guarantee
- **365 Days** Free Update
- **800,000+** Satisfied Customers

QUESTION 1

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

Domain Security

Domain Security is a feature of Exchange Server (both 2010 and 2013) that can secure SMTP traffic between two Exchange organizations.

It is implemented on server level, and it works without configuring any options on user (sender or recipient) side. Domain Security uses mutual TLS authentication to provide session-based authentication and encryption.

Mutual TLS authentication is different from TLS as it's usually implemented. Usually, when you implement TLS, client will verify the server certificate, and authenticate the server, before establishing a connection.

With mutual TLS authentication, each server verifies the connection with the other server by validating a certificate that's provided by that other server, so clients are not included at all.

We establish secure SMTP channel between two Exchange Servers, usually over the Internet.

Clients, Outlook and Outlook Web App, will be aware that Domain Security is established.

Green icon with check mark will be shown on each messages exchanged between servers on which Domain

Security is implemented.

Set-SendConnector

Use the Set-SendConnector cmdlet to modify a Send connector.

EXAMPLE 1

This example makes the following configuration changes to the Send connector named Contoso.com Send Connector:

Sets the maximum message size limit to 10 MB.

Changes the connection inactivity time-out to 15 minutes.

Set-SendConnector "Contoso.com Send Connector" -MaxMessageSize 10MB -ConnectionInactivityTimeOut

00:15:00 PARAMETERS Requiretls The RequireTLS parameter specifies whether all messages sent through this connector must be transmitted using TLS. The default value is $false.

Domainsecureenabled

The DomainSecureEnabled parameter is part of the process to enable mutual Transport Layer Security (TLS) authentication for the domains serviced by this Send connector. Mutual TLS authentication functions correctly only when the

following conditions are met:

The value of the DomainSecureEnabled parameter must be $true.

The value of the DNSRoutingEnabled parameter must be $true.

The value of the IgnoreStartTLS parameter must be $false.

The wildcard character (*) is not supported in domains that are configured for mutual TLS authentication. The same domain must also be defined on the corresponding Receive connector and in the TLSReceiveDomainSecureList attribute of

the transport configuration.

The default value for the DomainSecureEnabled parameter is $false for the following types of Send connectors:

All Send connectors defined in the Transport service on a Mailbox server.

User-created Send connectors defined on an Edge server.

The default value for the DomainSecureEnabled parameter is $true for default Send connectors defined on an Edge server.

NOT TLSAUTHLEVEL

The TlsAuthLevel parameter specifies the TLS authentication level that is used for outbound TLS connections established by this Send connector. Valid values are:

EncryptionOnly: TLS is used only to encrypt the communication channel. No certificate authentication is performed.

CertificateValidation: TLS is used to encrypt the channel and certificate chain validation and revocation lists checks are performed.

DomainValidation: In addition to channel encryption and certificate validation, the Send connector also verifies that the FQDN of the target certificate matches the domain specified in the TlsDomain parameter. If no domain is specified in the

TlsDomain parameter, the FQDN on the certificate is compared with the recipient\\'s domain.

You can\\'t specify a value for this parameter if the IgnoreSTARTTLS parameter is set to $true, or if the RequireTLS parameter is set to $false.

NOT ignorestarttls

The IgnoreSTARTTLS parameter specifies whether to ignore the StartTLS option offered by a remote sending server.

This parameter is used with remote domains. This parameter must be set to $false if the RequireTLS parameter is set to $true. Valid values for this parameter are $true or $false.

NOT tlsdomain The TlsDomain parameter specifies the domain name that the Send connector uses to verify the FQDN of the target certificate when establishing a TLS secured connection.

This parameter is used only if the TlsAuthLevel parameter is set to DomainValidation.

A value for this parameter is required if:

The TLSAuthLevel parameter is set to DomainValidation.

The DNSRoutingEnabled parameter is set to $false (smart host Send connector).

NOT smarthostauthmechanism

The SmartHostAuthMechanism parameter specifies the smart host authentication mechanism to use for authentication with a remote server.

Use this parameter only when a smart host is configured and the DNSRoutingEnabled parameter is set to $false.

Valid values are None, BasicAuth, BasicAuthRequireTLS, ExchangeServer, and ExternalAuthoritative.

All values are mutually exclusive. If you select BasicAuth or BasicAuthRequireTLS, you must use the AuthenticationCredential parameter to specify the authentication credential.

QUESTION 2

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.

