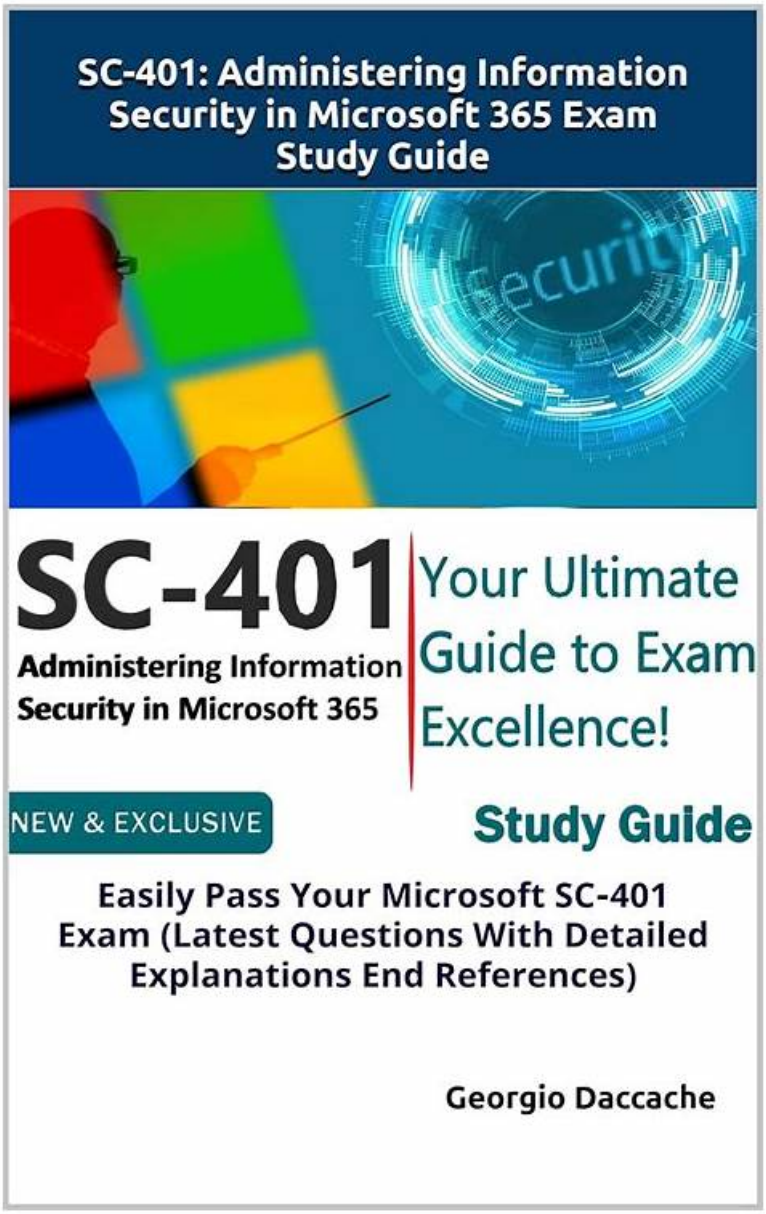
授權的SC-401資料＆資格考試的領導者和高質量的SC-401：Administering Information Security in Microsoft 365



從Google Drive中免費下載最新的NewDumps SC-401 PDF版考試題庫：https://drive.google.com/open?id=1AxcbwQdMhj1CxVttHq7GTWGzfuNjLGHU

要想通過Microsoft SC-401認證考試，選擇相應的訓練工具是非常有必要的。而關於Microsoft SC-401認證考試的研究材料是很重要的一部分，我們的NewDumps能很好很快地提供關於通過Microsoft SC-401認證考試的研究材料。我們的NewDumps的IT專家都很有經驗，他們的研究材料和你考試的考題十分接近的，幾乎一模一樣。NewDumps是一個專門為要參加認證考試的人提供便利的網站，能有效的幫助考生通過考試。

我受不了現在的生活和工作了，想做別的工作。你現在有這樣的想法嗎？但是，怎樣才能做更好的工作呢？你喜歡IT嗎？想通過IT來證明自己的實力嗎？如果你想從事IT方面的工作，那麼參加IT認定考試，取得認證資格是非常有必要的。你現在要做的就是參加被普遍認可的、有價值的IT資格考試。從而打開你職業生涯的新的大門。關於Microsoft的SC-401考試，你一定不陌生吧。取得這個資格可以讓你在找工作的時候得到一份助力。什麼？沒有信心參加這個考試嗎？沒關係，你可以使用NewDumps的SC-401考試資料。

>> SC-401資料 <<

Microsoft SC-401 PDF題庫 & SC-401通過考試

擁有Microsoft SC-401認證可以評估你在公司的價值和能力，但是通過這個考試是比較困難的。而SC-401考題資料能幫考生掌握考試所需要的知識點，擁有良好的口碑，只要你選擇Microsoft SC-401考古題作為你的考前復習資料，你就會相信自己的選擇不會錯。在您購買Microsoft SC-401考古題之前，我們所有的題庫都有提供對應免費試用的demo，您覺得適合在購買，這樣您可以更好的了解我們產品的品質。

Microsoft SC-401 考試大綱：

主題	簡介
主題 1	• 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.
主題 2	• 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.
主題 3	• 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.
主題 4	• 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.

