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 need to ensure that a notification email is sent to compliance@constoso.com when a user marks an email message as Not Junk in Microsoft Outlook.

A. See explanation below.

B. PlaceHolder

C. PlaceHolder

D. PlaceHolder

Correct Answer: A

Go to the Microsoft 365 Defender portal and under Email and collaboration select Policies and rules > Alert policy.

An alert policy consists of the following settings and conditions.

Activity the alert is tracking. You create a policy to track an activity or in some cases a few related activities, such a sharing a file with an external user by sharing it, assigning access permissions, or creating an anonymous link. When a

user performs the activity defined by the policy, an alert is triggered based on the alert threshold settings.

Activity conditions. For most activities, you can define additional conditions that must be met to trigger an alert. Common conditions include IP addresses (so that an alert is triggered when the user performs the activity on a computer with a

specific IP address or within an IP address range), whether an alert is triggered if a specific user or users perform that activity, and whether the activity is performed on a specific file name or URL. You can also configure a condition that

triggers an alert when the activity is performed by any user in your organization. The available conditions are dependent on the selected activity.

You can also define user tags as a condition of an alert policy. This results in the alerts triggered by the policy to include the context of the impacted user. You can use system user tags or custom user tags.

When the alert is triggered. You can configure a setting that defines how often an activity can occur before an alert is triggered. This allows you to set up a policy to generate an alert every time an activity matches the policy conditions, when

a certain threshold is exceeded, or when the occurrence of the activity the alert is tracking becomes unusual for

your organization.If you select the setting based on unusual activity, Microsoft establishes a baseline value that defines the normal frequency for the selected activity. It takes up to seven days to establish this baseline, during which alerts

won\\'t be generated. After the baseline is established, an alert is triggered when the frequency of the activity tracked by the alert policy greatly exceeds the baseline value. For auditing-related activities (such as file and folder activities), you

can establish a baseline based on a single user or based on all users in your organization; for malware-related activities, you can establish a baseline based on a single malware family, a single recipient, or all messages in your organization.

Alert category. To help with tracking and managing the alerts generated by a policy, you can assign one of the following categories to a policy.

1.

Data loss prevention

2.

Information governance

3.

Mail flow

4.

Permissions

5.

Threat management

6.

Others

When an activity occurs that matches the conditions of the alert policy, the alert that\\'s generated is tagged with the category defined in this setting. This allows you to track and manage alerts that have the same category setting on the Alerts

page in the compliance center because you can sort and filter alerts based on category.

Alert severity. Similar to the alert category, you assign a severity attribute (Low, Medium, High, or Informational) to alert policies. Like the alert category, when an activity occurs that matches the conditions of the alert policy, the alert that\\'s

generated is tagged with the same severity level that\\'s set for the alert policy. Again, this allows you to track and manage alerts that have the same severity setting on the Alerts page. For example, you can filter the list of alerts so that only

alerts with a High severity are displayed.

Email notifications. You can set up the policy so that email notifications are sent (or not sent) to a list of users when an alert is triggered. You can also set a daily notification limit so that once the maximum number of notifications has been

reached, no more notifications are sent for the alert during that day. In addition to email notifications, you or other

administrators can view the alerts that are triggered by a policy on the Alerts page.

Consider enabling email notifications for alert policies of a specific category or that have a higher severity setting.

QUESTION 2

DRAG DROP

You have a Microsoft Exchange Server 2019 organization.

You plan to implement a hybrid deployment between Exchange Online and Exchange Server.

You need to install the Exchange Online Hybrid Agent. The solution must use the principle of least privilege.

To which roles should you be assigned to perform the installation? To answer, drag the appropriate roles to the correct products. Each role 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.

NOTE: Each correct selection is worth one point.

Select and Place:

Department	Archive	Single item recovery
Finance	Enabled	Enabled
Manufacturing	Disabled	Disabled
Sales	Disabled	Disabled
Marketing	Enabled	Enabled

Correct Answer:

Administrator	Management role group	Organization	Management role
Admin1	Organization Management, Discovery Management	Exchange Online, on-premises	*None*
Admin2	Organization Management, Discovery Management	Exchange Online, on-premises	Mailbox Import Export

Reference: https://docs.microsoft.com/en-us/exchange/hybrid-deployment/hybrid-agent

QUESTION 3

HOTSPOT

Your company purchases new mobile devices for each user in its sales department and marketing department. The new devices only support Exchange ActiveSync.

You need to configure mobile device access to meet the following requirements:

1.

Apply a specific password policy to all the sales department users.

