

Latest Microsoft - MS-102 Practice Test

skillupnext

PRACTICE TEST

MS-102

Microsoft 365
Administrator

N2K



P.S. Free & New MS-102 dumps are available on Google Drive shared by ITPassLeader: <https://drive.google.com/open?id=13uyLBOoyxEpPzThz-rNMwkQyLZ-DoDF>

Most candidates reflect our MS-102 test questions matches more than 90% with the real exam. We get information from special channel. If MS-102 exam change questions, we will get the first-hand real questions and our professional education experts will work out the right answers so that MS-102 Test Questions materials produce. If you are looking for valid & useful exam study materials, our products are suitable for you. We offer one year free updates for every buyer so that you can share latest MS-102 test questions within a year.

Microsoft MS-102 Exam Syllabus Topics:

Topic	Details
Topic 1	<ul style="list-style-type: none">• Manage security and threats by using Microsoft Defender XDR: This topic discusses how to use Microsoft Defender portal to manage security reports and alerts. It also focuses on usage of Microsoft Defender for Office 365 to implement and manage email and collaboration protection. Lastly, it discusses the usage of Microsoft Defender for Endpoint for the implementation and management of endpoint protection.
Topic 2	<ul style="list-style-type: none">• Manage compliance by using Microsoft Purview: Implementation of Microsoft Purview information protection and data lifecycle management is discussed in this topic. Moreover, questions about implementing Microsoft Purview data loss prevention (DLP) also appear.
Topic 3	<ul style="list-style-type: none">• Deploy and manage a Microsoft 365 tenant: Management of roles in Microsoft 365 and management of users and groups are discussion points of this topic. It also focuses on implementing and managing a Microsoft 365 tenant.
Topic 4	<ul style="list-style-type: none">• Implement and manage Microsoft Entra identity and access: In this topic, questions about Microsoft Entra tenant appear. Moreover, it delves into implementation and management of authentication and secure access.

Microsoft MS-102 Valid Exam Vce | MS-102 Test Assessment

with our MS-102 exam dumps for 20 to 30 hours, we can claim that our customers are confident to take part in your MS-102 exam and pass it for sure. In the progress of practicing our MS-102 study materials, our customers improve their abilities in passing the MS-102 Exam, we also upgrade the standard of the exam knowledge. Therefore, this indeed helps us establish a long-term cooperation relationship on our exam braindumps.

Microsoft 365 Administrator Sample Questions (Q443-Q448):

NEW QUESTION # 443

You have a Microsoft 365 subscription that uses Microsoft Defender for Office 365.

You need to configure policies to meet the following requirements:

Customize the common attachments filter.

Enable impersonation protection for sender domains.

Which type of policy should you configure for each requirement? To answer, drag the appropriate policy types to the correct requirements. Each policy type 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.

Policy Types	Answer Area
<input type="text" value="Anti-malware"/>	Customize the common attachments filter: <input type="text"/>
<input type="text" value="Anti-phishing"/>	Enable impersonation protection for sender domains: <input type="text"/>
<input type="text" value="Anti-spam"/>	
<input type="text" value="Safe Attachments"/>	

Answer:

Explanation:

Policy Types	Answer Area
<input type="text" value="Anti-malware"/>	Customize the common attachments filter: <input type="text" value="Anti-malware"/>
<input type="text" value="Anti-phishing"/>	Enable impersonation protection for sender domains: <input type="text" value="Anti-phishing"/>
<input type="text" value="Anti-spam"/>	
<input type="text" value="Safe Attachments"/>	

Explanation

A close-up of a question Description automatically generated

Policy Types	Answer Area
<input type="text" value="Anti-malware"/>	Customize the common attachments filter: <input type="text" value="Anti-malware"/>
<input type="text" value="Anti-phishing"/>	Enable impersonation protection for sender domains: <input type="text" value="Anti-phishing"/>
<input type="text" value="Anti-spam"/>	
<input type="text" value="Safe Attachments"/>	

Box 1: Anti-malware

Customize the common attachments filter.