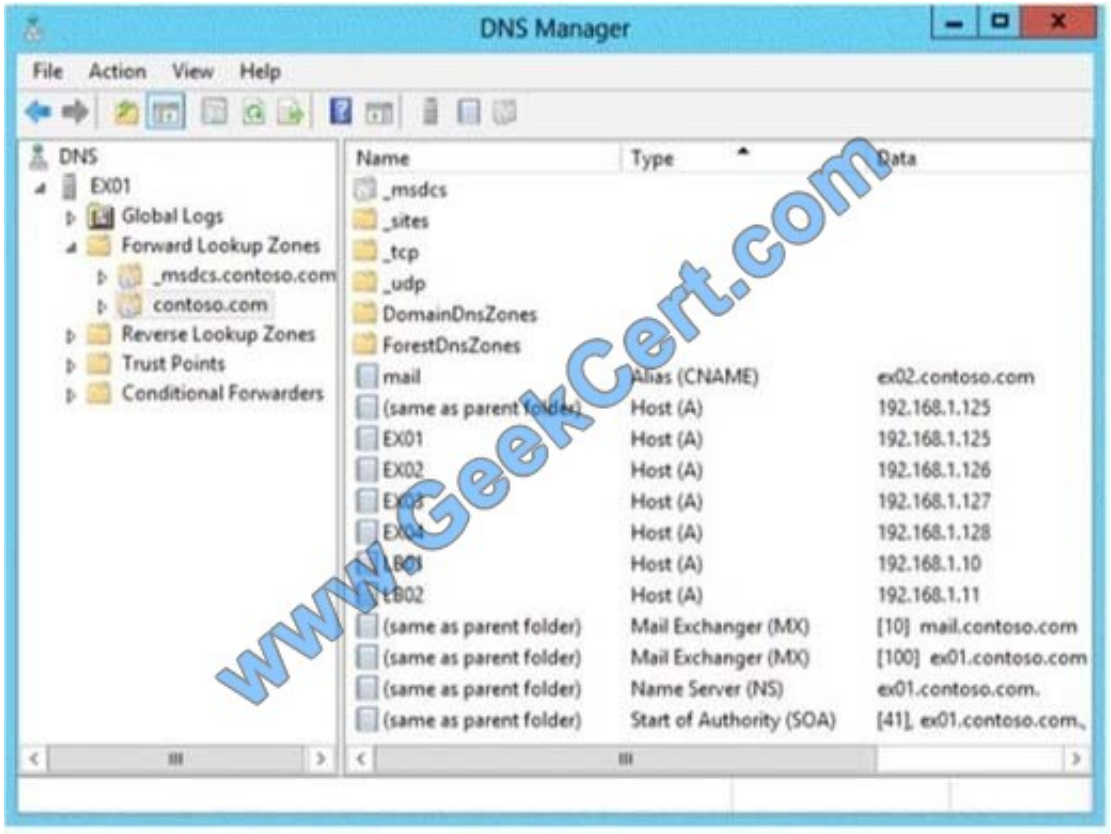
D. Create a new accepted domain for adatum.com and set the domain type to Authoritative Domain.

E. Create a new accepted domain for adatum.com and set the domain type to External RelayDomain.

Correct Answer: AD

QUESTION 3

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.



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

Hot Area:

Answer Area

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

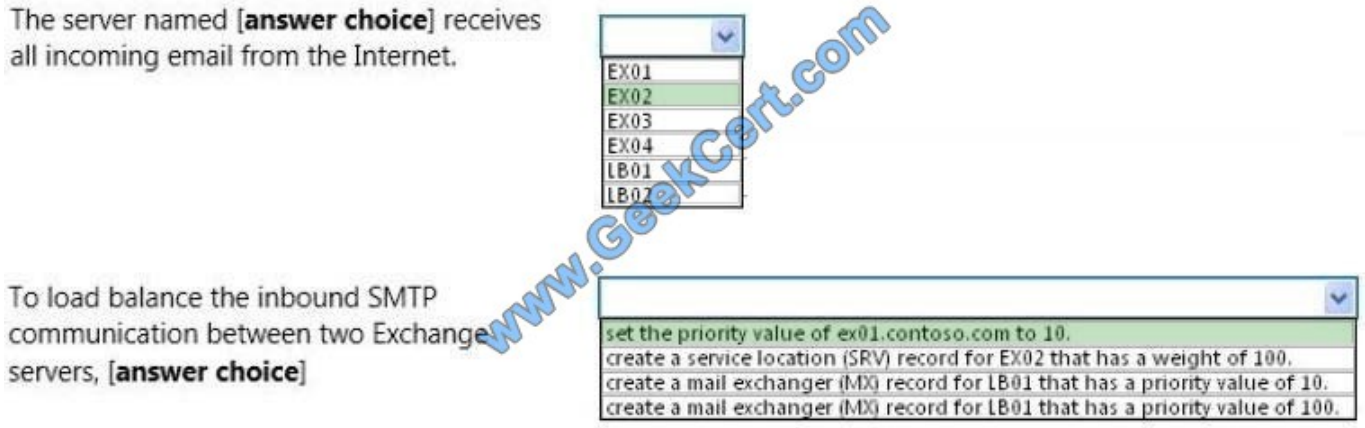
- EX01
- EX02
- EX03
- EX04
- LB01
- LB02

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

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

Correct Answer:

Answer Area



QUESTION 4

You have an Exchange Server 2013 organization.

