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.pass4itsure.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 prevent email messages that contain attachments that have the .js file extension from being delivered to any recipients in your organization.

To complete this task, sign in to the Microsoft 365 admin center.

A. See explanation below.

B. PlaceHolder

C. PlaceHolder

D. PlaceHolder

Correct Answer: A

1.

Go to Mail flow > Rules.

2.

Create the rule by using one of the following options:

-

To create a rule from a template, click Add and select a template.

-

To copy a rule, select the rule, and then select Copy .

-

To create a new rule from scratch, Add and then select Create a new rule.

3.

In the New rule dialog box, name the rule, and then select the conditions and actions for this rule:

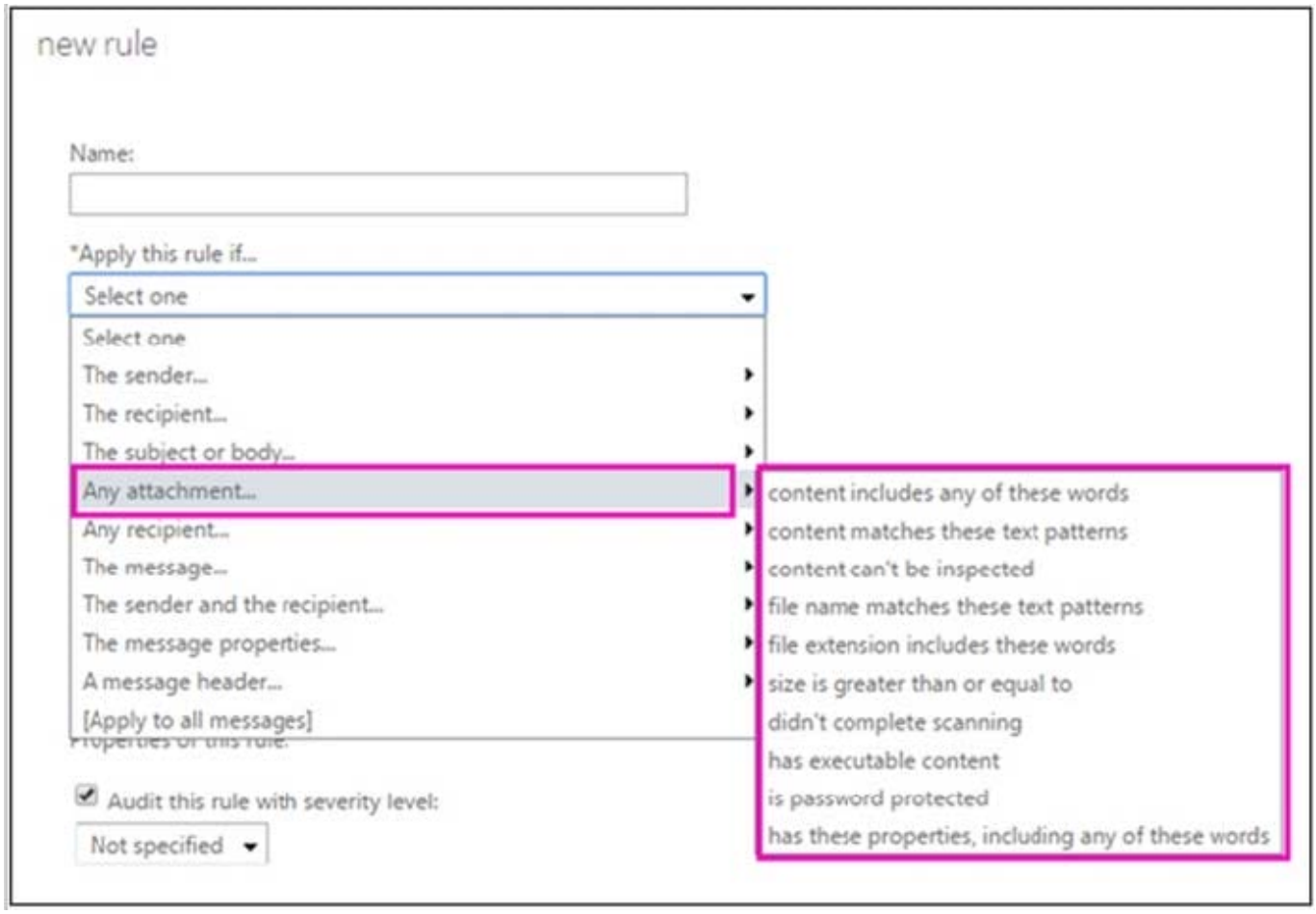
-In Apply this rule if..., select the condition you want from the list of available conditions: Some conditions require you to specify values. For example, if you select The sender is... condition, you must specify a sender address. If you\\'re adding a word or phrase, note that trailing spaces are not allowed. If the condition you want isn\\'t listed, or if you need to add exceptions, select More options. Additional conditions and exceptions will be listed. If you don\\'t want to specify a condition, and want this rule to apply to every message in your organization, select [Apply to all messages] condition.

