



Free Questions for MS-203 by actualtestdumps

Shared by Callahan on 06-06-2022

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

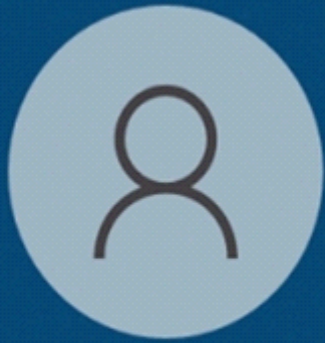
Please wait while the virtual machine loads. Once loaded, you may proceed to the lab section. This may take a few minutes, and the wait time will not be deducted from your overall test time.

When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external websites) will not be possible by design.

Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.

Labs are not timed separately, and this exam may have more than one lab that you must complete. You can use as much time as you would like to complete each lab. But, you should manage your time appropriately to ensure that you are able to complete the lab(s) and all other sections of the exam in the time provided.

Please note that once you submit your work by clicking the Next button within a lab, you will NOT be able to return to the lab.



ExamUser

Sign in

ENG



Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password, place your cursor in the Enter password box and click on the password below.

Microsoft 365 Username: admin@abc.com

Microsoft 365 Password: xxxxxx

If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support purposes only.

Lab Instance: XXXXXX

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.

Options:

A- Explanation:

Go toMail flow>Rules.

Create the rule by using one of the following options:

+



+

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:

-
-
-

- In **Do the following...**, select the action you want the rule to take on messages matching the criteria from the list of available actions:

-
-

- 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:

-
-
-

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.

new rule

Name:

*Apply this rule if...

Select one

Select one

The sender...

The recipient...

The subject or body...

Any attachment...

Any recipient...

The message...

The sender and the recipient...

The message properties...

A message header...

[Apply to all messages]

Properties of this rule:

Audit this rule with severity level:

Not specified

- ▶ content includes any of these words
- ▶ content matches these text patterns
- ▶ content can't be inspected
- ▶ file name matches these text patterns
- ▶ file extension includes these words
- ▶ size is greater than or equal to
- ▶ didn't complete scanning
- ▶ has executable content
- ▶ is password protected
- ▶ has these properties, including any of these words

Answer:

A

Explanation:

<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

Question Type: MultipleChoice

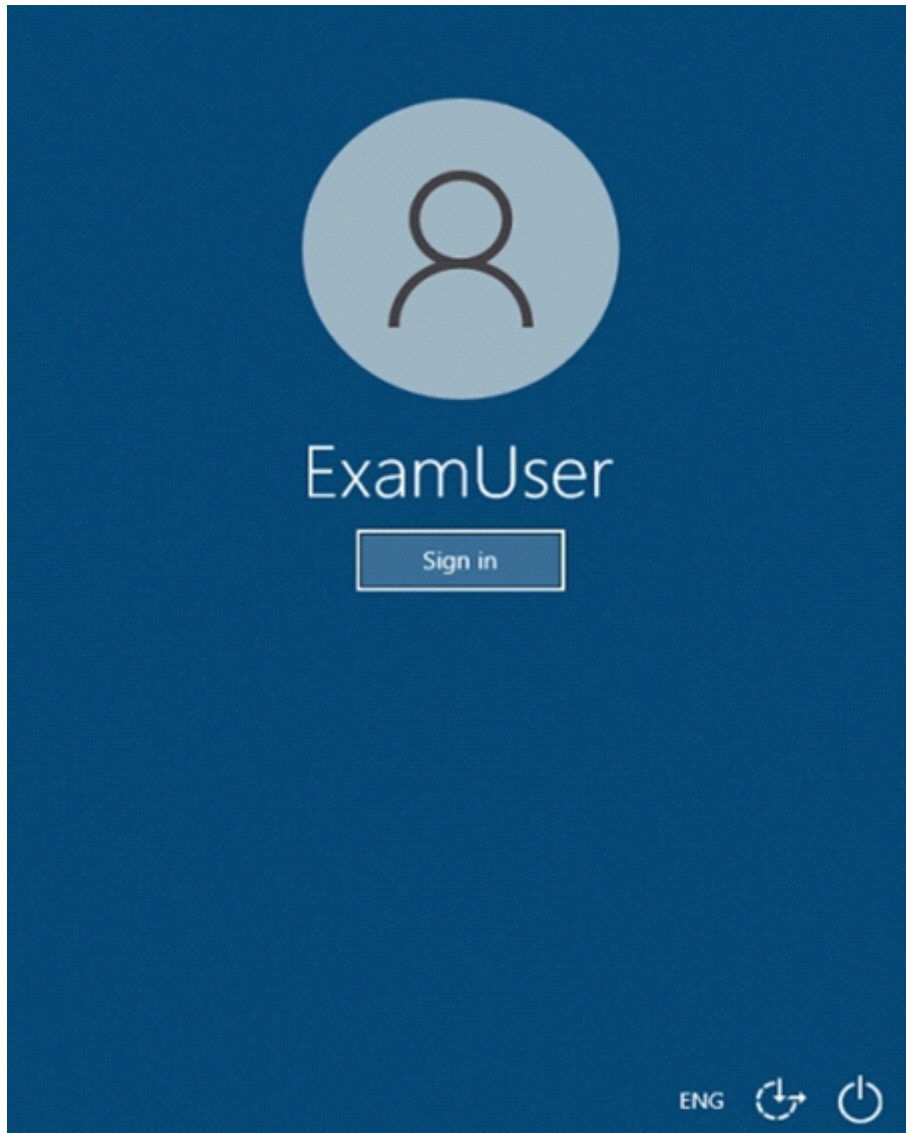
Please wait while the virtual machine loads. Once loaded, you may proceed to the lab section. This may take a few minutes, and the wait time will not be deducted from your overall test time.

