



Vendor: Microsoft

Exam Code: SC-500

Exam Name: Implementing End-to-End Security Controls for
Cloud and AI Workloads

Version: DEMO

QUESTION 1

You have an Azure subscription named Sub1 that contains a storage account named storage1. Sub1 has Microsoft Defender for Storage enabled. Defender for Storage has malware scanning enabled.

You need to configure a solution that automates the remediation of malware detected in storage1.

What should you include in the solution?

- A. Application Insights
- B. Azure Event Hubs
- C. Azure Event Grid
- D. Azure Policy

Answer: C

Explanation:

Azure Event Grid publishes Defender for Storage malware scan results as events, enabling event-driven automated remediation workflows such as quarantining, deleting, or moving malicious files after detection.

Reference:

<https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-storage-configure-malware-scan>

<https://learn.microsoft.com/en-us/azure/defender-for-cloud/understand-malware-scan-results>

QUESTION 2

Drag and Drop Question

You have an Azure virtual network named VNet1 that contains three subnets named Subnet1, Subnet2, and Subnet3. A single network security group (NSG) named NSG1 is associated with all the subnets. You have the following virtual machines:

- VM1 on Subnet1
- VM2 on Subnet2
- VM3 on Subnet3

You create two application security groups named ASG1 and ASG2. VM2 is a member of ASG1, and VM3 is a member of ASG2.

You need to ensure that only VM2 can connect to VM3. The solution must continue to work if the private IP address of VM2 changes.

How should you configure the inbound rule on NSG1? To answer, drag the settings to the correct configurations. Each setting may be used once, more than once, or not at all. You may need to drag the split bar between panes or scroll to view content.

NOTE: Each correct selection is worth one point.

Settings

ASG1
ASG2
IP address of VM1
IP address of VM2
IP address of VM3
VirtualNetwork

Answer Area

Source:	
Destination:	

Answer:

Settings

ASG1
ASG2
IP address of VM1
IP address of VM2
IP address of VM3
VirtualNetwork

Answer Area

Source:	ASG1
Destination:	ASG2

QUESTION 3

You have an Azure virtual network that contains 100 virtual machines and an Azure Firewall instance named FW1.

All the traffic from the virtual machines is routed through FW1.

You need to ensure that FW1 allows access to only a URL of updates.contoso.com and blocks all other outbound traffic.

What should you use?

- A. an inbound NAT rule
- B. an application rule

- C. an outbound NAT rule
- D. a network rule

Answer: B

Explanation:

An Azure Firewall application rule permits outbound HTTP or HTTPS access based on a fully qualified domain name, such as updates.contoso.com. With only that destination allowed, traffic to other outbound web destinations is denied when no matching allow rule exists.

Reference:

<https://learn.microsoft.com/en-us/azure/firewall/firewall-faq>

QUESTION 4

You use Azure Virtual Network Manager to manage multiple virtual networks in a network group named Group1.

You discover that the virtual machines in Group1 are accessible from the internet by using TCP port 3389.

You need to block inbound TCP 3389 from the internet across all the virtual networks in Group1. The solution must minimize administrative effort.

What should you use?

- A. a connectivity configuration
- B. a security admin configuration
- C. a user-defined route (UDR)
- D. a network security group (NSG)

Answer: B

Explanation:

A security admin configuration in Azure Virtual Network Manager applies centralized security admin rules to all virtual networks in a targeted network group. A deny inbound rule for TCP port 3389 from the internet blocks RDP exposure across Group1 with minimal administrative effort and is evaluated before NSG rules.

Reference:

<https://learn.microsoft.com/en-us/azure/virtual-network-manager/concept-security-admins>

QUESTION 5

You have an Azure subscription.

You need to deploy an Azure virtual WAN to meet the following requirements:

- Create three secured virtual hubs located in the East US, West US, and North Europe Azure regions.
- Ensure that security rules sync between the regions.

What should you use?

- A. Azure Network Function Manager
- B. Azure Firewall Manager

- C. Azure Virtual Network Manager
- D. Azure Front Door

Answer: B

Explanation:

Azure Firewall Manager is used to create and manage secured virtual hubs for Azure Virtual WAN. It supports centrally managed Azure Firewall policies across multiple secured virtual hubs in different Azure regions, allowing the same security rules to be consistently applied to the hubs in East US, West US, and North Europe.

Reference:

<https://learn.microsoft.com/en-us/azure/firewall-manager/overview>

<https://learn.microsoft.com/en-us/azure/firewall-manager/secured-virtual-hub>

<https://learn.microsoft.com/en-us/azure/firewall-manager/policy-overview>

QUESTION 6

Hotspot Question

You have an Azure Container Instances container group named CGI that has a DNS name of cg1.contoso.com. CG1 has the following configurations:

- A Linux container named container1 that serves HTTPS over TCP port 443 and hosts an application named App1
- A Linux container named contained that listens on TCP port 5000 and is accessed only by App1
- A public IP address

A security review finds that external clients can reach TCP port 5000 by using the public IP address of CG1.