See step 5 below.

1. Use the Microsoft 365 Defender portal to create anti-malware policies In the Microsoft 365 Defender portal at <https://security.microsoft.com>, go to Email & Collaboration > Policies & Rules > Threat policies > Anti-Malware in the Policies section. To go directly to the Anti-malware page, use <https://security.microsoft.com/antimalwarev2>

2. On the Anti-malware page, select Create to open the new anti-malware policy wizard.

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.

3. When you're finished on the Name your policy page, select Next.

4. On the Users and domains page, identify the internal recipients that the policy applies to (recipient conditions)

5. On the Protection settings page, configure the following settings:

Protection settings section:

Enable the common attachments filter: If you select this option, messages with the specified attachments are treated as malware and are automatically quarantined. You can modify the list by clicking Customize file types and selecting or deselecting values in the list.

6. Etc.

Box 2: Anti-phishing

Enable impersonation protection for sender domains.

Anti-phishing policies in Microsoft 365

The high-level differences between anti-phishing policies in EOP and anti-phishing policies in Defender for Office 365 are described in the following table:

Feature	Anti-phishing policies in EOP	Anti-phishing policies in Defender for Office 365
Automatically created default policy	✓	✓
Create custom policies	✓	✓
Common policy settings*	✓	✓
Spoof settings	✓	✓
First contact safety tip	✓	✓
Impersonation settings		✓
Advanced phishing thresholds		✓

Reference:

<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-malware-policies-configure>

<https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-phishing-policies-about>

NEW QUESTION # 444

You have a Microsoft 365 E5 subscription that has published sensitivity labels shown in the following exhibit.

Home > sensitivity

Labels Label policies Auto-labeling (preview)

Sensitivity labels are used to classify email messages, documents, sites, and more. When a label is applied (automatically or by the user), the content or site is protected based on the settings you choose. For example, you can create labels that encrypt files, add content marking, and control user access to specific sites. [Learn more about sensitivity labels](#)

+ Create a label Publish labels Refresh

Name ↑	Order	Created by	Last modified
Label1	0 - highest	Prvi	04/24/2020
Label2		Prvi	04/24/2020
Label3	0 - highest	Prvi	04/24/2020
Label4	0 - highest	Prvi	04/24/2020
Label5	5	Prvi	04/24/2020
Label6	0 - highest	Prvi	04/24/2020

Which labels can users apply to content?

- A. Label3, Label4, and Label6 only
- B. Label1, Label2, Label3, Label4, Label5, and Label6
- C. Label1, Label2, and Label5 only
- D. Label1, Label3, Label2, and Label6 only

Answer: D

NEW QUESTION # 445

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.

Your network contains an Active Directory forest.

You deploy Microsoft 365.

You plan to implement directory synchronization.

You need to recommend a security solution for the synchronized identities. The solution must meet the following requirements:

- * Users must be able to authenticate successfully to Microsoft 365 services if Active Directory becomes unavailable.
- * User passwords must be 10 characters or more.

Solution: implement password hash synchronization and modify the password settings from the Default Domain Policy in Active Directory.

Does this meet the goal?

- A. No
- B. Yes

Answer: B

NEW QUESTION # 446

HOTSPOT

You have a Microsoft 365 E5 subscription that contains a Microsoft SharePoint site named Site1 and a data loss prevention (DLP) policy named DLP1. DLP1 contains the rules shown in the following table.

Name	Priority	Action
Rule1	0	Notify users by using email and policy tips. Customize the policy tip as Rule1 tip. Disable user overrides.
Rule2	1	Notify users by using email and policy tips. Customize the policy tip as Rule2 tip. Restrict access to the content. Disable user overrides.
Rule3	2	Notify users by using email and policy tips. Customize the policy tip as Rule3 tip. Restrict access to the content. Enable user overrides.
Rule4	3	Notify users by using email and policy tips. Customize the policy tip as Rule4 tip. Restrict access to the content. Disable user overrides.

