# 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.geekcert.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 Online tenant.

You plan to place a hold on all email messages stored in the mailbox of a user named User1.

What should you create first?

A. an eDiscovery case

B. sensitive info type

C. a data loss prevention (DLP) policy

D. an information barrier segment

Correct Answer: A

You can use an eDiscovery case to create and manage eDiscovery holds that can be applied to user mailboxes and other content locations in Microsoft Purview1. You can also use an eDiscovery case to search for and export content from

mailboxes and other locations1.

An eDiscovery case is different from a Litigation Hold, which is a hold that is applied to user mailboxes in Exchange Online1. A Litigation Hold isn\\'t identified by a GUID1. A sensitive info type is a predefined or custom entity that can be used to

identify and protect sensitive data in Microsoft Purview2. It is not related to placing a hold on email messages.

A data loss prevention (DLP) policy is a policy that helps prevent the accidental or intentional sharing of sensitive information outside your organization2. It is not related to placing a hold on email messages.

An information barrier segment is a group of users who are allowed or blocked from communicating with each other in Microsoft Teams or SharePoint Online2. It is not related to placing a hold on email messages.

**QUESTION 2**

You have a Microsoft Exchange Online tenant that uses a third-party email gateway device.

You discover that inbound email messages are delayed.

The gateway device receives the following error message when sending email to the tenant.

4.7.500 Server busy, please try again later. You need to prevent inbound email delays. What should you configure?

A. Organization Sharing

B. an MX record for the domain

C. a transport rule

D. a connector

Correct Answer: D

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

**QUESTION 3**

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

On Server1, you create a new mailbox that uses an email address of user1@contoso.com

Users hosted in Exchange Online report that they receive a non-delivery report (NDR) When they attempt to send email messages to user1@contoso.com. The NDR contains the following text: "User1 wasn\\'t found at contoso.com."

You verify that the Exchange Online users can send email successfully to the other mailboxes hosted on Server1. Users hosted on Server1 can send email to user1@contoso.com successfully.

You need to identify what causes the email delivery to fail. What should you use?

A. the Azure Active Directory admin center

B. the Exchange admin center

C. Azure AD Connect Health

D. the on-premises Exchange admin center

Correct Answer: C

It\\'s likely that the new user account hasn\\'t replicated to Azure Active Directory. Azure AD Connect is responsible for account replication between on-prem AD and Azure AD.

**QUESTION 4**

You need to reduce the likelihood that malicious links contained in emails received by mailboxes in @lab.CloudCredential(1).TenantName are opened.

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.

Navigate to the Exchange Admin Center, and then choose the Advanced Threats section of the EAC.

2.

Click the Safe Links tab to examine all existing Safe Links policies:

3.

After navigating to the Safe Links policy page, choose the Add button (+) to create a new policy. The New Safe Links Policy window opens.

-In the resulting window we'll be presented with the options available for creating our new Safe Links policy.

4.

In Name enter an appropriate, unique, name that describes this policy. In the description enter some text that provides a little more detail for anyone trying to make sense of the options selected here.

5.

Next we'll choose the action to take for URLs. We can leave this Off, if for example we are creating a policy to exclude a group of users that would otherwise be affected by another Safe Links policy.

6.

The checkbox Do not track user click can be selected if you do not wish to use the reporting functionality available at a later date. This is a key feature when understanding which users clicked a link that was later found to be a threat, so be careful about choosing to disable user click tracking.

7.

Our final check box provides options for click-through is a link is found to be dangerous. In some circumstances you may trust users to click-through links, or they may request the ability to do so. In most circumstances you will not want a user to click-through the malicious link.

8.

Some URLs, such as those for internal addresses or even trusted partners, may not require re-writing. Enter these URLs here.

9.

Finally, we will select the scope for the rule under the Applied to section.

10.Using similar conditions to transport rules we can select who this rule applies to including:

-Individual recipients

-Recipient domains

-Members of distribution groups 11.The same conditions can be used for exceptions. When you have configured your rule, choose Save.

After saving the new Safe Links rule it will be shown in the EAC list. Just like Transport Rules, you can use the Enabled column to enable or disable the Safe Links policy.

Reference: https://techgenix.com/implementing-exchange-online-advanced-threat-protection-part2/

**QUESTION 5**

Lynne Robbins and the users in the sales department plan to collaborate on a project with a partner company named Contoso, Ltd. that has an email domain named contoso.com.

You need to ensure that only the sales department users can share all their calendar free/busy

information with the users in contoso.com.

How should you configure the organization relationship?

A. Select Calendar free/busy information with time only and enter Group1.

B. Select Calendar free/busy information with time, subject, and location and enter Group2.

C. Select Calendar free/busy information with time, subject, and location and enter Group3.

D. Select Calendar free/busy information with time only and enter Group3.

E. Select Calendar free/busy information with time only and enter Group2.

Correct Answer: C

Reference: https://docs.microsoft.com/en-us/exchange/sharing/organization-relationships/create-an-organization-relationship