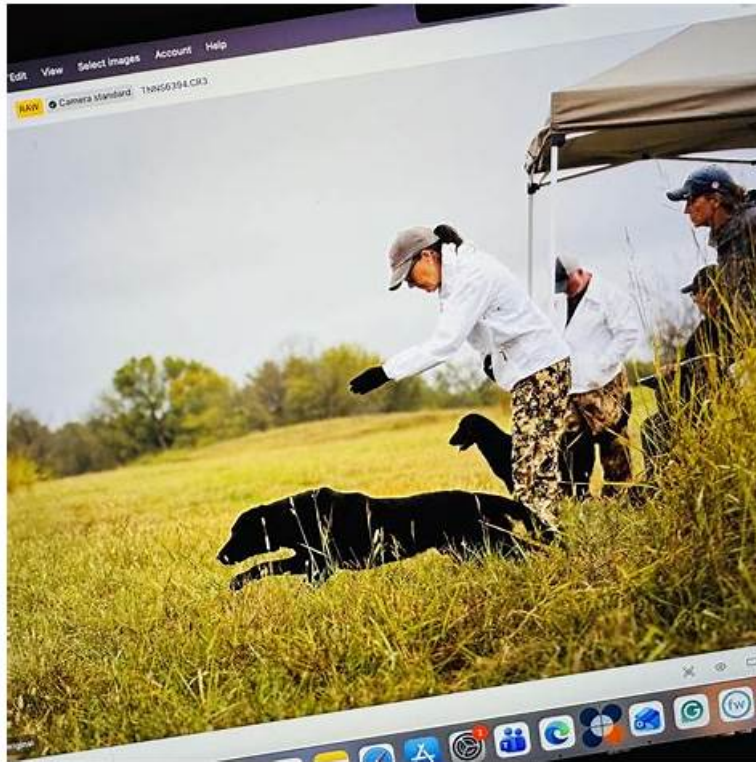


# Study Guide Microsoft SC-100 Pdf | New SC-100 Test Practice



DOWNLOAD the newest Itcertmaster SC-100 PDF dumps from Cloud Storage for free: [https://drive.google.com/open?id=1bCiNs9IGN8\\_dMM4XBWPw5MOnJ1Ky6wK-](https://drive.google.com/open?id=1bCiNs9IGN8_dMM4XBWPw5MOnJ1Ky6wK-)

The pass rate reaches 98.95%, and if you choose us, we can ensure you pass the exam. SC-100 study materials are edited by skilled professionals, and they are quite familiar with the dynamics of the exam center, therefore SC-100 study materials can meet your needs for exam. What's more, we offer you free demo to try before purchasing SC-100 Exam Dumps, so that you can know the mode of the complete version. If you have any questions about SC-100 study materials, you can ask for our service stuff for help.

Microsoft SC-100 (Microsoft Cybersecurity Architect) Certification Exam is a certification exam designed for individuals who are interested in pursuing a career in cybersecurity architecture. SC-100 exam is designed to test the knowledge and skills of individuals who are responsible for designing and implementing cybersecurity solutions for organizations. SC-100 Exam covers a range of topics, including threat management, identity and access management, security operations, and data protection. Individuals who pass SC-100 exam demonstrate their ability to design and implement effective cybersecurity solutions that protect organizations from various cyber threats.

>> Study Guide Microsoft SC-100 Pdf <<

## Microsoft SC-100 Exam Questions Learning Material in Three Different Formats

If you do not know how to pass the exam more effectively, I'll give you a suggestion is to choose a good training site. This can play a multiplier effect. Itcertmaster site has always been committed to provide candidates with a real Microsoft SC-100 Certification Exam training materials. The Itcertmaster Microsoft SC-100 Certification Exam software are authorized products by vendors, it is wide coverage, and can save you a lot of time and effort.

## Microsoft Cybersecurity Architect Sample Questions (Q10-Q15):

NEW QUESTION # 10

Your on-premises network contains an e-commerce web app that was developed in Angular and Node.js. The web app uses a MongoDB database. You plan to migrate the web app to Azure. The solution architecture team proposes the following architecture as an Azure landing zone.



You need to provide recommendations to secure the connection between the web app and the database. The solution must follow the Zero Trust model.

Solution: You recommend implementing Azure Front Door with Azure Web Application Firewall (WAF).

Does this meet the goal?

