MS-203 Q&As

Microsoft 365 Messaging

Pass Microsoft MS-203 Exam with 100% Guarantee

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

https://www.leads4pass.com/ms-203.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

You have a Microsoft Exchange Server 2019 organization.

You run the following commands.

New-Management-Scope -Name "VIP Mailboxes" -RecipientRoot "Contoso.com/Executives"

-RecipientRestrictionFilter (RecepientType -eq "UserMailbox")

New-ManagementRoleAssignment -SecurityGroup "VIP Admins" -Role "Mail Recipients"

-CustomRecipientWriteScope "VIP Mailboxes"

You have a user named Admin1.

You need to ensure that Admin1 can manage the mailboxes of users in the Executives organizational unit (OU) only.

What should you do?

A. Modify the membership of VIP Admins.

B. Create a custom role group.

C. Add Admin1 to the Recipient Management management role group.

D. Move Admin1 to the Executives OU.

Correct Answer: A

References: https://social.technet.microsoft.com/Forums/exchange/en-US/b316a841-c39d-483a-ac8e-64d5904c42e6/howto-limit-recipient-management-rights-to-users-in-a-ou-in-exchange-2010-sp1?forum=exchangesvradminlegacy

QUESTION 2

You deploy a Microsoft Exchange Server 2019 organization.

You need to ensure that users of all new mailboxes are prevented from editing their personal information.

What should you do?

A. From the Exchange admin center, create a new role assignment policy.

B. From PowerShell, run the New-Ro1eAssignmentPolicy cmdlet and specify the -isDefault parameter.

C. From the Exchange admin center, create a new role group and assign the role group to Domain Users.

D. From PowerShell, run the New-RoleGroup cmdlet and specify the -CustomRecipientWriteScope parameter.

Correct Answer: B

Reference: https://docs.microsoft.com/en-us/powershell/module/exchange/role-based-access-control/newroleassignmentpolicy?view=exchange-ps

QUESTION 3

You have a Microsoft 365 subscription that uses a default domain named contoso.com.

Users report that email messages from a domain named fabrikam.com are identified as spam even though the messages are legitimate.

You need to prevent messages from fabrikam.com from being identified as spam.

What should you do?

A. Create a new remote domain.

B. Edit a spam filter policy.

C. Enable the safe list on a connection filter.

D. Enable the Zero-hour auto purge (ZAP) email protection feature.

Correct Answer: C

Safe list: The safe list is a dynamic allow list in the Microsoft datacenter that requires no customer configuration. Microsoft identifies these trusted email sources from subscriptions to various third-party lists. You enable or disable the use of the safe list; you can\\'t configure the source email servers on the safe list. Spam filtering is skipped on incoming messages from the email servers on the safe list.

Incorrect:

*

Remote Domains are an organizational setting that allow you to control certain message types such as “Out of Office” and “Non-Delivery Reports”.

*

In Microsoft 365 organizations with mailboxes in Exchange Online, zero-hour auto purge (ZAP) is an email protection feature that retroactively detects and neutralizes malicious phishing, spam, or malware messages that have already been delivered to Exchange Online mailboxes.

Reference: https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/configure-the-connection-filter-policy?view=o365-worldwide

QUESTION 4

You have a Microsoft Exchange Online tenant.

The mail exchanger (MX) record of your company points to a third-party message hygiene provider that forwards email messages to the tenant.

You need to ensure that Exchange Online can filter the email by using the original IP address of the sender\\'s company.

What should you do?

A. Modify the Inbound connector to use the -EFSkipIPs parameter.

B. Modify the Receive connector to use the -EFSkipIPs parameter.

C. Enable DMARC.

D. Create a remote domain.

Correct Answer: A

Reference: https://docs.microsoft.com/en-us/exchange/mail-flow-best-practices/use-connectors-to-configure-mail-flow/enhanced-filtering-for-connectors

QUESTION 5

You have a hybrid deployment that contains a Microsoft Exchange Online tenant and an on-premises Exchange Server 2019 server named Server1. All users use an email address suffix of @contoso.com.

You migrate 200 mailboxes from Server1 to Exchange Online by using Exchange PowerShell cmdlets. Users hosted on Server1 can send email messages to the migrated mailboxes.

In Microsoft 365, you create a new mailbox that uses an email address of user1@contoso.com.

When email is sent from the mailboxes hosted on Server1 to user1@contoso.com, the senders receive a non-delivery report (NDR) that contains the following text:

"550 5.1.10 RESOLVER.ADR.RecipientNotFound;

Recipient not found by SMTP address lookup."

You verify that Microsoft 365 mailboxes can send email to user1@contoso.com successfully.