You plan to delegate the following administrative tasks:

View the status of the message queue.

Create, mount, and dismount databases.

Restore mailboxes from a recovery database,

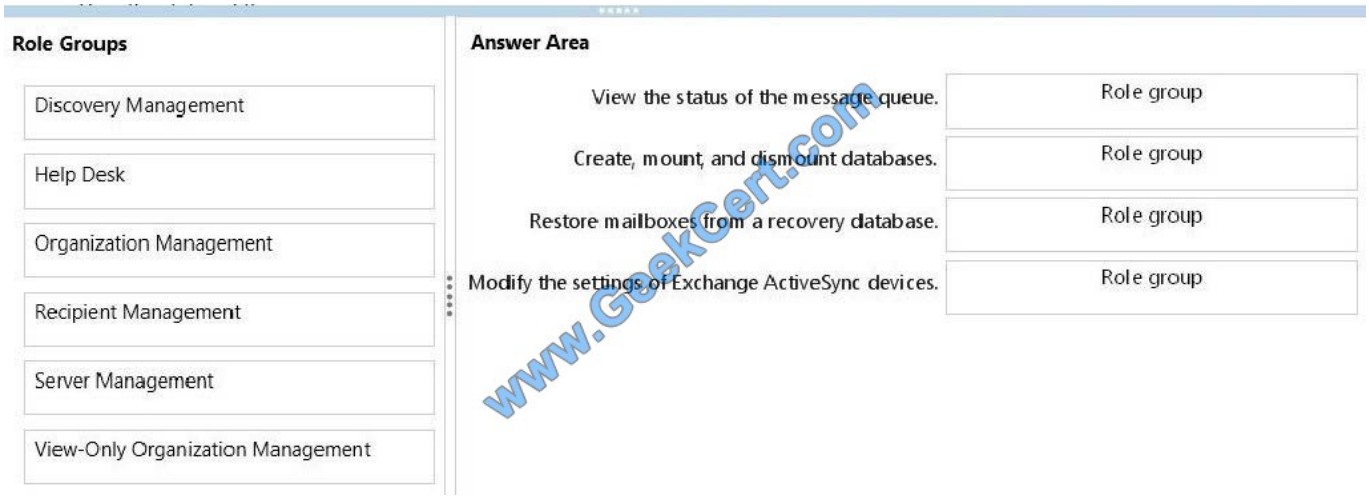
Modify the settings of Exchange ActiveSync devices.

You need to identify which role group must be used to delegate each administrative task. The solution must ensure that the role group that has the fewest administrative privileges is used.

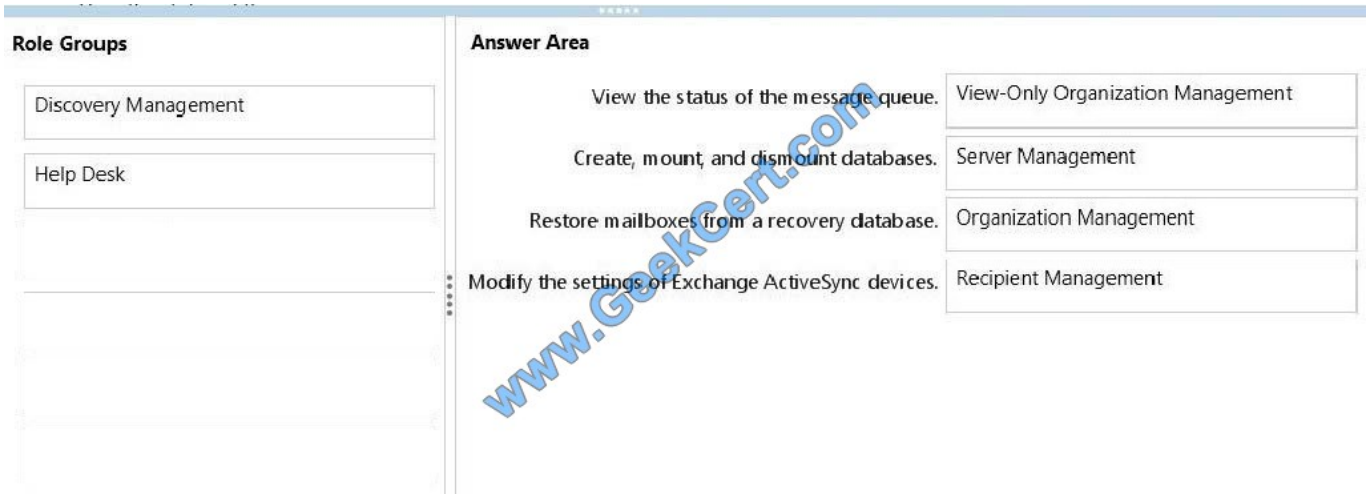
Which role groups should you identify? {To answer, drag the appropriate role groups to the correct tasks. Each role group may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view

content.)

Select and Place:



Correct Answer:



QUESTION 5

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