Free Questions for SC-100 by braindumpscollection

Shared by Mullins on 09-08-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

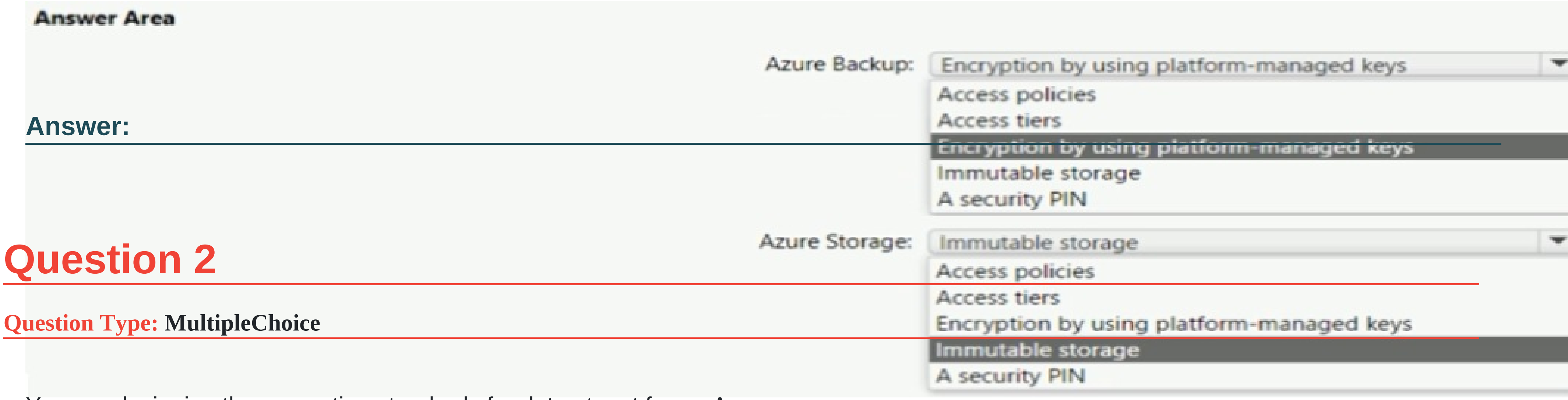
Question Type: Hotspot

Your company wants to optimize using Azure to protect its resources from ransomware.

You need to recommend which capabilities of Azure Backup and Azure Storage provide the strongest protection against ransomware attacks. The solution must follow Microsoft Security Best Practices.

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

NOTE: Each correct selection is worth one point.



Answer Area

Azure Backup: Encryption by using platform-managed keys

- Access policies
- Access tiers
- Encryption by using platform-managed keys
- Immutable storage
- A security PIN

Azure Storage: Immutable storage

- Access policies
- Access tiers
- Encryption by using platform-managed keys
- Immutable storage
- A security PIN

Answer:

Question 2

Question Type: MultipleChoice

You are designing the encryption standards for data at rest for an Azure resource

You need to provide recommendations to ensure that the data at rest is encrypted by using AES-256 keys. The solution must support rotating the encryption keys monthly.

Solution: For Azure SQL databases, you recommend Transparent Data Encryption (TDE) that uses customer-managed keys (CMKs).

Does this meet the goal?

Options:

A- Yes

B- No

Answer:

A

Question 3

Question Type: **MultipleChoice**

You have a Microsoft 365 subscription and an Azure subscription. Microsoft 365 Defender and Microsoft Defender for Cloud are enabled.

The Azure subscription contains 50 virtual machines. Each virtual machine runs different applications on Windows Server 2019.

You need to recommend a solution to ensure that only authorized applications can run on the virtual machines. If an unauthorized application attempts to run or be installed, the application must be blocked automatically until an administrator authorizes the application.

Which security control should you recommend?

Options:

A- app discovery anomaly detection policies in Microsoft Defender for Cloud Apps

B- adaptive application controls in Defender for Cloud

C- Azure Security Benchmark compliance controls m Defender for Cloud

D- app protection policies in Microsoft Endpoint Manager

Answer:

B

Explanation:

https://docs.microsoft.com/en-us/azure/defender-for-cloud/recommendations-reference#compute-recommendations

Question 4

Question Type: **MultipleChoice**

A customer has a Microsoft 365 E5 subscription and an Azure subscription.

The customer wants to centrally manage security incidents, analyze log, audit activity, and search for potential threats across all deployed services.

You need to recommend a solution for the customer. The solution must minimize costs.

What should you include in the recommendation?

