SC-500的中率、SC-500日本語版と英語版

話と行動の距離はどのぐらいありますか。これは人の心によることです。意志が強い人にとって、行動は目と鼻の先にあるのです。あなたはきっとこのような人でしょう。MicrosoftのSC-500認定試験に申し込んだ以上、試験に合格しなければならないです。これもあなたの意志が強いことを表示する方法です。GoShikenが提供したトレーニング資料はインターネットで最高のものです。MicrosoftのSC-500認定試験に合格したいのなら、GoShikenのMicrosoftのSC-500試験トレーニング資料を利用してください。

Microsoft SC-500 Exam Syllabus Topics:

Section	Weight	Objectives
Topic 1: Secure storage, databases, and networking	25–30%	- Network security • 1. NSGs and ASGs • 2. Network Watcher diagnostics • 3. Azure Virtual Network Manager • 4. VPN security • 5. Azure Firewall • 6. Virtual WAN security • 7. Private endpoints and Private Link - Storage security • 1. Defender for Storage • 2. Storage firewall rules • 3. Access policies for storage • 4. Storage account security configuration - Database security • 1. Database auditing • 2. Defender for Databases • 3. Azure SQL security configuration

Topic 2: Secure compute	20–25%	- Servers and virtual machines • 1. Secure boot and vTPM • 2. Agentless scanning and EDR • 3. Defender for Servers onboarding • 4. Just-in-time (JIT) VM access • 5. Azure Arc hybrid security • 6. Disk encryption • 7. Azure Bastion - Application platform security • 1. Web Application Firewall (WAF) • 2. Azure Functions security • 3. API Management security policies • 4. AKS security and Defender for Containers • 5. Container Registry security • 6. App Service security controls - Security for AI workloads • 1. AI Gateway (Azure API Management) • 2. Microsoft Purview DSPM for AI • 3. Entra Agent ID security and access control • 4. Microsoft Copilot and AI risk identification • 5. Security Copilot agents and monitoring • 6. Defender for AI services
Topic 3: Manage and monitor security posture	20–25%	- Microsoft Sentinel • 1. Workspaces and role assignment • 2. Retention policies • 3. Data connectors (Azure, syslog, CEF) • 4. Data collection rules and WEF • 5. Custom logs and tables • 6. Automation rules and playbooks - Microsoft Defender for Cloud • 1. External Attack Surface Management (EASM) • 2. Defender CSPM risk identification • 3. Defender Vulnerability Management • 4. Compliance frameworks evaluation • 5. Workload protection plans • 6. Multi-cloud (AWS/GCP) integration - Security Copilot • 1. Security Store agents • 2. Workspace configuration • 3. Plugins and integrations • 4. Permissions and roles

Topic 4: Manage identity, access, and governance	20–25%	- Governance and compliance enforcement • 1. Microsoft Defender for Cloud compliance • 2. Resource locks • 3. Infrastructure as Code security controls • 4. Azure Policy (built-in and custom) • 5. Azure Backup security controls • 6. RBAC and role management (Azure & Entra roles) - Secure secrets and keys using Azure Key Vault • 1. Key Vault deployment and configuration • 2. Defender for Key Vault and CSPM scanning • 3. Keys, secrets, and certificates management • 4. Access policies and firewall settings - Secure access to resources by using Microsoft Entra ID • 1. Enterprise applications and app registrations • 2. Privileged Identity Management (PIM) • 3. Conditional Access policies • 4. OAuth consent and permission grants • 5. Managed identities for Azure resources • 6. Authentication methods (MFA, passwordless)

Microsoft Implementing End-to-End Security Controls for Cloud and AI Workloads 認定 SC-500 試験問題 (Q28-Q33):

質問 # 28
You have an Azure Storage account named storage1 that hosts a blob container used by an internal application.
You plan to enable a third-party workflow system to upload blobs to storage1.
You need to provide time-bound, least-privilege upload access to the third-party system.
Which authorization method should you use?

- A. Enable a managed identity for the workflow system and assign a role for storage1.
- B. Configure the workflow system to use Shared Key authorization.
- C. Configure the workflow system to use a user delegation shared access signature (SAS).
- D. Enable anonymous public read access for the blob container.

正解：C

解説：
The best authorization method is to configure the workflow system to use a user delegation shared access signature (SAS).
A user delegation SAS fulfills all three requirements perfectly: it is time-bound (expires automatically), provides least-privilege access (restricted to the specific container/blob and "write" permissions), and is designed for third-party systems that cannot use Entra identities User Delegation SAS.
Reference:
https://learn.microsoft.com/en-us/azure/azure-functions/storage-considerations

質問 # 29
Hotspot Question
You have a Microsoft Entra tenant that contains the users shown in the following table.