You delete the user account and mailbox of User1.

You need to ensure that when new mailboxes are created, all the users at your company can exchange email successfully

Which two actions should you perform? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. From Azure AD Connect, modify the synchronization settings

B. From Server1, run the New-RemoteMailbox cmdlet

C. From Server1, run the Enable-Mailbox cmdlet

D. From the on-premises network, create new mailboxes, and then migrate the mailboxes to Microsoft 365

E. From the Exchange admin center, modify the properties of the Outbound connector

Correct Answer: BD

The problem happens because the on-premise Exchange server is not aware of the existence of the mailbox created in Exchange Online. To prevent this happening, new mailboxes need to be created from the on-premise Exchange server.

You can create on Exchange Online mailbox from the on-premise server by running New- RemoteMailbox cmdlet. Alternatively, you can create a local mailbox on the on-premise server and then migrate the mailbox to Exchange Online.

QUESTION 6

You have a Microsoft Exchange Online tenant named contoso.com.

You create a partnership with two other companies named fabhkam.com and wingtiptoys.com. All the mailboxes of fabnkam.com are hosted in Microsoft 365. All the mailboxes of wingtiptoys.com are hosted in an on-premises Exchange

Server 2019 organization.

You need to ensure that all the email messages sent from contoso.com to fabrikam.com and wingtiptoys.com is encrypted by using TLS.

What should you do?

A. Configure one connector.

B. Create an organizational relationship.

C. Create two remote domains.

D. Run the Office 365 Exchange Hybrid Configuration wizard.

E. Configure two mail flow rules.

Correct Answer: A

Reference: https://docs.microsoft.com/en-us/exchange/mail-flow-best-practices/use-connectors-to-configure-mail-flow/set-up-connectors-for-secure-mail-flow-with-a-partner

QUESTION 7

You have a hybrid deployment between a Microsoft Exchange Online tenant and an Exchange Server 2019 organization.

You need to enable journaling for outbound email.

Where can you store the journal reports?

A. an Exchange Server 2019 mailbox

B. a mail-enabled public folder

C. an Exchange Online mailbox

D. a Microsoft SharePoint Online document library

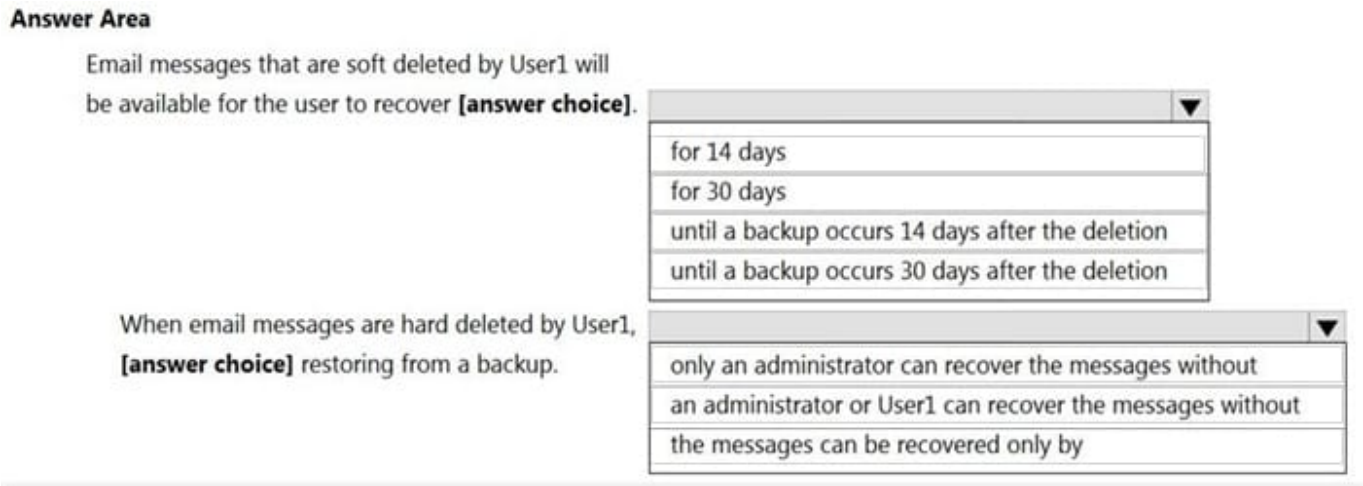
Correct Answer: B

QUESTION 8

HOTSPOT

You are evaluating the email hygiene configuration of a Microsoft Exchange Server 2019 organization.