Options:

A- Microsoft 365 Defender

B- Microsoft Defender for Cloud

C- Microsoft Defender for Cloud Apps

D- Microsoft Sentinel

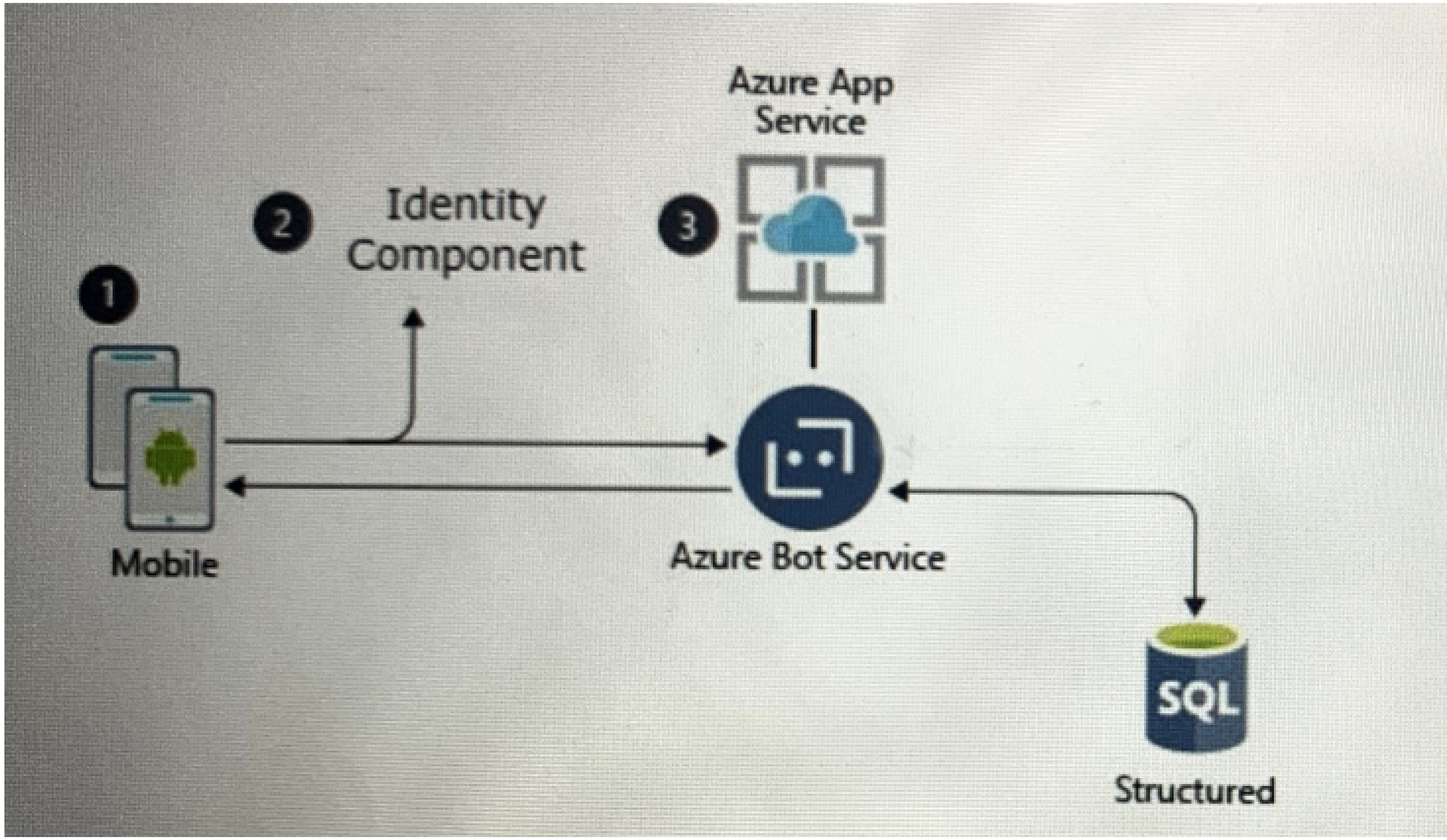
Answer:

D

Question 5

Question Type: MultipleChoice

A customer uses Azure to develop a mobile app that will be consumed by external users as shown in the following exhibit.



You need to design an identity strategy for the app. The solution must meet the following requirements:

* Enable the usage of external IDs such as Google, Facebook, and Microsoft accounts.

* Be managed separately from the identity store of the customer.

* Support fully customizable branding for each app.