When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external websites) will not be possible by design.

Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.

Labs are not timed separately, and this exam may have more than one lab that you must complete. You can use as much time as you would like to complete each lab. But, you should manage your time appropriately to ensure that you are able to complete the lab(s) and all other sections of the exam in the time provided.

Please note that once you submit your work by clicking the Next button within a lab, you will NOT be able to return to the lab.



Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password, place your cursor in the Enter password box and click on the password below.

Microsoft 365 Username: admin@abc.com

Microsoft 365 Password: xxxxxx

If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support purposes only.

Lab Instance: XXXXXX

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.

Options:

A- Explanation:

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

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

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**.

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, <recipient1> or <recipient2>). Different conditions use AND logic (for example, <recipient1> and <member of group 1>).

- **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**.

On the **Bulk email threshold & 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 **MarkAsSpamBulkMailIsOn** in anti-spam policies. This setting dramatically affects the results of a **Bulk filtering** verdict:

- **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**.

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:
 -
 -
 -
 -
- 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:

-
-

When you're finished, click **Next**.

On the **Allow & 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:

-
-
-

- In the flyout that appears, do the following steps:

-
-
-

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:

-

-
-

When you're finished, clickDone.

Back on theAllow & block listpage, clickNextwhen you're read to continue.

On theReviewpage that appears, review your settings. You can selectEditin each section to modify the settings within the section. Or you can clickBackor select the specific page in the wizard.

When you're finished, clickCreate.

On the confirmation page that appears, clickDone.

Answer:

A

Explanation:

