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

The tenant uses an email domain named @contoso.com.

You recently purchased an email domain named fabrikam.com.

You need to ensure that all the users in the tenant can receive email messages by using the @fabrikam.com email domain. The solution must ensure that the users can continue to receive email by using the @contoso.com email domain.

Which three actions should you perform? Each correct answer presents part of the solution. NOTE; Each correct selection is worth one point.

A. From Azure AD Connect add a domain for fabrikam.com.

B. From the on-premises Exchange admin center, add an accepted domain for fabrikam.com.

C. From the Exchange Management Shell, create a script that runs the

D. From the Microsoft 365 admin center, verify the fabrikam.com email domain

E. From the on-premises Exchange admin center, modify the email address policy

F. From the Microsoft 365 admin center, add the fabrikam.com email domain.

Correct Answer: BDE

QUESTION 2

You have two servers named EXCH1 and EXCH2 that run Windows Server 2012 R2 and have Microsoft Exchange Server 2016 installed.

You purchase a Microsoft 365 subscription. You plan to configure a hybrid deployment between an Exchange Online tenant and the on-premises Exchange Server organization.

You need to identify the prerequisites to installing the Microsoft Hybrid Agent on EXCH1 and EXCH2.

Which two prerequisites should you identify? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. Enable TLS 1.2.

B. Upgrade the operating system of EXCH1 and EXCH2 to Windows Server 2019.

C. Enable Hybrid Modem Authentication (HMA).

D. Allow outbound HTTPS connections to Microsoft Online Services.

Correct Answer: AD

Microsoft Hybrid Agent System requirements

The Hybrid Agent has multiple methods of installation with different requirements. In all cases, the core computer requirements are the same as described in the following list:

Windows Server 2012 R2, Windows Server 2016, or Windows Server 2019

.NET Framework 4.6.2 or later, as supported by the version of Exchange version.

TLS 1.2 enabled.

Azure Application Proxy

Capable of establishing outbound HTTPS connections to the internet.

Capable of establishing HTTPS connections to the Exchange Server chosen for hybrid configuration.

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

QUESTION 3

You need to prevent email messages from a domain named fabrikam.com from being delivered to the mailboxes of 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.

In the Microsoft 365 Defender portal at https://security.microsoft.com, go to Email and Collaboration > Policies and Rules > Threat policies > Anti-spam in the Policies section. To go directly to the Anti-spam policies page, use https://security.microsoft.com/antispam.

2.

On the Anti-spam policies page, click Create policy and then select Inbound from the drop down list.

3.

The policy wizard opens. On the Name your policy page, configure these settings:

-Name: Enter a unique, descriptive name for the policy.

-Description: Enter an optional description for the policy.

When you\\'re finished, click Next.

4.

On the Users, groups, and domains page that appears, identify the internal recipients that the policy applies to (recipient conditions):

-Users: The specified mailboxes, mail users, or mail contacts in your organization.

-Groups: The specified distribution groups, mail-enabled security groups, or Microsoft 365 Groups in your organization.

-Domains: All recipients in the specified accepted domains in your organization.

Click in the appropriate box, start typing a value, and select the value that you want from the results. Repeat this process as many times as necessary. To remove an existing value, click remove × next to the value.

For users or groups, you can use most identifiers (name, display name, alias, email address, account name, etc.), but the corresponding display name is shown in the results. For users, enter an asterisk (*) by itself to see all available

values. Multiple values in the same condition use OR logic (for example, or). Different conditions use AND logic (for example, and).

- Exclude these users, groups, and domains: To add exceptions for the internal recipients that the policy applies to (recipient exceptions), select this option and configure the exceptions. The settings and behavior are exactly like the

conditions. When you\\'re finished, click Next.

5. On the Bulk email threshold and spam properties page that appears, configure the following settings:

- Bulk email threshold: Specifies the bulk complaint level (BCL) of a message that triggers the specified action for the Bulk spam filtering verdict that you configure on the next page (greater than the specified value, not greater than or equal

to). A higher value indicates the message is less desirable (more likely to resemble spam). The default value is 7. For more information, see Bulk complaint level (BCL) in EOP and What\\'s the difference between junk email and bulk email?. By default, the PowerShell only setting MarkAsSpamBulkMail is On in anti-spam policies. This setting dramatically affects the results of a Bulk filtering verdict: MarkAsSpamBulkMail is On: A BCL that\\'s greater than the threshold is converted to an SCL 6 that corresponds to a filtering verdict of Spam, and the action for the Bulk filtering verdict is taken on the message. MarkAsSpamBulkMail is Off: The message is stamped with the BCL, but no action is taken for a Bulk filtering verdict. In effect, the BCL threshold and Bulk filtering verdict action are irrelevant.

-Increase spam score, Mark as spam* and Test mode: Advanced Spam Filter (ASF) settings that are turned off by default.

The Contains specific languages and from these countries settings are not part of ASF.

- Contains specific languages: Click the box and select On or Off from the drop down list. If you turn it on, a box appears. Start typing the name of a language in the box. A filtered list of supported languages will appear. When you find the language that you\\'re looking for, select it. Repeat this step as many times as necessary. To remove an existing value, click remove × next to the value.