- A. Yes
- B. No

**Answer: B**

Explanation:

Explanation

<https://www.varonis.com/blog/securing-access-azure-webapps>

### NEW QUESTION # 11

Your company has an Azure App Service plan that is used to deploy containerized web apps. You are designing a secure DevOps strategy for deploying the web apps to the App Service plan. You need to recommend a strategy to integrate code scanning tools into a secure software development lifecycle. The code must be scanned during the following two phases:

Uploading the code to repositories Building containers

Where should you integrate code scanning for each phase? To answer, select the appropriate options in the answer area.

**Answer Area**

Uploading code to repositories:

- ☐ Azure Boards
- ☐ Azure Pipelines
- ☐ GitHub Enterprise
- ☐ Microsoft Defender for Cloud

Building containers:

- ☐ Azure Boards
- ☐ Azure Pipelines
- ☐ GitHub Enterprise
- ☐ Microsoft Defender for Cloud

**Answer:**

Explanation:

**Answer Area**

Uploading code to repositories:

- ☐ Azure Boards
- ☐ Azure Pipelines
- ☒ GitHub Enterprise
- ☐ Microsoft Defender for Cloud

Building containers:

- ☐ Azure Boards
- ☒ Azure Pipelines
- ☐ GitHub Enterprise
- ☐ Microsoft Defender for Cloud

### NEW QUESTION # 12

Your company finalizes the adoption of Azure and is implementing Microsoft Defender for Cloud.

You receive the following recommendations in Defender for Cloud

- \* Access to storage accounts with firewall and virtual network configurations should be restricted,
- \* Storage accounts should restrict network access using virtual network rules.
- \* Storage account should use a private link connection.

\* Storage account public access should be disallowed.

You need to recommend a service to mitigate identified risks that relate to the recommendations. What should you recommend?

- A. Azure Network Watcher
- **B. Azure Policy**
- C. Azure Storage Analytics
- D. Microsoft Sentinel

**Answer: B**

Explanation:

<https://docs.microsoft.com/en-us/azure/defender-for-cloud/security-policy-concept> <https://docs.microsoft.com/en-us/security/benchmark/azure/baselines/storage-security-baseline>

### NEW QUESTION # 13

Hotspot Question

You are designing the security architecture for a cloud-only environment.

You are reviewing the integration point between Microsoft 365 Defender and other Microsoft cloud services based on Microsoft Cybersecurity Reference Architectures (MCRA).

You need to recommend which Microsoft cloud services integrate directly with Microsoft 365 Defender and meet the following requirements:

- Enforce data loss prevention (DLP) policies that can be managed directly from the Microsoft 365 Defender portal.
- Detect and respond to security threats based on User and Entity Behavior Analytics (UEBA) with unified alerting.

What should you include in the recommendation for each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

### Answer Area

DLP:

Azure Data Catalog
Azure Data Explorer
Microsoft Purview

UEBA:

Azure AD Identity Protection
Microsoft Defender for Identity
Microsoft Entra Verified ID

**Answer:**

Explanation:



## Answer Area

DLP:

Azure Data Catalog  
Azure Data Explorer  
Microsoft Purview

UEBA:

Azure AD Identity Protection  
Microsoft Defender for Identity  
Microsoft Entra Verified ID

Explanation:

1. Purview - For the requirement to enforce data loss prevention (DLP) policies that can be managed directly from the Microsoft 365 Defender portal, you should include Microsoft Purview in your recommendation. <https://learn.microsoft.com/en-us/microsoft-365/security/defender/dlp-investigate-alerts-defender?view=o365-worldwide>

2. MS Defender for Identity. Microsoft Defender for Cloud Apps provides user entity behavioral analytics (UEBA) in the cloud. This can be extended to your on-premises environment by integrating with Microsoft Defender for Identity. After you integrate with Defender for Identity, you'll also gain context around user identity from its native integration with Active Directory. <https://learn.microsoft.com/en-us/defender-cloud-apps/tutorial-ueba>

### NEW QUESTION # 14

You need to recommend a solution to meet the compliance requirements.

What should you recommend? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

To enforce compliance to the regulatory standard, create:

- An Azure Automation account
- A blueprint
- A managed identity
- Workflow automation

To exclude TestRG from the compliance assessment:

- Edit an Azure blueprint
- Modify a Defender for Cloud workflow automation
- Modify an Azure policy definition
- Update an Azure policy assignment

Answer:

Explanation:

Answer Area

To enforce compliance to the regulatory standard, create:

- An Azure Automation account
- A blueprint
- A managed identity
- Workflow automation

To exclude TestRG from the compliance assessment:

- Edit an Azure blueprint
- Modify a Defender for Cloud workflow automation
- Modify an Azure policy definition
- Update an Azure policy assignment

Explanation:

Box 1 = A Blueprint

Box 2 = Update an Azure Policy assignment

<https://learn.microsoft.com/en-us/azure/governance/policy/tutorials/create-and-manage#update-assignment-with-exclusion>

<https://docs.microsoft.com/en-us/azure/governance/policy/concepts/definition-structure> while it is in policy assignment

- <https://docs.microsoft.com/en-us/azure/governance/policy/concepts/assignment-structure>

Topic 2, Litware, inc. Case Study 2

Overview

Litware, inc. is a financial services company that has main offices in New York and San Francisco. Litware has 30 branch offices and remote employees across the United States. The remote employees connect to the main offices by using a VPN.