- In Do the following..., select the action you want the rule to take on messages matching the criteria from the list of available actions: Some of the actions will require you to specify values. For example, if you select the Forward the message for approval to... condition, you will need to select a recipient in your organization. If the condition you want isn\\'t listed, select More options. Additional conditions will be listed.

- Specify how rule match data for this rule is displayed in the Data Loss Prevention (DLP) reports and the Mail protection reports.

- Set the mode for the rule. You can use one of the two test modes to test the rule without impacting mail flow. In both test modes, when the conditions are met, an entry is added to the message trace: Enforce: This turns on the rule and it starts processing messages immediately. All actions on the rule will be performed. Test with Policy Tips: This turns on the rule, and any Policy Tip actions (Notify the sender with a Policy Tip) will be sent, but no actions related to message delivery will be performed. Data Loss Prevention (DLP) is required in order to use this mode. Test without Policy Tips: Only the Generate incident report action will be enforced. No actions related to message delivery are performed.

Exchange Online admins can create mail flow rules in the Exchange admin center (EAC) at Mail flow > Rules. You need permissions to do this procedure. After you start to create a new rule, you can see the full list of attachment-related conditions by clicking More options > Any attachment under Apply this rule if. The attachment-related options are shown in the following diagram.



Reference:

https://docs.microsoft.com/en-us/exchange/security-and-compliance/mail-flow-rules/manage-mail-flow-rules

https://docs.microsoft.com/en-us/exchange/security-and-compliance/mail-flow-rules/inspect-message-attachments

QUESTION 2

You have a Microsoft Exchange Online tenant that has Office 365 Advanced Threat Protection (ATP) enabled.

The tenant contains a user named Ben Smith who has a UPN of ben.smith@fabrikam.com. Ben Smith is protected by using an ATP anti-phishing policy.

Ben Smith reports that emails sent from his personal account of ben.smith@relecloud.com are not delivered to his work email account.

You need to ensure that personal emails are delivered to the ben.smith@fabrikam.com

What should you do?

A. Create a transport rule to assign the MS-Exchange-Organization-PhishThresholdLevel header a value of 2 for the message received from ben.smith@relecloud.com

B. Add ben.smith@fabrikam.com as a trusted sender to the ATP anti-phishing policy.

C. Add ben.smith@relecloud.com as a trusted sender to the ATP anti phishing.

D. Add relecloud.com to the ATP anti-phishing list of misted domains.

Correct Answer: C

Reference: https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/configure-atp-anti-phishing-policies?view=o365-worldwide

QUESTION 3

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while

others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

You have a Microsoft Exchange Server 2019 organization that contains 200 mailboxes.

You need to add a second email address to each mailbox. The address must have a syntax that uses the first letter of each user\\'s last name, followed by the user\\'s first name, and then @fabrikam.com.

Solution: You create an email address policy that uses the %1g%s@fabrikam.com email address format.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Reference: https://docs.microsoft.com/en-us/exchange/email-addresses-and-address-books/email-address-policies/email-address-policies?view=exchserver-2019

QUESTION 4

You have an Exchange Online tenant.

You need to ensure that the users in your company\\'s finance department can select email messages that will be deleted automatically one year later. The solution must apply only to the finance department users.

Which two actions should you perform? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Publish a label to the finance department.