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

Question 3

Question Type: MultipleChoice

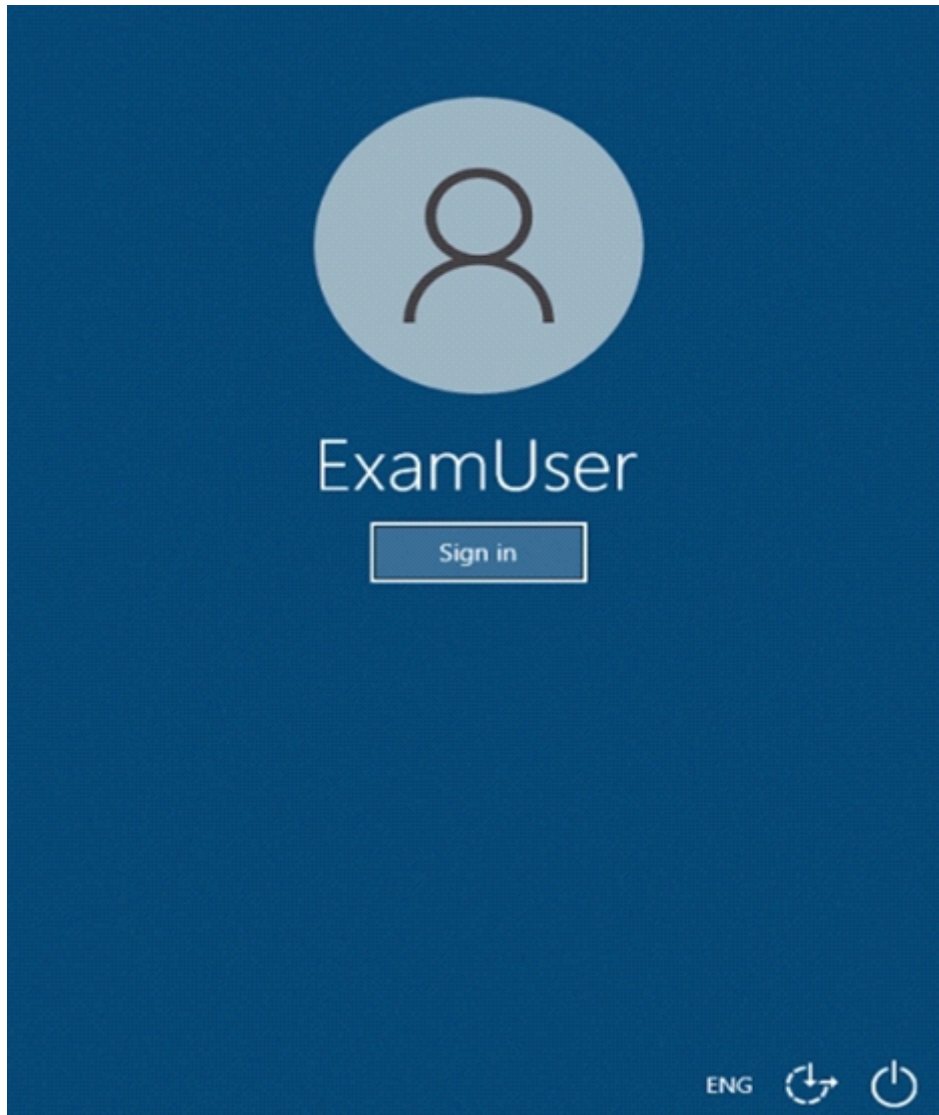
Please wait while the virtual machine loads. Once loaded, you may proceed to the lab section. This may take a few minutes, and the wait time will not be deducted from your overall test time.

When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external websites) will not be possible by design.

Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.

Labs are not timed separately, and this exam may have more than one lab that you must complete. You can use as much time as you would like to complete each lab. But, you should manage your time appropriately to ensure that you are able to complete the lab(s) and all other sections of the exam in the time provided.

Please note that once you submit your work by clicking the Next button within a lab, you will NOT be able to return to the lab.



Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password, place your cursor in the Enter password box and click on the password below.

Microsoft 365 Username: admin@abc.com

Microsoft 365 Password: xxxxxx

If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support purposes only.

Lab Instance: XXXXXX

You need to ensure that all email messages in the mailbox of a user named Pradeep Gupta are retained for 90 days.

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

Options:

A- Explanation:

Go to the Microsoft 365 admin center and then click Users > Active users.

Select Pradeep Gupta.

On the properties flyout page, click the Mail tab, and then under More actions, click Manage litigation hold.



Abraham McMahon

[Reset password](#) [Block sign-in](#) [Delete user](#)

[Change photo](#)

[Account](#) [Devices](#) [Licenses and apps](#) **Mail** [OneDrive](#)

Mailbox permissions



Email apps

POP blocked
OWA blocked
IMAP blocked
Other email apps allowed

[Manage email apps](#)

Show in global address list

Yes

[Manage global address list visibility](#)

Email forwarding

None

[Manage email forwarding](#)

Automatic replies

On

[Manage automatic replies](#)

More actions

[Convert to shared mailbox](#)

[Edit Exchange properties](#)

[Manage litigation hold](#)

On the Manage litigation hold flyout page, select the Turn on litigation hold checkbox and then enter the following optional information:

-
-
-

Click Save changes on the Litigation hold flyout page to create the hold.

The system displays a banner saying it might take up to 240 minutes for the change to take effect.

Answer:

A

Explanation:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/create-a-litigation-hold?view=o365-worldwide>

Question 4

Question Type: MultipleChoice

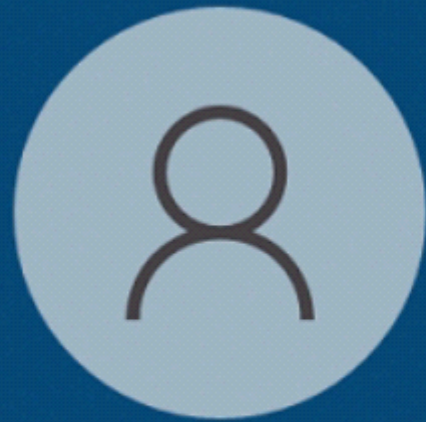
Please wait while the virtual machine loads. Once loaded, you may proceed to the lab section. This may take a few minutes, and the wait time will not be deducted from your overall test time.

