SC-401専門知識訓練 & SC-401日本語サンプル

2026年JPNTestの最新SC-401 PDFダンプおよびSC-401試験エンジンの無料共有：https://drive.google.com/open?id=1T7nRjOBNJT9xp_Zutcg99UJ6Cuy7_krT

JPNTestのMicrosoftのSC-401試験のトレーニングキットはJPNTestのIT技術専門家たちによって開発されたのです。そのデザインは当面の急速に変化するIT市場と密接な関係があります。JPNTestのトレーニングはあなたを助けて継続的に発展している技術を利用して、問題を解決する能力を高めると同時に仕事についての満足度を向上させることができます。JPNTestのMicrosoftのSC-401の認証したカバー率は１００パーセントに達したのですから、弊社の問題と解答を利用する限り、あなたがきっと気楽に試験に合格することを保証します。

Microsoft SC-401 認定試験の出題範囲:

トピック	出題範囲
トピック 1	• Implement Data Loss Prevention and Retention: This section evaluates Data Protection Officers on designing and managing data loss prevention (DLP) policies and retention strategies. It includes setting policies for data security, configuring Endpoint DLP, and managing retention labels and policies. Candidates must understand adaptive scopes, policy precedence, and data recovery within Microsoft 365.
トピック 2	• Manage Risks, Alerts, and Activities: This section assesses Security Operations Analysts on insider risk management, monitoring alerts, and investigating security activities. It covers configuring risk policies, handling forensic evidence, and responding to alerts using Microsoft Purview and Defender tools. Candidates must also analyze audit logs and manage security workflows.
トピック 3	• Protect Data Used by AI Services: This section evaluates AI Governance Specialists on securing data in AI-driven environments. It includes implementing controls for Microsoft Purview, configuring Data Security Posture Management (DSPM) for AI, and monitoring AI-related security risks to ensure compliance and protection.
トピック 4	• Implement Information Protection: This section measures the skills of Information Security Analysts in classifying and protecting data. It covers identifying and managing sensitive information, creating and applying sensitivity labels, and implementing protection for Windows, file shares, and Exchange. Candidates must also configure document fingerprinting, trainable classifiers, and encryption strategies using Microsoft Purview.

>> SC-401専門知識訓練 <<

Microsoft SC-401日本語サンプル & SC-401試験復習赤本

JPNTestの専門家チームがMicrosoftのSC-401認証試験に対して最新の短期有効なトレーニングプログラムを研究しました。MicrosoftのSC-401「Administering Information Security in Microsoft 365」認証試験に参加者に対して30時間

ぐらいの短期の育成訓練でらくらくに勉強しているうちに多くの知識を身につけられます。

Microsoft Administering Information Security in Microsoft 365 認定 SC-401 試験問題 (Q122-Q127):

質問 # 122
You have a Microsoft 365 E5 subscription that contains a user named User1.
You deploy Microsoft Purview insider risk management.
You need ensure that insider risk management events related to User1 are visible only to specific users.
What should you create?

- A. a priority user group
- B. an indicator variant
- C. a global exclusion
- D. a detection group

正解：D

解説：
You need to prevent users from sharing sensitive information with third-party generative AI websites.
A). Information Protection # Classifies and labels data but does not block sharing with external AI sites.
B). Information Barriers # Restricts communication between groups of users (e.g., compliance walls), not web uploads.
C). Insider Risk Management # Detects risky behavior (like data exfiltration), but does not actively block data sharing.
D). Data Loss Prevention (DLP) # Detects and prevents sensitive data being copied to browsers, USBs, or uploaded to restricted domains (like ChatGPT, Bard, etc.).

質問 # 123
Hotspot Question
You have a Microsoft 365 subscription. Auditing is enabled.
A user named User1 is a member of a dynamic security group named Group1.
You discover that User1 is no longer a member of Group1.
You need to search the audit log to identify why User1 was removed from Group1.
Which two activities should you use in the search? To answer, select the appropriate activities in the answer area.
NOTE: Each correct selection is worth one point.