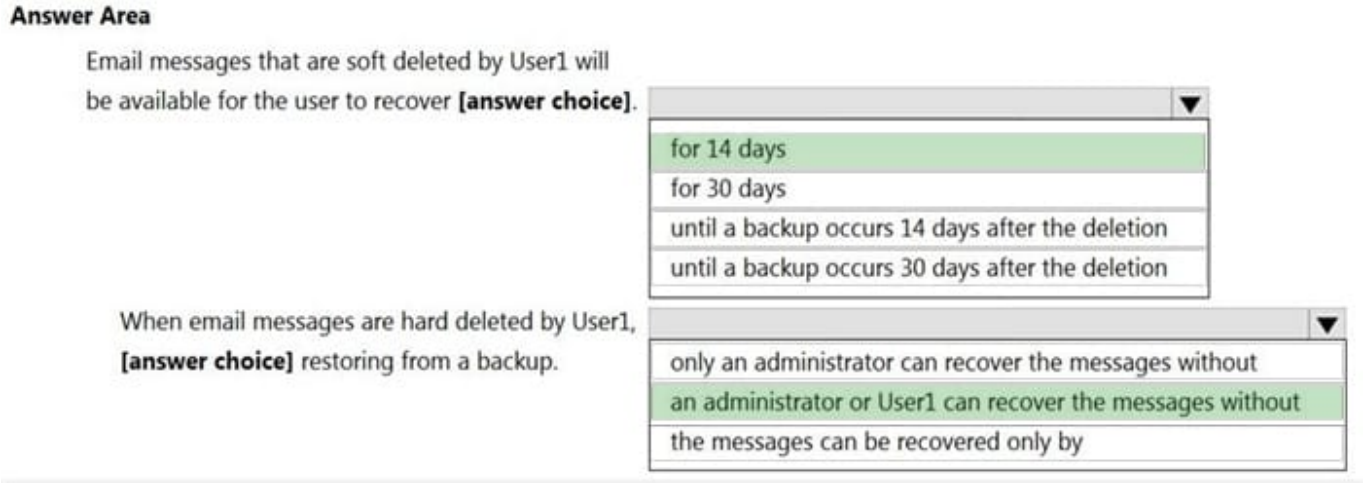
You run the command shown in the following exhibit.



Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:

Answer Area

Priority	1	
Status	On	
Last modified	December 10, 2018	
Policy setting	Policy name	Test
	Description	
	Applied to	If the recipient domain is: M365x051451.onmicrosoft.com
Impersonation	Users to protect	Off
	Protect all domains I own	Off
	Protect specific domains	Off
	Action > User impersonation	Don't apply any action
	Action > Domain impersonation	Don't apply any action
	Safety tips > User impersonation	Off
	Safety tips > Domain impersonation	Off
	Safety tips > Unusual characters	Off
	Mailbox intelligence	On
Spoof	Enable antispoofing protection	On
	Action	Move message to the recipients' Junk Email folders
Advanced settings	Advanced phishing thresholds	1 - Standard

Reference: https://docs.microsoft.com/en-us/powershell/module/exchange/antispam-antimalware/set-contentfilterconfig?view=exchange-ps

QUESTION 9

You have a hybrid deployment between a Microsoft Exchange Online tenant and an on-premises Exchange Server 2019 server.

Users report that the email they send to external recipients is marked as spam.

You need to validate the Reverse DNS and Sender ID data for the on-premises server.

What should you use in the Microsoft Remote Connectivity Analyzer?

A. Exchange Online Custom Domains DNS Connectivity Test

B. Message Analyzer

C. Inbound SMTP Email

D. Outbound SMTP Email

Correct Answer: D

Outbound SMTP E-Mail: This test checks your outbound IP address for certain requirements. This includes Reverse DNS, Sender ID, and RBL checks. Reference: https://docs.microsoft.com/en-us/exchange/clients-and-mobile-in-exchange-online/remote-connectivity-analyzer-tests

QUESTION 10

You have a Microsoft Exchange Online tenant that uses an email domain named contoso.corn.

An in-caning email messages route through an third-party filtering service named Filter1 to connector named Connector

You discover that incoming messages contain headers that specify the source IP address as Filter1.

You to ensure that incoming email messages contain headers that specify source IP address of the original sender. The solution must prevent any charges to the service.

What should you do?

A. From Microsoft 365 Defender portal configure enhanced filtering for Connector1.

B. Configure Connector to authenticate messages by using the IP address of Filter service.

C. Configure the MX Of contoso.com to point to contoso-can.mailgotection.outbok.com.

D. From the Exchange admin center. create a transport rule to rewrite header for incoming messages.

Correct Answer: C

QUESTION 11

You need to ensure that all email messages received from an organization named contoso.com are encrypted by using TLS.