Which service should you recommend to complete the design?

Options:

A- Azure Active Directory (Azure AD) B2C

B- Azure Active Directory (Azure AD) B2B

C- Azure AD Connect

D- Azure Active Directory Domain Services (Azure AD DS)

Answer:

A

Explanation:

https://docs.microsoft.com/en-us/azure/active-directory-b2c/identity-provider-facebook?pivots=b2c-user-flow

https://docs.microsoft.com/en-us/azure/active-directory-b2c/customize-ui-with-html?pivots=b2c-user-flow

Question 6

Question Type: **MultipleChoice**

You have a customer that has a Microsoft 365 subscription and uses the Free edition of Azure Active Directory (Azure AD)

The customer plans to obtain an Azure subscription and provision several Azure resources.

You need to evaluate the customer's security environment.

What will necessitate an upgrade from the Azure AD Free edition to the Premium edition?

Options:

A- role-based authorization

B- Azure AD Privileged Identity Management (PIM)

C- resource-based authorization

D- Azure AD Multi-Factor Authentication

Answer:

D

Explanation:

(https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure)

https://www.microsoft.com/en-us/security/business/identity-access/azure-active-directory-pricing?rtc=1

Question 7

Question Type: MultipleChoice

You are designing the security standards for a new Azure environment.

You need to design a privileged identity strategy based on the Zero Trust model.

Which framework should you follow to create the design?

Options:

A- Enhanced Security Admin Environment (ESAE)

B- Microsoft Security Development Lifecycle (SDL)

C- Rapid Modernization Plan (RaMP)

D- Microsoft Operational Security Assurance (OSA)

Answer:

C

Explanation:

https://docs.microsoft.com/en-us/security/compass/security-rapid-modernization-plan This rapid modernization plan (RAMP) will help you quickly adopt Microsoft's recommended privileged access strategy.