Name	Group membership
User1	Group1
User2	Group2
User3	None

You have a location named HQ-Trusted that contains the IP address of the corporate network.
The tenant contains a Conditional Access policy named CA1 that has the following settings:
Assignments:
- Users or agents:
-- Include: All users
-- Exclude: Group1
Target resources:
- Resources (formerly cloud apps):
-- Include: Office 365
Conditions:
- Client apps: Not configured
Access controls:
- Grant:
-- Require multifactor authentication
- Grant:
-- Require device to be marked as compliant
- For multiple controls:
-- Require all the selected controls
The tenant contains a Conditional Access policy named CA2 that has the following settings:
Assignments:
- Users or agents:
-- Include: All users
-- Exclude: Group2
Target resources:
- Resources (formerly cloud apps):
-- Include: All resources
Conditions:
- Locations:
-- Configure: Yes
-- Include: Any network or location
-- Exclude: HQ-Trusted
Access controls:
- Grant:
-- Block access
For each of the following statements, select Yes if the statement is true. Otherwise, select No.
NOTE: Each correct selection is worth one point.

Answer Area

Statements	Yes	No
User2 can sign in to Microsoft 365 services from their home network.	○	○
User3 can sign in to the Azure portal from a public Wi-Fi network by using a compliant device.	○	○
User1 will be prompted for multifactor authentication (MFA) when they sign in to Microsoft 365 services from the HQ-Trusted network.	○	○

正解：

解説：

Explanation:
Box 1: Yes
Yes, User2 can sign in to Microsoft 365 services from their home network.
Policy 1 (CA1): Targets "All users" but excludes Group1. Because User2 is in Group2, this policy applies to them. It requires MFA and a compliant device. However, because they are on their home network, they cannot fulfill both requirements simultaneously, and it would ordinarily block them.
Policy 2 (Block Access): Targets "All users" but excludes Group2. Since User2 is a member of Group2, they are completely excluded from this policy.
The Result: Because User2 is not subject to the blocking policy, and the strict device/MFA policy only applies to Group1, User2's sign-in is allowed.
Box 2: No
No, User3 cannot sign in to the Azure portal.
Policy targeting: The block access policy applies to "All users" and excludes only "Group2". Since User3 is not in any group, they are included in this policy.
Block takes precedence: The policy applies to "All resources" (which includes the Azure portal) and blocks access.
Public Wi-Fi: User3 is attempting to sign in from a public Wi-Fi network, satisfying the policy's condition (they are outside the MyTrusted corporate network).
When both block and grant policies exist, the block access policy always wins.
Box 3: No
No, User3 will be blocked from signing in to the Azure portal.
Although User3 is using a compliant device, they do not meet the location condition of the second Conditional Access (CA) policy, which triggers a Block Access. In Microsoft Entra ID, a single block policy will always override any grant controls, no matter what other policies are in place.
Reference:
https://learn.microsoft.com/en-us/entra/identity/conditional-access/what-if-tool

質問 # 30
You have an Azure subscription that contains the virtual machines shown in the following table.

Name	Location	Virtual network
VM1	East US	VNET1
VM2	West US	VNET2
VM3	East US	VNET1
VM4	West US	VNET3

All the virtual networks are peered.
You deploy Azure Bastion to VNET2.
Which virtual machines can be protected by the bastion host?

- A. VM2 and VM4 only
- B. VM1, VM2, and VM3 only
- C. VM2 only
- D. VM1, VM2, VM3, and VM4

正解：D

解説：
All four virtual machines (VM1, VM2, VM3, and VM4) can be protected by this single Azure Bastion host.
Key Technical Reasons
Virtual Network Peering Support: Azure Bastion natively supports Virtual Network (VNet) Peering.
When VNet peering is configured, an Azure Bastion host deployed in one centralized "hub" VNet can securely connect to virtual machines in any peered "spoke" VNets.
No Regional Restrictions: VNet peering works seamlessly both within the same region and across different Azure regions (known as Global VNet peering). Because Azure Bastion routes your connection over the private Azure backbone network using private IP addresses, the region of the target virtual machine does not restrict access.
Individual Virtual Machine StatusVM1 (East US / VNET1): Accessible because VNET1 is peered with VNET2.
VM2 (West US / VNET2): Accessible because the Azure Bastion host is deployed directly into VNET2.
VM3 (East US / VNET1): Accessible because VNET1 is peered with VNET2.
VM4 (West US / VNET3): Accessible because VNET3 is peered with VNET2.
Reference:
https://learn.microsoft.com/en-us/azure/bastion/vnet-peering

質問 # 31
You have an Azure SQL Database logical server named Server1 that contains a database named DB1.
You need to configure authentication for Server1 to meet the following requirements;
*SQL authentication cannot be used for any databases on Server1.
*The solution must be enforced centrally at the server level.
What should you do?

- A. Enable Microsoft Entra-only authentication for Server1.
- B. Remove SQL logins from DB1.
- C. Enable a managed identity for Server1.
- D. Configure a Microsoft Entra administrator for Server1.