You need to meet the following requirements:

- Ensure that the external clients can access container1 only by using TCP port 443.
- Ensure that container1 can continue to access contained.

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

NOTE: Each correct selection is worth one point.

Answer Area

Exposed ports on the public IP address of CG1:

▼
443 and 5000
443 only
5000 only

Network endpoint for App1:

▼
cg1.contoso.com:443
cg1.contoso.com:5000
localhost:443
localhost:5000

Answer:

Answer Area

Exposed ports on the public IP address of CG1:

▼
443 and 5000
443 only
5000 only

Network endpoint for App1:

▼
cg1.contoso.com:443
cg1.contoso.com:5000
localhost:443
localhost:5000

QUESTION 7

Hotspot Question

You have an Azure subscription that contains the following servers:

- 200 virtual machines that run either Windows Server or Ubuntu Server
- 50 Azure Arc-enabled servers

You use Azure Policy to manage compliance across all the servers.

You need to enforce an organization-specific security baseline. The solution must meet the following requirements:

- Customize a built-in security baseline.
- Ensure that configuration changes to the servers are enforced automatically after the security baseline is deployed.

- Minimize administrative effort.

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

NOTE: Each correct selection is worth one point.

Answer Area

To customize the baseline:

Use Azure Machine Configuration.
Use Desired State Configuration (DSC).
Edit the built-in initiative in JSON directly.

Set enforcement mode to:

Apply and Autocorrect
Apply and Monitor
Audit
DeployIfNotExists

Answer:

Answer Area

To customize the baseline:

Use Azure Machine Configuration.
Use Desired State Configuration (DSC).
Edit the built-in initiative in JSON directly.

Set enforcement mode to:

Apply and Autocorrect
Apply and Monitor
Audit
DeployIfNotExists

QUESTION 8

You have an Azure subscription named Sub1 that contains a storage account named storage1.

Sub1 has Microsoft Defender for Storage enabled. Defender for Storage has on-upload malware

scanning enabled for a monthly cap of 10,000 GB per storage account.

You use a Microsoft Sentinel workspace to monitor security events on all Azure resources.

You need to configure storage1 to use a malware scanning cap of 2,000 GB per month.

What should you do?

- A. Enable the Override Defender for Storage subscription-level settings for storage1.
- B. From Microsoft Sentinel, modify the data collection rule (DCR) to restrict log ingestion from storage1.
- C. Modify the malware scanning configuration of Sub1.
- D. From the Microsoft Sentinel workspace, modify the daily cap.

Answer: A

Explanation:

Defender for Storage settings can be overridden for an individual storage account when the subscription-level configuration applies a different malware scanning cap. Enabling the override for storage1 allows its on-upload malware scanning monthly cap to be changed to 2,000 GB while the subscription-level 10,000-GB setting continues to apply to other storage accounts.

Reference:

<https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-storage-introduction>

<https://learn.microsoft.com/en-us/azure/defender-for-cloud/defender-for-storage-azure-portal-enablement?tabs=enable-subscription>

QUESTION 9

You have an Azure subscription named Sub1 that contains multiple virtual machines. Sub1 has the Microsoft Defender Cloud Security Posture Management (CSPM) plan enabled.

You discover that Defender for Cloud fails to identify plaintext connection strings and SSH keys stored on the virtual machines.

You need to ensure that secrets can be identified on the virtual machines.

What should you do?

- A. Configure the Defender for Cloud data connector in Microsoft Sentinel.
- B. Enable agentless machine scanning.
- C. Deploy the Azure Monitor Agent to all the virtual machines.
- D. Enable Microsoft Defender for Key Vault.

Answer: B

Explanation:

Agentless machine scanning enables Defender CSPM to scan virtual machine disks for exposed plaintext secrets, including connection strings and SSH private keys. It uses disk snapshots and cloud APIs without requiring an agent installation or affecting virtual machine performance.

Reference:

<https://learn.microsoft.com/en-us/azure/defender-for-cloud/secrets-scanning-servers>

<https://learn.microsoft.com/en-us/azure/defender-for-cloud/secrets-scanning>

Thank You for Trying Our Product

Lead2pass Certification Exam Features:

- ★ More than **99,900** Satisfied Customers Worldwide.
- ★ Average **99.9%** Success Rate.
- ★ **Free Update** to match latest and real exam scenarios.
- ★ **Instant Download** Access! No Setup required.
- ★ Questions & Answers are downloadable in **PDF** format and **VCE** test engine format.
- ★ Multi-Platform capabilities - **Windows, Laptop, Mac, Android, iPhone, iPod, iPad**.
- ★ **100%** Guaranteed Success or **100%** Money Back Guarantee.
- ★ **Fast**, helpful support **24x7**.



View list of all certification exams: <http://www.lead2pass.com/all-products.html>



10% Discount Coupon Code: ASTR14