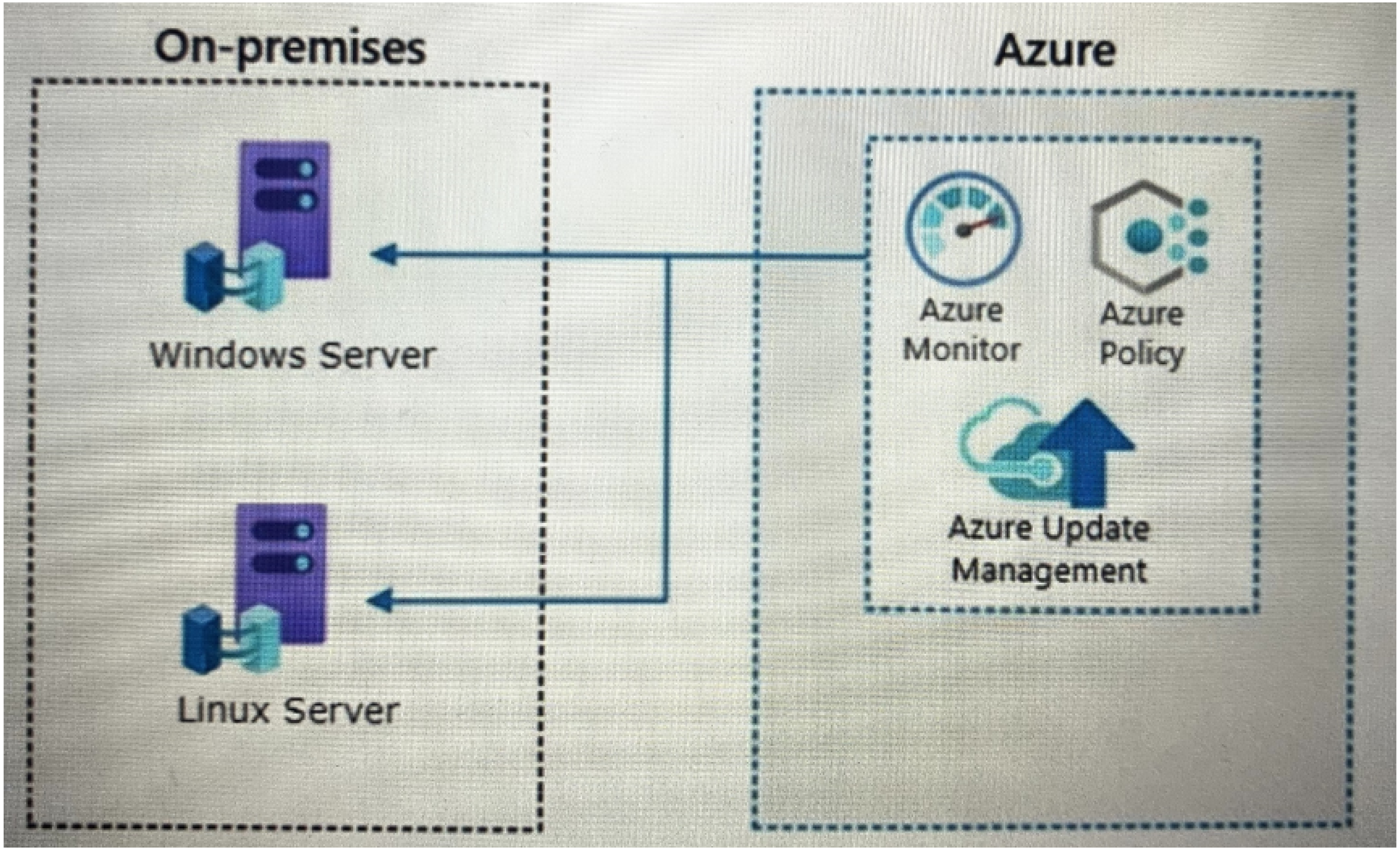
Question 8

Question Type: **MultipleChoice**

Your company has a hybrid cloud infrastructure.

Data and applications are moved regularly between cloud environments.

The company's on-premises network is managed as shown in the following exhibit.



You are designing security operations to support the hybrid cloud infrastructure. The solution must meet the following requirements:

Govern virtual machines and servers across multiple environments.

Enforce standards for all the resources across all the environment across the Azure policy.

Which two components should you recommend for the on-premises network? Each correct answer presents part of the solution.

NOTE Each correct selection is worth one point.

Options:

A- Azure VPN Gateway

B- guest configuration in Azure Policy

C- on-premises data gateway

D- Azure Bastion

E- Azure Arc

Answer:

B, E

Explanation:

https://docs.microsoft.com/en-us/azure/governance/machine-configuration/overview

Question 9

Question Type: **MultipleChoice**

You have a customer that has a Microsoft 365 subscription and an Azure subscription.

The customer has devices that run either Windows, iOS, Android, or macOS. The Windows devices are deployed on-premises and in Azure.

You need to design a security solution to assess whether all the devices meet the customer's compliance rules.

What should you include in the solution?

Options:

A- Microsoft Information Protection

B- Microsoft Defender for Endpoint

C- Microsoft Sentinel

D- Microsoft Endpoint Manager

Answer:

D

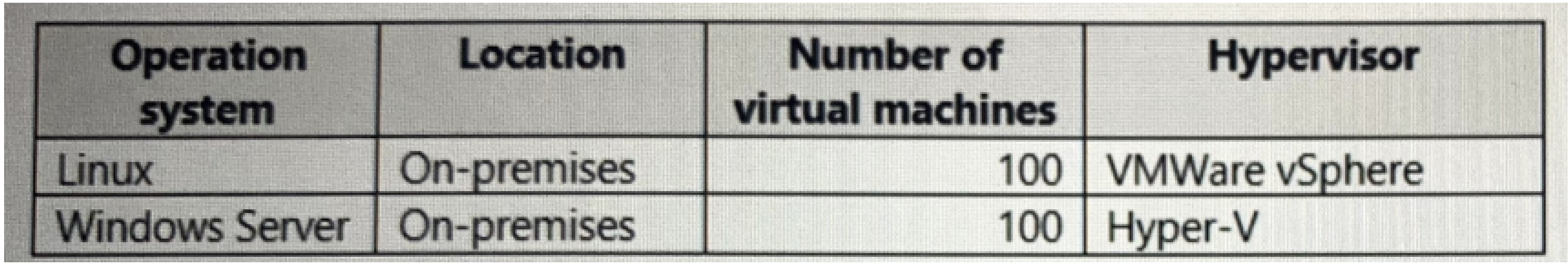
Explanation:

https://docs.microsoft.com/en-us/mem/intune/protect/compliance-policy-monitor#open-the-compliance-dashboard

Question 10

Question Type: **MultipleChoice**

Your company has the virtual machine infrastructure shown in the following table.



Operation system	Location	Number of virtual machines	Hypervisor
Linux	On-premises	100	VMWare vSphere
Windows Server	On-premises	100	Hyper-V

The company plans to use Microsoft Azure Backup Server (MABS) to back up the virtual machines to Azure.