正解：

解説：
Explanation:
Box 1: Removed member from a group
Audit log activities
Microsoft Entra group administration activities
The following table lists group administration activities that are logged when an admin or a user creates or changes a Microsoft 365 group or when an admin creates a security group by using the Microsoft 365 admin center or the Azure management portal.
* Removed member from group
A member was removed from a group.
* Updated group
A property of a group was changed.
* Etc.
Box 2: Updated group
Reference:
https://learn.microsoft.com/en-us/purview/audit-log-activities

質問 # 124
You have Microsoft 365 E5 subscription that uses data loss prevention (DLP) to protect sensitive information.
You have a document named Form.docx.
You plan to use PowerShell to create a document fingerprint based on Form.docx.
You need to first connect to the subscription.

Which cmdlet should you run?

- A. Connect-SPOService
- B. Connect-ExchangeOnline
- C. Connect-IPPSSession
- D. Connect-MgGraph

正解：C

解説：
Currently, you can create a document fingerprint only in Security & Compliance PowerShell, and Connect-IPPSSession is how you connect to it.
https://learn.microsoft.com/en-us/purview/document-fingerprinting#create-a-custom-sensitive- information-type-based-on-document-fingerprinting-using-powershell
https://learn.microsoft.com/en-us/powershell/module/exchange/connect-ippssession?view=exchange-ps

質問 # 125
You have a Microsoft 365 E5 subscription.
You plan to implement insider risk management for users that manage sensitive data associated with a project.
You need to create a protection policy for the users. The solution must meet the following requirements:
*Minimize the impact on users who are NOT part of the project.
*Minimize administrative effort.
What should you do first?

- A. From the Microsoft Purview portal, create an insider risk management policy.
- B. From the Microsoft Entra admin center, create a security group.

正解：B

解説：
C From the Microsoft Entra admin center create a User risk policy
D From the Microsoft Purview portal create a priority user group
Explanation:
To implement insider risk management for users managing sensitive project data while minimizing the impact on other users and reducing administrative effort, you should first create a security group in Microsoft Entra ID (formerly Azure AD).
Security groups allow you to scope insider risk management policies to specific users instead of applying policies to all users, which helps in minimizing unnecessary alerts and reducing administrative overhead. After creating the security group, you can assign this group to a Microsoft Purview Insider Risk Management policy, ensuring that only project-related users are affected.

質問 # 126
SIMULATION
Username and password
Use the following login credentials as needed:
To enter your username, place your cursor in the Sign in box and select the username below.
To enter your password, place your cursor in the Enter password box and select the password below.
Microsoft 365 Username:
admin@WWLx121586.onmicrosoft.com
Microsoft 365 Password: XXXXXXXXX
If the Microsoft Edge browser or Microsoft 365 portal does not load successfully, select the Microsoft Edge browser icon from the task bar, type the URL "https://admin.microsoft.com", and press Enter.
The following information is for technical support purposes only:
Lab Instance: XXXXXXXXX
Task 1
You plan to implement Endpoint data loss prevention (Endpoint DLP). You plan to create a policy that will restrict OneDrive.exe from accessing files that have the Highly Confidential sensitivity label.
You need to configure the Endpoint DLP settings so that onedrive.exe actions can be restricted by a DLP policy.
You do NOT need to create a DLP policy at this time.

正解：

解説：
To restrict onedrive.exe actions in Microsoft Purview, you first configure it as a restricted app group in Endpoint DLP settings and then add that group to a DLP policy in the Microsoft Purview portal. In the Endpoint DLP settings, navigate to Data loss prevention > Settings > Data loss prevention > Endpoint settings > Restricted apps and app groups. Create a new group called "Cloud Sync apps," select the Auto-quarantine option, and add onedrive.exe as the executable name for Windows.
Configure the restricted app group
Step 1: Sign in to the Microsoft Purview portal.
Step 2: Go to Data loss prevention > Settings (gear icon) > Data loss prevention > Endpoint settings.
Step 3: Expand Restricted apps and app groups.
Step 4: Under "Restricted app groups," select Add restricted app group.
Step 5: Enter a group name, such as Cloud Sync apps.
Step 6: Check the box for Auto-quarantine.
Step 7: In the "App name" field, add the executable name:
For Windows, enter onedrive.exe and click the + button.
Reference:
https://learn.microsoft.com/en-us/purview/endpoint-dlp-using

質問 # 127
......

myportal.utt.edu.tt, Disposable vapes

2026年JPNTestの最新SC-401 PDFダンプおよびSC-401試験エンジンの無料共有：https://drive.google.com/open?id=1T7nRjOBNJT9xp_Zutcg99UJ6Cuy7_krT