最新的 Microsoft Certified: Information Security Administrator Associate SC-401 免費考試真題 (Q120-Q125):

問題 #120
You have a Microsoft 365 subscription that contains two Microsoft SharePoint Online sites named Site1 and Site2.
You plan to use policies to meet the following requirements:
- Add a watermark of Confidential to a document if the document contains the words Project1 or Project2.
- Retain a document for seven years if the document contains credit card information.
- Add a watermark of Internal Use Only to all the documents stored on Site2.
- Add a watermark of Confidential to all the documents stored on Site1.
You need to recommend the minimum number of sensitive info types required.
How many sensitive info types should you recommend?

- A. 0
- B. 1
- C. 2
- D. 3

答案：C

解題說明：

(1) Add a watermark of Confidential to a document if the document contains the words Pro-ject1 or Project2.
(2 - Retention) Retain a document for seven years if the document contains credit card infor- mation.
(3) Add a watermark of Internal Use Only to all the documents stored on Site2.
(1 the same can be used) Add a watermark of Confidential to all the documents stored on Site1.
Reference:
https://learn.microsoft.com/en-us/purview/sit-sensitive-information-type-learn-about

問題 #121
You have a Microsoft 36S ES subscription that contains the devices shown in the following table.
You plan to implement inside' risk management and capture forensic evidence Which devices support the collection of forensic evidence, and what should you do lo prepare each supported device? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

答案：

解題說明：
Explanation:

問題 #122
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.

答案：

解題說明：
Explanation:
Step 1 - Scenario
A user named User1 was a member of a dynamic security group (Group1).
User1 is no longer a member of that group.
You need to determine why User1 was removed by searching the audit log.
Step 2 - How group membership changes are logged in Microsoft 365 audit logs Microsoft 365 audit logs record group membership activities in Azure AD. The most relevant activities for a user disappearing from a group are:
Removed member from group - Directly indicates that a user was removed from a group.
Updated group - Logged when group properties or membership rules (for dynamic groups) are modified. If Group1 is a dynamic group, changes to membership rules could have caused User1 to no longer qualify, and this would appear as an Updated group event.
Step 3 - Why not other options
Deleted user / Deleted group: Would mean the entire user or group object was deleted, not just removal.
Changed user password, Reset user password, Set license properties, Changed user license: These are account- related, not group membership-related.
Added member to group: The opposite action.
Step 4 - Microsoft Reference
From Microsoft documentation:
Audit logs include events such as when a member is added or removed from a group, and when group properties or membership rules are updated.
Reference: Search the audit log in the Microsoft Purview compliance portal

問題 #123
You have a Microsoft 365 E5 subscription that contains the users shown in the following table.
Which users will Microsoft Purview insider risk management flag as potential high-impact users?

- A. User1, User2, and User3 only
- B. User1, User2, User3, and User4
- C. User2 and User3 only
- D. User1 and User2 only

答案：B

解題說明：
Microsoft Purview Insider Risk Management flags high-impact users based on various risk factors, including role, access to confidential data, and influence within an organization. Let's analyze each user:
User1 (Regional Manager, assigned Reader role, manages department managers) Risk Factors:
*Holds a managerial position (regional manager).
*Manages multiple department managers, indicating organizational influence.
*Access to critical business information.
Flagged? -Yes (Managerial role and access to confidential data).
User2 (HR department manager, no Microsoft Entra roles, manages HR department users) Risk Factors:
*Manages HR department users, meaning they likely handle sensitive employee data.
*HR roles are often considered high-risk due to access to personal and payroll data.
Flagged? -Yes (HR role and access to sensitive employee data).
User3 (Developer, reports to User2, only user in compliance, assigned Compliance Administrator role) Risk Factors:
*Compliance Administrator role grants access to sensitive security and regulatory data.
*Only person in the compliance department, meaning they hold a critical role.
*Potentially high impact on compliance and security settings.
Flagged? -Yes (Privileged Compliance Administrator role).
User4 (Assistant to User1, no Entra roles, handles confidential data on behalf of User1) Risk Factors:
*Handles a high volume of confidential data on behalf of a regional manager.
*Assistants with access to sensitive data are considered insider risk candidates.
Flagged? -Yes (High access to sensitive information).
Since all four users fit high-impact criteria (managerial roles, privileged compliance access, handling sensitive data), Microsoft Purview Insider Risk Management will flag all of them.

問題 #124
You have a Microsoft J65 ES subscription.
You need to create a Microsoft Defender for Cloud Apps policy that will detect data loss prevention (DIP) violations. What should you create?

- A. a session policy
- B. a file policy
- C. an activity policy
- D. an access policy

答案：B

解題說明：
The question asks about creating a Microsoft Defender for Cloud Apps (MCAS / MDA) policy that will detect Data Loss Prevention (DLP) violations.
Understanding the policy types in Defender for Cloud Apps:
File Policy
Used for monitoring and controlling files stored in cloud apps (e.g., SharePoint, OneDrive, Box, Google Drive).
Can detect sensitive information types (like credit cards, SSNs, SWIFT codes) and flag DLP violations.
Can apply governance actions (e.g., quarantine, remove sharing, notify user).
Correct for DLP violation detection.
Activity Policy
Monitors user activities (e.g., login attempts, mass downloads, suspicious behavior).
Not for file content DLP.
Session Policy
Applied through Conditional Access App Control for real-time monitoring/control during a user session.
Used for controlling actions (download, cut/paste) but not for broad DLP scanning of stored files.
Access Policy
Controls access to apps based on conditions (e.g., unmanaged device access).

Not designed for DLP content inspection.
Why File Policy is correct
Since the requirement is:
"detect DLP violations"
That means scanning file content for sensitive information. This is only possible with a File Policy in Microsoft Defender for Cloud Apps.
Reference: File policies in Microsoft Defender for Cloud Apps

問題 #125
......