B. Create a data loss prevention (DLP) policy that uses the sensitive information type.

C. For each mailbox in the finance department, configure the retention policy settings.

D. Create a label that has a retention setting of one year.

E. For each mailbox in the finance department, configure Message Delivery Restrictions.

Correct Answer: AD

Create a retention label and publish it to the finance department users.

Reference: https://docs.microsoft.com/en-us/microsoft-365/compliance/retention?view=o365-worldwide

QUESTION 5

Another administrator at contoso.com plans to deploy an SMTP smart host that uses an IP address of 131.107.2.200.

You need to prepare a solution to route all emails sent to users in the @contoso.com domain from your organization by using the SMTP host. The solution must have a status set to Off until the administrator deploys the smart host.

To complete this task, sign in to the Exchange admin center.

A. See explanation below.

B. PlaceHolder

C. PlaceHolder

D. PlaceHolder

Correct Answer: A

1.

In the EAC, navigate to Mail flow > Send connectors, and then click Add +. This starts the New Send connector wizard.

2.

On the first page, enter the following information:

-Name: Enter a descriptive name for the Send connector, for example, Smart host to Internet.

-Type: Select a descriptive value. For example, Internet or Custom.

When you\\'re finished, click Next.

3.

On the next page, select Route mail through smart hosts, and then click Add +. In the Add smart host dialog box that appears, identify the smart host by using one of the following values:

-IP address: For example, 192.168.3.2.

-Fully qualified domain name (FQDN): For example, securitydevice01.contoso.com. Note that the Exchange source servers for the Send connector must be able to resolve the smart host in DNS by using this FQDN.

When you\\'re finished, click Save.

4.

You can enter multiple smart hosts by repeating Step 3. When you\\'re finished, click Next.

5.

On the next page, in the Route mail through smart hosts section, select the authentication method that\\'s required by the smart host. Valid values are:

6.

When you\\'re finished, click Next.

7.

On the next page, in the Address space section, click Add +. In the Add domain dialog box that appears, enter the following information:

TABLE 1

Authentication mechanism	Description
None	No authentication. For example, when access to the smart host is restricted by the source IP address.
Basic authentication	Basic authentication. Requires a username and password. The username and password are sent in clear text.
Offer basic authentication only after starting TLS	Basic authentication that's encrypted with TLS. This requires a server certificate on the smart host that contains the exact FQDN of the smart host that's defined on the Send connector.
Exchange Server authentication	Generic Security Services application programming interface (GSSAPI) and Mutual GSSAPI authentication.
Externally secured	The connection is presumed to be secured by using a security mechanism that's external to Exchange. The connection may be an Internet Protocol security (IPsec) association or a virtual private network (VPN). Alternatively, the servers may reside in a trusted, physically controlled network.

-Type: Verify SMTP is entered.

-Fully Qualified Domain Name (FQDN): Enter an asterisk (*) to indicate the Send connector applies to messages addressed to all external domains. Alternatively, you can enter a specific external domain (for example, contoso.com), or a domain and all subdomains (for example, *.contoso.com).

-Cost: Verify 1 is entered. A lower value indicates a more preferred route for the domains you specified. When you\\'re finished, click Save.

8. Back on the previous page, the Scoped send connector setting is important if your organization has Exchange servers installed in multiple Active Directory sites:

-If you don\\'t select Scoped send connector, the connector is usable by all transport servers (Exchange 2013 or later Mailbox servers and Exchange 2010 Hub Transport servers) in the entire Active Directory forest. This is the default value.

-If you select Scoped send connector, the connector is only usable by other transport servers in the same Active Directory site.

When you\\'re finished, click Next.

9. On the next page, in the Source server section, click Add +. In the Select a Server dialog box that appears, select one or more Mailbox servers that you want to use to send outbound mail to the smart host. If you have multiple Mailbox servers in your environment, select the ones that can route mail to the smart host. If you have only one Mailbox server, select that one. After you\\'ve selected at least one Mailbox server, click Add, click OK, and then click Finish.

After you create the Send connector, it appears in the Send connector list.

From the Send connector list, you can turn the connector on or off.

Reference: https://docs.microsoft.com/en-us/exchange/mail-flow/connectors/outbound-smart-host-routing?view=exchserver-2019#how-do-you-know-this-worked