Site1 contains the files shown in the following table.

Name	Matched DLP rule
File1.docx	Rule1, Rule2, Rule3
File2.docx	Rule1, Rule3, Rule4

Which policy tips are shown for each file? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area

File1.docx:

▼
Rule1 tip only
Rule2 tip only
Rule3 tip only
Rule1 tip and Rule2 tip only
Rule1 tip, Rule2 tip, and Rule3 tip

File2.docx:

▼
Rule1 tip only
Rule3 tip only
Rule4 tip only
Rule1 tip and Rule4 tip only
Rule1 tip, Rule3 tip, and Rule4 tip

Answer:

Explanation:

Answer Area

File1.docx:

Rule1 tip only
Rule2 tip only
Rule3 tip only
Rule1 tip and Rule2 tip only
Rule1 tip, Rule2 tip, and Rule3 tip

File2.docx:

Rule1 tip only
Rule3 tip only
Rule4 tip only
Rule1 tip and Rule4 tip only
Rule1 tip, Rule3 tip, and Rule4 tip

Explanation:

Answer Area

File1.docx:

Rule1 tip only
Rule2 tip only
Rule3 tip only
Rule1 tip and Rule2 tip only
Rule1 tip, Rule2 tip, and Rule3 tip

File2.docx:

Rule1 tip only
Rule3 tip only
Rule4 tip only
Rule1 tip and Rule4 tip only
Rule1 tip, Rule3 tip, and Rule4 tip

Box 1: Rule1 tip only

File1 matches Rule1, Rule2, and Rule3.

Rule1 has the highest priority.

Note: The Priority parameter specifies a priority value for the policy that determines the order of policy processing. A lower integer value indicates a higher priority, the value 0 is the highest priority, and policies can't have the same priority value.

Box 2: Rule1 tip only

Note: User Override support

The option to override is per rule, and it overrides all of the actions in the rule (except sending a notification, which can't be overridden).

It's possible for content to match several rules in a DLP policy or several different DLP policies, but only the policy tip from the most restrictive, highest-priority rule will be shown (including policies in Test mode). For example, a policy tip from a rule that blocks access to content will be shown over a policy tip from a rule that simply sends a notification. This prevents people from seeing a cascade of policy tips.

If the policy tips in the most restrictive rule allow people to override the rule, then overriding this rule also overrides any other rules that the content matched.

Reference:

<https://learn.microsoft.com/en-us/microsoft-365/compliance/dlp-overview-plan-for-dlp>

<https://learn.microsoft.com/en-us/microsoft-365/compliance/use-notifications-and-policy-tips>

NEW QUESTION # 447

HOTSPOT

You have a Microsoft 365 subscription.

You deploy the anti-phishing policy shown in the following exhibit.

Use the drop-down menus to select the answer choice that completes each statement based on the information presented in the graphic.

NOTE: Each correct selection is worth one point.

Answer Area

To ensure that malicious email impersonating the CEO of a partner company is blocked, you must modify the [answer choice] setting.

To minimize disrupting users that frequently exchange legitimate email with the CEO of a partner company, you must configure the [answer choice] setting.

Answer:

Explanation:

Answer Area

To ensure that malicious email impersonating the CEO of a partner company is blocked, you must modify the [answer choice] setting.

To minimize disrupting users that frequently exchange legitimate email with the CEO of a partner company, you must configure the [answer choice] setting.

Explanation:

Answer Area

To ensure that malicious email impersonating the CEO of a partner company is blocked, you must modify the [answer choice] setting.

To minimize disrupting users that frequently exchange legitimate email with the CEO of a partner company, you must configure the [answer choice] setting.

Box 1: Enable users to protect

Anti-phishing policies in Defender for Office 365 also have impersonation settings where you can specify individual sender email addresses or sender domains that will receive impersonation protection.

User impersonation protection

id=13uyLBOoyxEpPztThz-rNMwkQyLZ-DoDF