Litware has grown significantly during the last two years due to mergers and acquisitions. The acquisitions include several companies based in France.

Existing Environment

Litware has an Azure Active Directory (Azure AD) tenant that syncs with an Active Directory Domain Services (AD DS) forest named Utvware.com and is linked to 20 Azure subscriptions. Azure AD Connect is used to implement pass-through authentication. Password hash synchronization is disabled, and password writeback is enabled. All Litware users have Microsoft 365 E5 licenses. The environment also includes several AD DS forests, Azure AD tenants, and hundreds of Azure subscriptions that belong to the subsidiaries of Litware.

Planned Changes

Litware plans to implement the following changes:

- \* Create a management group hierarchy for each Azure AD tenant.
- \* Design a landing zone strategy to refactor the existing Azure environment of Litware and deploy all future Azure workloads.
- \* Implement Azure AD Application Proxy to provide secure access to internal applications that are currently accessed by using the VPN.

Business Requirements

Litware identifies the following business requirements:

- \* Minimize any additional on-premises infrastructure.
- \* Minimize the operational costs associated with administrative overhead.

Hybrid Requirements

Litware identifies the following hybrid cloud requirements:

- \* Enable the management of on-premises resources from Azure, including the following:
- \* Use Azure Policy for enforcement and compliance evaluation.
- \* Provide change tracking and asset inventory.
- \* Implement patch management.
- \* Provide centralized, cross-tenant subscription management without the overhead of maintaining guest accounts.

Microsoft Sentinel Requirements

Litware plans to leverage the security information and event management (SIEM) and security orchestration automated response (SOAR) capabilities of Microsoft Sentinel. The company wants to centralize Security Operations Center (SOC) by using Microsoft Sentinel.

Identity Requirements

Litware identifies the following identity requirements:

- \* Detect brute force attacks that directly target AD DS user accounts.
- \* Implement leaked credential detection in the Azure AD tenant of Litware.
- \* Prevent AD DS user accounts from being locked out by brute force attacks that target Azure AD user accounts.
- \* Implement delegated management of users and groups in the Azure AD tenant of Litware, including support for:
- \* The management of group properties, membership, and licensing
- \* The management of user properties, passwords, and licensing
- \* The delegation of user management based on business units.

Regulatory Compliance Requirements

Litware identifies the following regulatory compliance requirements:

- \* Insure data residency compliance when collecting logs, telemetry, and data owned by each United States- and France-based subsidiary.
- \* Leverage built-in Azure Policy definitions to evaluate regulatory compliance across the entire managed environment.
- \* Use the principle of least privilege.

Azure Landing Zone Requirements

Litware identifies the following landing zone requirements:

- \* Route all internet-bound traffic from landing zones through Azure Firewall in a dedicated Azure subscription.
- \* Provide a secure score scoped to the landing zone.
- \* Ensure that the Azure virtual machines in each landing zone communicate with Azure App Service web apps in the same zone over the Microsoft backbone network, rather than over public endpoints.
- \* Minimize the possibility of data exfiltration.
- \* Maximize network bandwidth.

The landing zone architecture will include the dedicated subscription, which will serve as the hub for internet and hybrid connectivity.

- \* Be created in a dedicated subscription.
- \* Use a DNS namespace of `litware.com`.

Litware identifies the following application security requirements:

- \* Identify internal applications that will support single sign-on (SSO) by using Azure AD Application Proxy.
- \* Monitor and control access to Microsoft SharePoint Online and Exchange Online data in real time.

• • • • •

**New SC-100 Test Practice:** <https://www.itcertmaster.com/SC-100.html>

- 2026 Latest Itcertmaster SC-100 PDF Dumps and SC-100 Exam Engine Free Share: [https://drive.google.com/open?id=1bCiNs9lGN8\\_dMM4XBWPw5MOnJlKy6wK-](https://drive.google.com/open?id=1bCiNs9lGN8_dMM4XBWPw5MOnJlKy6wK-)