



Microsoft SC-500

Implementing End-to-End Security Controls for Cloud and AI Workloads

Thank You for Downloading SC-500 Updated Exam Questions

<https://certs4sale.com/microsoft/sc-500-pdf-exam-dumps>

Implementing End-to-End Security Controls for Cloud and AI Workloads

This reference assessment guide covers cloud security controls, identity governance, secrets management, container security, network microsegmentation, and workload threat protection across Microsoft Azure and hybrid environments.

VENDOR

Microsoft

EXAM CODE

SC-500

CERTIFICATION SPECIALTY

Cloud and AI Security
Engineer Associate

Core Competencies Evaluated

- Privileged Identity Management (PIM) and Identity Governance
- Key Vault, Secrets Management, and Network Firewall Isolation
- Multi-tier Subnet Security and Application Security Groups (ASGs)
- Defender for Servers and Azure Arc Hybrid Workload Security
- Azure Kubernetes Service (AKS) Pod Security Standards and Runtime Defense

Microsoft SC-500

PRACTICE ASSESSMENT

Question 1

SINGLE CHOICE

Your organization is implementing Privileged Identity Management (PIM) for Microsoft Entra ID to manage access to critical Azure resources. You need to configure PIM so that when users request access to resources with the Owner role, they must provide business justification and approval from a designated reviewer before activation. You also want to enforce multifactor authentication (MFA) at the time of activation and set an expiration time of 8 hours for the activated role. Which PIM configuration settings should you apply to meet these requirements?

A. Configure role activation requirements to require MFA, set justification as required, assign a designated approver, and set the activation maximum duration to 8 hours

B. Enable PIM alerts for the Owner role and set a blanket 8-hour expiration for all role assignments without requiring approval or MFA

C. Create an Azure Policy to enforce Owner role assignments with 8-hour expiry and require MFA at the Microsoft Entra sign-in level only

D. Configure conditional access policies to require approval for Owner role activation and set role assignment duration to 8 hours through RBAC

Answer: A

Explanation:

The correct answer is to configure role activation requirements within PIM itself to require MFA, justification, approvers, and maximum duration. PIM's activation policy settings allow you to enforce these requirements specifically for role activation, ensuring privileged access follows the principle of least privilege and includes audit trails.

Why other options are incorrect:

- Option B: PIM alerts alone do not enforce requirements before activation; they only notify after the fact. Expiration without approval defeats the justification requirement.
- Option C: Azure Policy cannot enforce PIM activation workflows. MFA at sign-in level does not enforce activation-time MFA for privileged roles.
- Option D: Conditional Access policies apply to authentication and resource access, not to the internal PIM activation workflow itself.

Microsoft SC-500

PRACTICE ASSESSMENT

Question 2

SINGLE CHOICE

Your organization stores encryption keys and database connection strings in Azure Key Vault. You have configured network connectivity to Key Vault through a private endpoint. A compliance audit requires that you prevent any access to Key Vault from the public internet, block Azure services from bypassing the firewall, and ensure that only your trusted on-premises network and specific Azure services can access the vault. What should you configure on the Key Vault firewall to meet these requirements?

A. Set the firewall default action to Deny, disable the 'Allow Trusted Microsoft Services' option, add your on-premises IP address range to the firewall allowlist, and configure virtual network service endpoints for your Azure services

B. Set the firewall default action to Allow, then add deny rules for public IP addresses and enable the 'Allow Trusted Microsoft Services' option

C. Disable the Key Vault firewall entirely and rely on the private endpoint to prevent internet access

D. Set the firewall default action to Deny and allow all Azure services through the 'Allow Azure Services' bypass option

Answer: A

Explanation:

The correct approach is to set the firewall default action to Deny, disable the 'Allow Trusted Microsoft Services' option for explicit control, add your on-premises IP address range to the allowlist, and configure service endpoints or managed identities for the specific Azure services that need access.

Why other options are incorrect:

- Option B: Setting default action to Allow is the opposite of a deny-by-default security posture.
- Option C: A private endpoint alone does not enforce explicit identity and network access firewall constraints.
- Option D: Allowing all Azure services globally violates the requirement to limit access only to specific trusted services.

Microsoft SC-500

PRACTICE ASSESSMENT

Question 3

SINGLE CHOICE

Your organization is configuring network security for a multi-tier application deployed in Azure. The application consists of a public-facing web tier, a middle-tier API server, and a backend database tier. Each tier is deployed in its own subnet. You need to ensure that only the web tier can accept inbound internet traffic on port 443, the API tier can only receive traffic from the web tier, and the database tier can only receive traffic from the API tier. Which combination of security mechanisms should you implement?