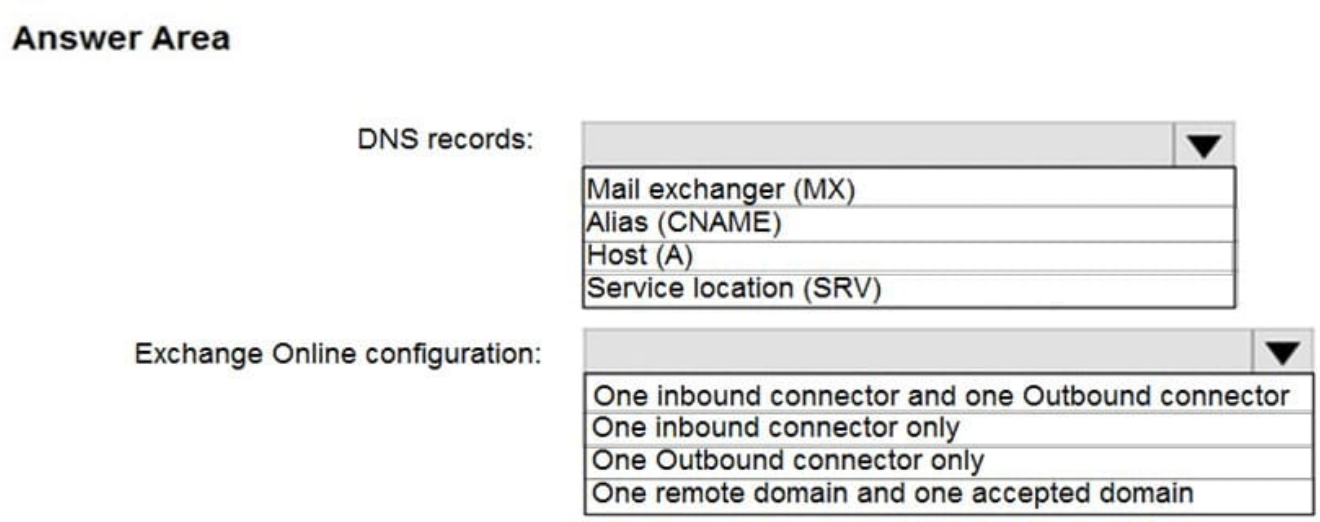
2.

Prevent all the marketing department users from using ActiveSync to access their mailbox from their new mobile devices.

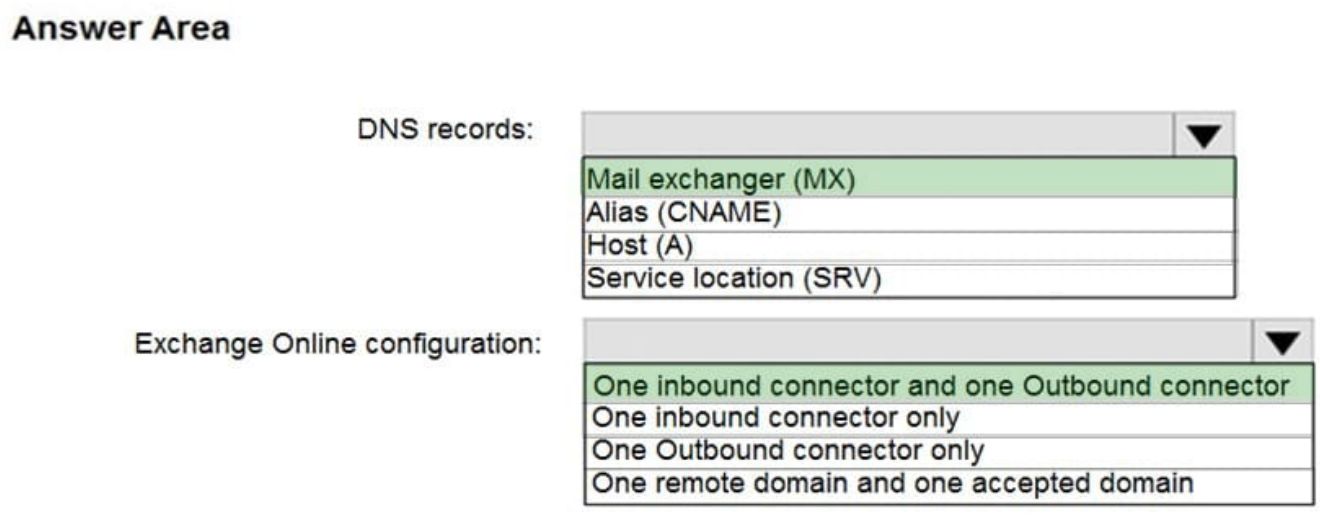
What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



QUESTION 4

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 5

You have a Microsoft Exchange Online tenant.

Users report that legitimate email messages are delivered to their Junk Email folder.

You plan to use the Microsoft Remote Connectivity Analyzer to identify the cause of the issue.

Which test should you run?

A. Outlook Connectivity

B. Inbound SMTP Email

C. Outbound SMTP Email

D. Message Analyzer

Correct Answer: D