A. See explanation below.

B. PlaceHolder

C. PlaceHolder

D. PlaceHolder

Correct Answer: A

Navigate to Mail flow in the Exchange Admin Center, > Connectors.

The Connectors screen appears.

Click +Add a connector. The New connector screen appears.

Name	Operating system	Microsoft Outlook version
Device1	Windows	Outlook 2019
Device2	MacOS	Outlook 2016 for Mac
Device3	iOS	Outlook for iOS
Device4	Windows	Outlook on the web

Under Connection from, choose Partner organization.

Object type	Configuration	Location
Accepted domain	Contoso.com	Microsoft 365
Remote domain	*	Microsoft 365
Outbound connector	Use DNS routing	Microsoft 365
Inbound connector	Default settings	Microsoft 365
Mail exchanger (MX) record	Contoso-com.mail.protection.outlook.com	Public DNS
Send connector	Use DNS routing	Exchange Server 2019

Click Next. The Connector name screen appears.

Provide a name for the connector and click Next. The Authenticating sent email screen appears.

Choose one of the two options between By verifying that the sender domain matches one of the following domains and By verifying that the IP address of the sending server matches one of the following IP addresses, which belong to your

partner organization.

Click Next. The Security restrictions screen appears.

Check the check box for Reject email messages if they aren\\'t sent over TLS.

Check the check box for Reject email messages if they aren\\'t sent from within this IP address range, and provide the IP address range.

Click Next. The Review connector screen appears.

Review the settings you have configured, and click Create connector.

QUESTION 12

You need to encrypt email between Fabrikam and Litware to support the planned changes. What should you configure in the Exchange admin center?

A. a connector

B. an organization relationship

C. a sharing policy

D. a remote domain

Correct Answer: A

Reference: https://docs.microsoft.com/en-us/exchange/mail-flow-best-practices/use-connectors-to-configure-mail-flow/set-up-connectors-for-secure-mail-flow-with-a-partner

QUESTION 13

You have a Microsoft Exchange Server 2019 hybrid deployment that contains the public folders shown in the following table.

```
PS C:\> Get-Mailbox | Select-Object Alias, RecipientTypeDetails | FT –AutoSize

Alias                                                RecipientTypeDetails
-----                                                --------------------
Mailbox1                                             SharedMailbox
Mailbox2                                             RoomMailbox
```

You plan to migrate the public folders to Exchange Online to improve the collaboration options available to users. Which public folders can be migrated to Office 365 groups without losing the folders\\' existing functionality?

A. PF2 and PF3 only

B. PF2 only

C. PF1 and PF2 only

D. PF1 only

E. PF3 only

Correct Answer: A

Not PF1. Office 365 groups are `flat\\' so you would lose the folder hierarchy.

Reference: https://docs.microsoft.com/en-us/exchange/collaboration/public-folders/migrate-to-microsoft-365-groups?view=exchserver-2019

QUESTION 14

You have a Microsoft 365 subscription that contains a sensitivity label named Confidential and a data loss prevention (DLP) policy named Policy1. Policy1 contains a rule named Rule1. Policy1 is applied to the Exchange email location. Rule1 is configured as shown in the following table.

Office	Subnet
London	192.168.8.0/22
New York	192.168.28.0/22
Paris	192.168.48.0/22

You need to ensure that when a user applies the Confidential sensitivity label to an email and sends the email to an external recipient, the message is forwarded to the user\\'s manager for approval. What should you do?

A. Modify the protection settings of the Confidential sensitivity label.

B. Add a user override to Rule1.

C. Add an action to Rule1.

D. Modify the policy settings of the Confidential sensitivity label policy.

Correct Answer: C

Data loss prevention (DLP) helps you prevent the unintentional or accidental sharing of sensitive information.

DLP examines email messages and files for sensitive information, like a credit card number. Using DLP you can detect sensitive information, and take action.

When editing a rule within a DLP policy, you can change:

1.

The actions that are taken, such as restricting access to the content.

2.

Etc.

Actions included in the DLP policy tips: Forward the message for approval to sender\\'s manager.

Reference: https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-policy-reference
https://docs.microsoft.com/en-us/microsoft-365/compliance/dlp-policy-tips-reference

QUESTION 15

You have a Microsoft Exchange Server 2019 organization.

You need to ensure that all email is retained for one year, and then moved to an archive mailbox.

What should you use?

A. a default policy tag

B. a data loss prevention (DLP) policy

C. a personal tag

D. a retention policy tag

Correct Answer: A

https://docs.microsoft.com/en-us/exchange/policy-and-compliance/mrm/retention-tags-and-retention-policies?view=exchserver-2019