You need to provide recommendations to increase the resiliency of the backup strategy to mitigate attacks such as ransomware.

What should you include in the recommendation?

Options:

A- Use geo-redundant storage (GRS).

B- Use customer-managed keys (CMKs) for encryption.

C- Require PINs to disable backups.

D- Implement Azure Site Recovery replication.

Answer:

C

Explanation:

https://docs.microsoft.com/en-us/azure/security/fundamentals/backup-plan-to-protect-against-ransomware#azure-backup

Question 11

Question Type: Hotspot

You have a Microsoft 365 subscription and an Azure subscription. Microsoft 365 Defender and Microsoft Defender for Cloud are enabled.

The Azure subscription contains a Microsoft Sentinel workspace. Microsoft Sentinel data connectors are configured for Microsoft 365, Microsoft 365 Defender, Defender for Cloud, and Azure.

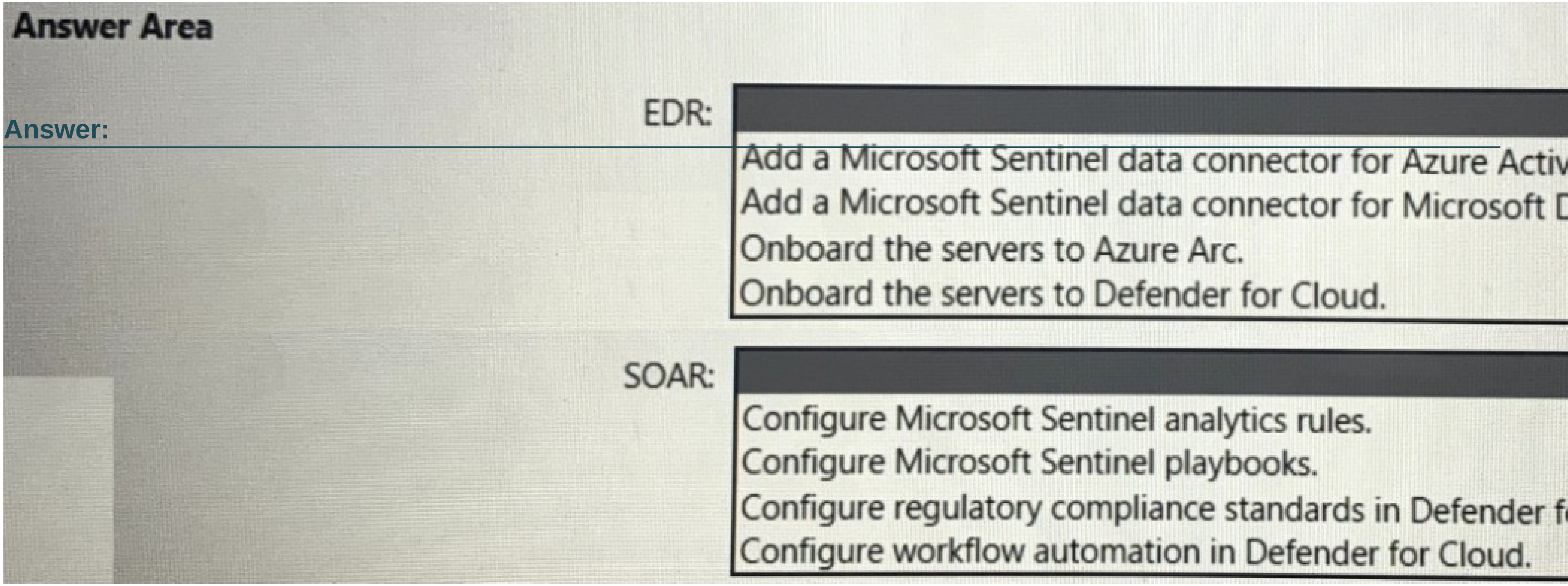
You plan to deploy Azure virtual machines that will run Windows Server.

You need to enable extended detection and response (EDR) and security orchestration, automation, and response (SOAR) capabilities for Microsoft Sentinel.

How should you recommend enabling each capability? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer:



Answer Area

EDR:

Add a Microsoft Sentinel data connector for Azure Activ

Add a Microsoft Sentinel data connector for Microsoft D

Onboard the servers to Azure Arc.

Onboard the servers to Defender for Cloud.

SOAR:

Configure Microsoft Sentinel analytics rules.

Configure Microsoft Sentinel playbooks.

Configure regulatory compliance standards in Defender fo

Configure workflow automation in Defender for Cloud.