正解：A

解説：
The requirement is centralized enforcement for all databases on the logical server. Microsoft Entra-only authentication disables SQL authentication at the server level, so SQL logins cannot be used against any database hosted there. Configuring an Entra administrator is typically a prerequisite or supporting step, but by itself it does not disable SQL authentication. A managed identity for the server and deleting logins from one database do not meet the central enforcement requirement. For SC-500, the decisive distinction is whether the control authenticates an identity, grants authorization, or merely changes configuration visibility. The incorrect choices generally either grant excessive privilege, change the application model, or operate at the wrong scope. Microsoft expects the least-privilege identity path that satisfies the scenario without introducing shared secrets or unnecessary tenant-wide rights. The result is a direct exam-style implementation choice: it changes the required security behavior without relying on unrelated monitoring, manual cleanup, or excessive privilege. Official Microsoft source/topic: SC-500 Study Guide > Azure SQL authentication; Microsoft Learn
> Microsoft Entra-only authentication for Azure SQL.

質問 # 32
Your organization plans to allow developers to access Azure OpenAI resources. Management wants to ensure that access permissions follow the principle of least privilege. What should you use?

- A. Management groups only
- B. Role-Based Access Control (RBAC) roles
- C. Resource locks
- D. Azure Policy exemptions

正解：B

解説：
Azure RBAC enables administrators to assign only the permissions required for specific tasks.
Developers can receive limited access to Azure OpenAI resources without granting excessive privileges. Resource locks prevent

accidental deletion, while management groups and policy exemptions do not directly enforce least-privilege authorization.

質問 # 33
.....

GoShikenは、魅力的なキャラクターで世界中の試験受験者を招きます。当社の専門家は彼らの卓越性に大きく貢献しました。したがって、試験をシミュレートするSC-500が最良であると率直に言うことができます。 SC-500学習教材のコンテンツを作成する取り組みは、学習ガイドの開発につながり、完成度を高めます。関心を集め、いくつかの難しい点を簡素化するために、当社の専門家は当社のSC-500学習資料を設計し、SC-500学習ガイドをよりよく理解できるように最善を尽くします。

SC-500日本語版と英語版: https://www.goshiken.com/Microsoft/SC-500-mondaishu.html

- Microsoft SC-500的中率: Implementing End-to-End Security Controls for Cloud and AI Workloads - www.goshiken.com パスリーディングプロバイダー □ 【 www.goshiken.com 】で【 SC-500 】を検索し、無料でダウンロードしてくださいSC-500全真問題集
- SC-500試験の準備方法 | 更新するSC-500的中率試験 | 真実的なImplementing End-to-End Security Controls for Cloud and AI Workloads日本語版と英語版 □ ✔ www.goshiken.com □✔□サイトにて最新➤ SC-500 □問題集をダウンロードSC-500的中合格問題集
- SC-500日本語資格取得 □ SC-500日本語版参考資料 □ SC-500模擬試験最新版 □ ウェブサイト⇒ www.it-passports.com⇐から□ SC-500 □を開いて検索し、無料でダウンロードしてくださいSC-500試験
- SC-500資格トレーリング □ SC-500ファンデーション □ SC-500的中合格問題集 □ 今すぐ➡ www.goshiken.com □□□を開き、➠ SC-500 □を検索して無料でダウンロードしてくださいSC-500日本語資格取得
- SC-500試験解説問題 □ SC-500専門知識 □ SC-500試験解説問題 □ ウェブサイト▹ jp.fast2test.com ◃を開き、□ SC-500 □を検索して無料でダウンロードしてくださいSC-500試験感想
- 更新するSC-500的中率 - 合格スムーズSC-500日本語版と英語版 | ハイパスレートのSC-500リンクグローバル □ [www.goshiken.com]で➠ SC-500 □を検索して、無料でダウンロードしてくださいSC-500試験解説問題
- 更新するSC-500的中率 - 合格スムーズSC-500日本語版と英語版 | ハイパスレートのSC-500リンクグローバル □ Open Webサイト□ www.xhs1991.com □検索➡ SC-500 □□□無料ダウンロードSC-500資格専門知識
- SC-500試験感想 □ SC-500全真問題集 □ SC-500試験解説問題 □ □ www.goshiken.com □サイトで➤ SC-500 □の最新問題が使えるSC-500トレーニング
- 有難いSC-500的中率 - 合格スムーズSC-500日本語版と英語版 | 権威のあるSC-500リンクグローバル Implementing End-to-End Security Controls for Cloud and AI Workloads □ （ www.xhs1991.com ）を開いて⇒ SC-500 ⇐を検索し、試験資料を無料でダウンロードしてくださいSC-500専門知識
- 最高SC-500 | ユニークなSC-500的中率試験 | 試験の準備方法Implementing End-to-End Security Controls for Cloud and AI Workloads日本語版と英語版 □ 【 www.goshiken.com 】から簡単に“ SC-500 ”を無料でダウンロードできますSC-500テスト問題集
- SC-500資格専門知識 □ SC-500トレーニング □ SC-500専門知識 □ サイト☀ www.passtest.jp □☀□で⇒ SC-500 ⇐問題集をダウンロードSC-500試験
- myportal.utt.edu.tt, divisionmidway.org, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, www.stes.tyc.edu.tw, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, myportal.utt.edu.tt, Disposable vapes