- From these countries*: Click the box and select On or Off from the drop down list. If you turn it on, a box appears. Start typing the name of a country in the box. A filtered list of supported countries will appear. When you find the country

that you\\'re looking for, select it. Repeat this step as many times as necessary. To remove an existing value, click remove × next to the value. When you\\'re finished, click Next.

6. On the Actions page that appears, configure the following settings:

-Message actions: Select or review the action to take on messages based on the following spam filtering verdicts: Spam High confidence spam Phishing High confidence phishing Bulk

-

Retain spam in quarantine for this many days: Specifies how long to keep the message in quarantine if you selected Quarantine message as the action for a spam filtering verdict. After the time period expires, the message is deleted, and is not recoverable. A valid value is from 1 to 30 days.

-

Add this X-header text: This box is required and available only if you selected Add X-header as the action for a spam filtering verdict. The value you specify is the header field name that\\'s added to the message header. The header field value is always This message appears to be spam.

- Prepend subject line with this text: This box is required and available only if you selected Prepend subject line with text as the action for a spam filtering verdict. Enter the text to add to the beginning of the message\\'s subject line.

-

Redirect to this email address: This box is required and available only if you selected the Redirect message to email address as the action for a spam filtering verdict. Enter the email address where you want to deliver the message. You can enter multiple values separated by semicolons (;).

-Enable safety Tips: By default, Safety Tips are enabled, but you can disable them by clearing the checkbox.

- Enable zero-hour auto purge (ZAP): ZAP detects and takes action on messages that have already been delivered to Exchange Online mailboxes.

ZAP is turned on by default. When ZAP is turned on, the following settings are available: Enable ZAP for phishing messages: By default, ZAP is enabled for phishing detections, but you can disable it by clearing the checkbox. Enable ZAP for spam messages: By default, ZAP is enabled for spam detections, but you can disable it by clearing the checkbox.

When you\\'re finished, click Next.

7. On the Allow and block list flyout that appears, you are able to configure message senders by email address or email domain that are allowed to skip spam filtering. In the Allowed section, you can configure allowed senders and allowed domains. In the Blocked section, you can add blocked senders and blocked domains. The steps to add entries to any of the lists are the same:

-Click the link for the list that you want to configure: Allowed > Senders: Click Manage (nn) sender(s). Allowed > Domains: Click Allow domains. Blocked > Senders: Click Manage (nn) sender(s). Blocked > Domains: Click Block domains.

-In the flyout that appears, do the following steps: Click + Add senders or Add domains. In the Add senders or Add domains flyout that appears, enter the sender\\'s email address in the Sender box or the domain in the Domain box. As you\\'re typing, the value appears below the box. When you\\'re finished typing the email address or domain, select the value below the box. Repeat the previous step as many times as necessary. To remove an existing value, click remove × next to the value.

When you\\'re finished, click Add senders or Add domains.

- Back on the main flyout, the senders or domains that you added are listed on the page. To remove an entry from this page, do the following steps: Select one or more entries from the list. You can also use the Search box to find values in the list. After you select at least one entry, the delete icon appears Click the delete icon to remove the selected entries

When you\\'re finished, click Done.

Back on the Allow and block list page, click Next when you\\'re read to continue.

8.

On the Review page that appears, review your settings. You can select Edit in each section to modify the settings within the section. Or you can click Back or select the specific page in the wizard. When you\\'re finished, click Create.

9.

On the confirmation page that appears, click Done.

Reference: https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/configure-your-spam-filter-policies?view=o365-worldwide

---

QUESTION 4

You have a Microsoft Exchange Online tenant.

All users are assigned only an Office 365 Enterprise E3 license.

You need to ensure that the users can use only Microsoft Outlook to connect to their Microsoft 365 mailbox when they connect from an Android device.

What should you create?

A. a conditional access policy in Azure Active Directory (Azure AD)

B. a connection filter policy in Exchange Online Protection (EOP)

C. an Outlook Web App policy in Exchange Online

D. an app protection policy in Microsoft Endpoint Manager

Correct Answer: A

Office 365 Enterprise E3 includes Azure Active Directory Premium P1 which is required for Azure conditional access policies.

QUESTION 5

You have a Microsoft 365 subscription that contains two users named User1 and User2.

User1 reports to have received a suspicious email message that appears to have come from User2.

You identify that the message was sent by an external user impersonating User2.

You need to block email that contains the email address of an impersonated sender.

What should you configure?

A. a Tenant Allow/Block Lists rule

B. an anti-phishing policy

C. an anti-spam policy

D. an Enhanced filtering rule

Correct Answer: A

Explanation:

You can use the Microsoft 365 Defender portal to create block entries for spoofed senders in the Tenant Allow/Block List.

You can also use PowerShell to create block entries for spoofed senders in the Tenant Allow/Block List

In Exchange Online PowerShell, use the following syntax:

New-TenantAllowBlockListSpoofItems -Identity Default -Action Block -SpoofedUser -SendingInfrastructure -SpoofType

This example creates a block entry for the sender laura@adatum.com from the source 172.17.17.17/24.

PowerShell

New-TenantAllowBlockListSpoofItems -Identity Default -Action Allow -SendingInfrastructure Reference: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/tenant-allow-block-list-email-spoof-configure