When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external websites) will not be possible by design.

Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.

Labs are not timed separately, and this exam may have more than one lab that you must complete. You can use as much time as you would like to complete each lab. But, you should manage your time appropriately to ensure that you are able to complete the lab(s) and all other sections of the exam in the time provided.

Please note that once you submit your work by clicking the Next button within a lab, you will NOT be able to return to the lab.



ExamUser

Sign in

Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password, place your cursor in the Enter password box and click on the password below.

Microsoft 365 Username: admin@abc.com

Microsoft 365 Password: xxxxxx

If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support purposes only.

Lab Instance: XXXXXX

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

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

Options:

A- Explanation:

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

Click+Add a connector. TheNew connectorscreen appears.

New connector

Specify your mail flow scenario, and we'll let you know if you need to set up a connector.

Connection from

- Office 365
- Your organization's email server
- Partner organization

Connection to

Under Connection from, choose Partner organization.

New connector

Specify your mail flow scenario, and we'll let you know if you need to set up a connector.

Connection from

- Office 365
- Your organization's email server
- Partner organization

Connection to

- Office 365

Click Next. The Connector namescreen appears.

Provide a name for the connector and click Next. The Authenticating sent emails 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.

ClickNext. TheReview connectorscreen appears.

Review the settings you have configured, and clickCreate connector.

Answer:

A

Explanation:

<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 5

Question Type: MultipleChoice

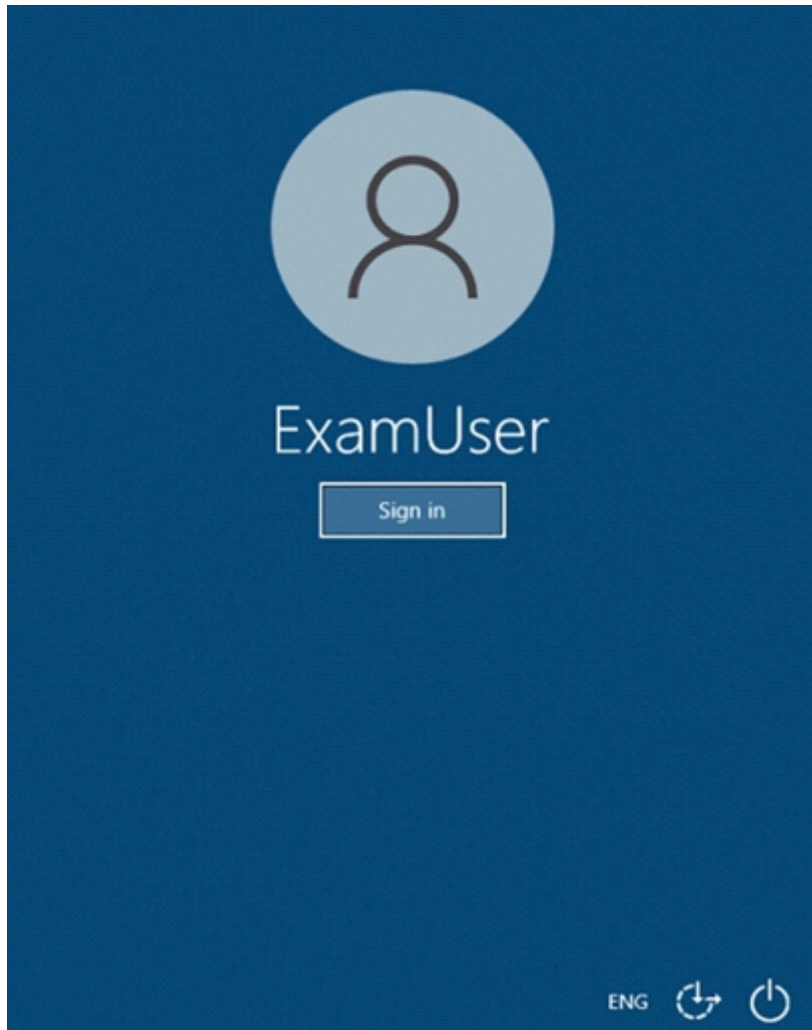
Please wait while the virtual machine loads. Once loaded, you may proceed to the lab section. This may take a few minutes, and the wait time will not be deducted from your overall test time.

When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external websites) will not be possible by design.

Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.

Labs are not timed separately, and this exam may have more than one lab that you must complete. You can use as much time as you would like to complete each lab. But, you should manage your time appropriately to ensure that you are able to complete the lab(s) and all other sections of the exam in the time provided.

Please note that once you submit your work by clicking the Next button within a lab, you will NOT be able to return to the lab.



Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password, place your cursor in the Enter password box and click on the password below.

Microsoft 365 Username: admin@abc.com

Microsoft 365 Password: xxxxxx

If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support purposes only.

Lab Instance: XXXXXX

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.

Options:

A- Explanation:

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

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

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.

In the Name field 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.

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.

The checkbox Do not track user clicks 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.

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.

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

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

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

- Individual recipients
- Recipient domains
- Members of distribution groups

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.

Answer:

A

Explanation:

Question 6

Question Type: MultipleChoice

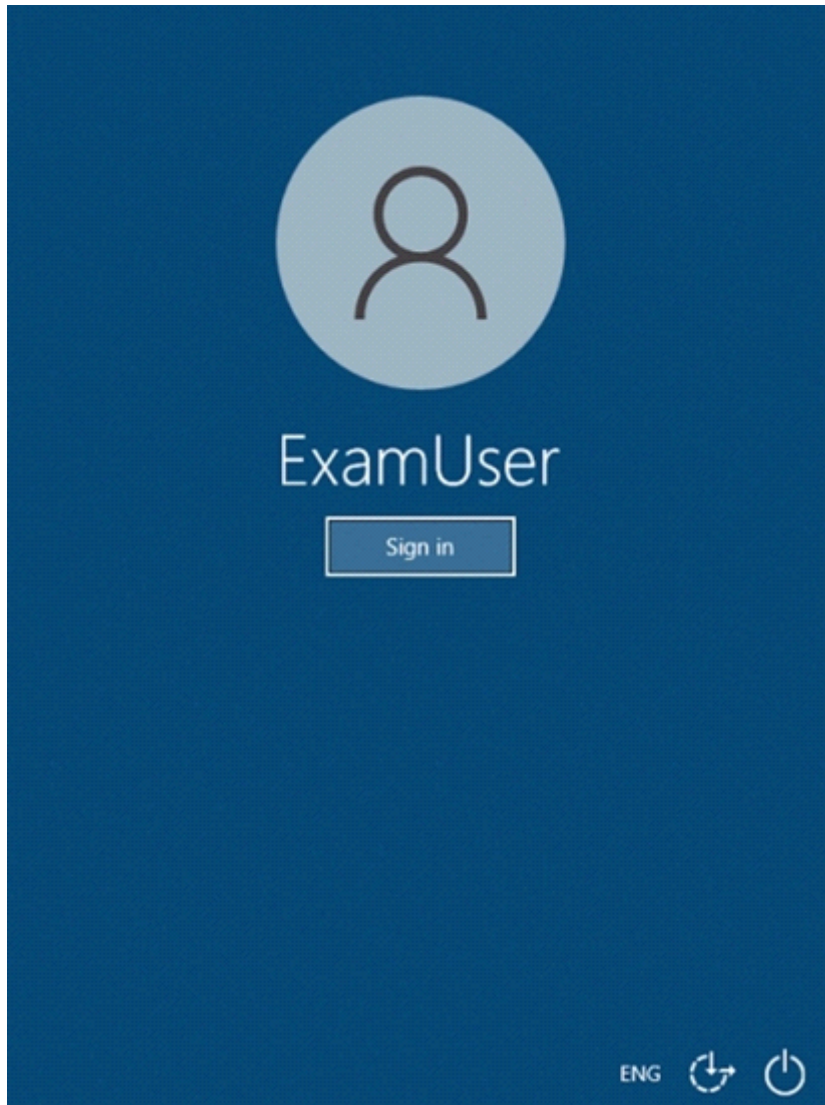
Please wait while the virtual machine loads. Once loaded, you may proceed to the lab section. This may take a few minutes, and the wait time will not be deducted from your overall test time.

When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external websites) will not be possible by design.

Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.

Labs are not timed separately, and this exam may have more than one lab that you must complete. You can use as much time as you would like to complete each lab. But, you should manage your time appropriately to ensure that you are able to complete the lab(s) and all other sections of the exam in the time provided.

Please note that once you submit your work by clicking the Next button within a lab, you will NOT be able to return to the lab.



Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password, place your cursor in the Enter password box and click on the password below.