A. Create network security groups for each subnet with inbound rules configured to allow only the required source tiers, and implement application security groups to logically group VMs by tier for simplified rule management

B. Configure only NSGs on the database tier to deny all internet traffic; allow Azure Firewall to manage all inbound rules for the web tier

C. Deploy Azure Firewall to block all internet traffic except port 443, then configure NSGs only on the web tier

D. Use conditional access policies to restrict network traffic between tiers based on user identity

Answer: A

Explanation:

The correct answer is to create network security groups (NSGs) for each subnet with granular inbound rules that enforce tier-to-tier communication requirements, combined with application security groups (ASGs) to simplify management of rules across multiple VMs within the same logical tier.

Why other options are incorrect:

- Option B: NSGs on the database tier alone do not protect the API tier. Azure Firewall is for perimeter defense, not subnet-to-subnet NSG substitution.
- Option C: Azure Firewall cannot efficiently replace layer-4 subnet NSG segmentation rules inside the VNet.
- Option D: Conditional Access controls user identity sign-in, not infrastructure layer-4 network traffic.

Microsoft SC-500

PRACTICE ASSESSMENT

Question 4

SINGLE CHOICE

Your organization is implementing Defender for Servers on a hybrid infrastructure that includes Azure VMs, on-premises servers running Windows and Linux, and servers hosted in AWS. You need to enable vulnerability scanning, endpoint detection and response (EDR), and ensure all servers are visible in a single security posture view within Defender for Cloud. Some on-premises servers have network connectivity constraints. Which approach should you use to onboard all server types and enable the required protections?

A. Use Azure Arc to onboard hybrid and multicloud servers with the Defender for Servers agent, enable EDR and vulnerability assessment plugins on the Arc-connected machines, and select the Defender for Servers P2 plan in Defender for Cloud

B. Install the Log Analytics agent directly on all servers, enable Defender for Servers on Azure VMs only, and use AWS Systems Manager to manage on-premises and AWS servers separately

C. Deploy Azure Monitor agent only on Azure VMs; use AWS native security services for AWS servers and rely on Windows Defender EDR for on-premises servers

D. Implement a custom script deployment using Azure Automation to push agents to all servers without using Azure Arc

Answer: A

Explanation:

The correct approach is to use Azure Arc to onboard hybrid and multicloud servers, then enable the Defender for Servers agent extension. Selecting the Defender for Servers P2 plan in Defender for Cloud provides EDR and vulnerability scanning capabilities with a single unified view.

Why other options are incorrect:

- Option B: Log Analytics agent alone does not provide EDR. Managing systems separately violates the single view requirement.
- Option C: Prevents unified visibility inside Defender for Cloud.
- Option D: Custom scripts without Azure Arc bypass the supported hybrid onboarding architecture.

Microsoft SC-500

PRACTICE ASSESSMENT

Question 5

SINGLE CHOICE

Your organization is implementing security controls for an Azure Kubernetes Service (AKS) cluster that will host microservices processing sensitive customer data. You need to enforce that containers can only run as non-root users, prevent privilege escalation, restrict access to the host filesystem, enforce Pod Security Standards, and ensure that image pulls occur only from your approved container registry. Additionally, you must enable Defender for Containers to monitor runtime security threats. Which combination of controls should you implement?

A. Configure Azure Policy to enforce Pod Security Standards with the restricted policy level, configure AKS network policies to limit pod-to-pod communication, enable Azure Container Registry (ACR) authentication and image pull policies, and enable Defender for Containers in Defender for Cloud

B. Set pod security policies on the AKS cluster to run containers as non-root and enable Azure Firewall to restrict container image access

C. Enforce NSG rules at the pod level and configure the kubelet to block privilege escalation cluster-wide

D. Use role-based access control (RBAC) on the AKS cluster to prevent container execution and enable Azure Defender for Container Registry

Answer: A

Explanation:

The correct answer combines Azure Policy Pod Security Standards (enforcing non-root and host isolation), network policies, ACR image pull controls, and Defender for Containers for runtime threat detection.

Why other options are incorrect:

- Option B: Pod security policies are deprecated in favor of Pod Security Standards via Azure Policy.
- Option C: NSG rules cannot be directly applied to individual pods inside a Kubernetes network overlay.
- Option D: RBAC controls API access, not pod runtime security constraints.

THANK YOU FOR DOWNLOADING SC-500 UPDATED EXAM QUESTIONS

Note: Thanks For Trying The Demo Of Our SC-500 Exam Product

Visit Our Site to Purchase the Full Set of Actual SC-500 Exam Questions With Answers.

Money Back Guarantee



Click The Link Below

<https://certs4sale.com/microsoft/sc-500-pdf-exam-dumps>