Microsoft 365 Username: admin@abc.com

Microsoft 365 Password: xxxxxx

If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support purposes only.

Lab Instance: XXXXXX

You need to ensure that when emails containing an attachment that uses an .ace extension is sent to your company, the email is blocked. Each time an email is blocked, a notification must be sent to security@contoso.com.

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

Options:

A- Explanation:

In the EAC, in the left navigation pane, select mail flow, and then select rules.

Select New(+), and then select Create a new rule.

In the New Rule window, select More options.

In the Name box, specify a name for the new rule.

Select the *Apply this rule if drop-down list, point to Any attachment, and then select File extension includes these words.

In the Specify words or phrases window, type the file name extension of any attachment that you want to block, and then select the plus symbol (+) to add the file name extension to the list. When the list is completed, select OK.

Select the Do the following drop-down list, point to Block the message, and then select Reject the message and include an explanation or select Delete the message without notifying anyone.

If it's required, add a statement to inform users who will receive the non-delivery report (NDR) of the reason that mail delivery failed, and then select OK.

Specify any additional options such as rule auditing and rule activation or deactivation time, and then select Save.

Answer:

A

Explanation:

<https://docs.microsoft.com/en-us/exchange/troubleshoot/email-delivery/how-to-block-message-from-being-sent-or-received>

Question 7

Question Type: MultipleChoice

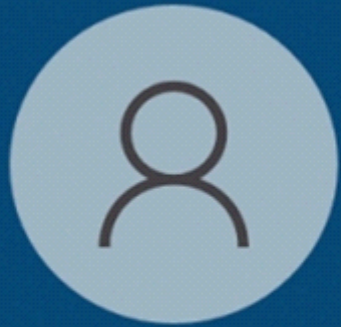
Please wait while the virtual machine loads. Once loaded, you may proceed to the lab section. This may take a few minutes, and the wait time will not be deducted from your overall test time.

When the Next button is available, click it to access the lab section. In this section, you will perform a set of tasks in a live environment. While most functionality will be available to you as it would be in a live environment, some functionality (e.g., copy and paste, ability to navigate to external websites) will not be possible by design.

Scoring is based on the outcome of performing the tasks stated in the lab. In other words, it doesn't matter how you accomplish the task, if you successfully perform it, you will earn credit for that task.

Labs are not timed separately, and this exam may have more than one lab that you must complete. You can use as much time as you would like to complete each lab. But, you should manage your time appropriately to ensure that you are able to complete the lab(s) and all other sections of the exam in the time provided.

Please note that once you submit your work by clicking the Next button within a lab, you will NOT be able to return to the lab.



ExamUser

Sign in

ENG



Use the following login credentials as needed:

To enter your username, place your cursor in the Sign in box and click on the username below.

To enter your password, place your cursor in the Enter password box and click on the password below.

Microsoft 365 Username: admin@abc.com

Microsoft 365 Password: xxxxxx

If the Microsoft 365 portal does not load successfully in the browser, press CTRL-K to reload the portal in a new browser tab.

The following information is for technical support purposes only.

Lab Instance: XXXXXX

You need to ensure that all emails sent from the users in your company to recipients who use a suffix of @fabnkam.com are encrypted by using Microsoft Office 365 Message Encryption (OME).

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

Options:

A- Explanation:

In the Microsoft 365 admin center, choose Admin centers > Exchange.

In the EAC, go to Mail flow > Rules and select New+ > Create a new rule.

In Name, type a name for the rule, such as Encrypt mail for DrToniRamos@hotmail.com.

In Apply this rule if, select a condition, and enter a value if necessary. For example, to encrypt messages going to DrToniRamos@hotmail.com:

-
-

- To select an existing name, select it from the list and then click OK.

- To enter a new name, type an email address in the check names box and then select check names > OK.

To add more conditions, choose More options and then choose add condition and select from the list.

For example, to apply the rule only if the recipient is outside your organization, select add condition and then select The recipient is external/internal > Outside the organization > OK.

To enable encryption using the new OME capabilities, from Do the following, select Modify the message security and then choose Apply Office 365 Message Encryption and rights protection. Select an RMS template from the list, choose Save, and then choose OK.

Answer:

A

Explanation:

<https://docs.microsoft.com/en-us/microsoft-365/compliance/define-mail-flow-rules-to-encrypt-email?view=o365-worldwide>

To Get Premium Files for MS-203 Visit

<https://www.p2pexams.com/products/ms-203>

For More Free Questions Visit

<https://www.p2pexams.com/microsoft/pdf/ms-203>

