

# Exam Questions SC-100

Microsoft Cybersecurity Architect

<https://www.2passeasy.com/dumps/SC-100/>



NEW QUESTION 1

- (Exam Topic 1)

You are evaluating the security of ClaimsApp.

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
FD1 can be used to protect all the instances of ClaimsApp.	<input type="radio"/>	<input type="radio"/>
FD1 must be configured to have a certificate for claims.fabrikam.com.	<input type="radio"/>	<input type="radio"/>
To block connections from North Korea to ClaimsApp, you require a custom rule in FD1.	<input type="radio"/>	<input type="radio"/>

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Statements	Yes	No
FD1 can be used to protect all the instances of ClaimsApp.	<input type="radio"/>	<input checked="" type="radio"/>
FD1 must be configured to have a certificate for claims.fabrikam.com.	<input checked="" type="radio"/>	<input type="radio"/>
To block connections from North Korea to ClaimsApp, you require a custom rule in FD1.	<input checked="" type="radio"/>	<input type="radio"/>

NEW QUESTION 2

- (Exam Topic 1)

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.

Answer Area

To enforce compliance to the regulatory standard, create:	<div><div>An Azure Automation account</div><div>A blueprint</div><div>A managed identity</div><div>Workflow automation</div></div>
To exclude TestRG from the compliance assessment:	<div><div>Edit an Azure blueprint</div><div>Modify a Defender for Cloud workflow automation</div><div>Modify an Azure policy definition</div><div>Update an Azure policy assignment</div></div>

- A. Mastered
- B. Not Mastered

Answer: A

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> <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>

NEW QUESTION 3

- (Exam Topic 1)

You need to recommend a solution to secure the MedicalHistory data in the ClaimsDetail table. The solution must meet the Contoso developer requirements.

What should you include in the recommendation?

- A. Transparent Data Encryption (TDE)
- B. Always Encrypted
- C. row-level security (RLS)
- D. dynamic data masking
- E. data classification

Answer: B

Explanation:

<https://docs.microsoft.com/en-us/learn/modules/protect-data-transit-rest/4-explain-object-encryption-secure-encl>

#### NEW QUESTION 4

- (Exam Topic 1)

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

What should you include in the recommendation? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

**Answer Area**

For the AWS EC2 instances:

- Azure Blueprints
- Defender for Cloud
- Microsoft Defender for Cloud Apps
- Microsoft Defender for servers
- Microsoft Endpoint Manager
- Microsoft Sentinel

For the AWS service logs:

- Azure Blueprints
- Defender for Cloud
- Microsoft Defender for Cloud Apps
- Microsoft Defender for servers
- Microsoft Endpoint Manager
- Microsoft Sentinel

A. Mastered

B. Not Mastered

Answer: A

Explanation:

**Answer Area**

For the AWS EC2 instances:

- Azure Blueprints
- Defender for Cloud
- Microsoft Defender for Cloud Apps
- Microsoft Defender for servers
- Microsoft Endpoint Manager
- Microsoft Sentinel

For the AWS service logs:

- Azure Blueprints
- Defender for Cloud
- Microsoft Defender for Cloud Apps
- Microsoft Defender for servers
- Microsoft Endpoint Manager
- Microsoft Sentinel

#### NEW QUESTION 5

- (Exam Topic 1)

You need to recommend a solution to meet the requirements for connections to ClaimsDB.

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

NOTE: Each correct selection is worth one point.

**Answer Area**

ClaimsDB must be accessible only from Azure virtual networks:

- A NAT gateway
- A network security group
- A private endpoint
- A service endpoint

The app services permission for ClaimsApp must be assigned to ClaimsDB:

- A custom role-based access control (RBAC) role
- A managed identity
- An access package
- Azure AD Privileged Identity Management (PIM)

A. Mastered

B. Not Mastered

Answer: A



**Explanation:**  
**Answer Area**

ClaimsDB must be accessible only from Azure virtual networks:

- A NAT gateway
- A network security group
- A private endpoint
- A service endpoint

The app services permission for ClaimsApp must be assigned to ClaimsDB:

- A custom role-based access control (RBAC) role
- A managed identity
- An access package
- Azure AD Privileged Identity Management (PIM)

**NEW QUESTION 6**

- (Exam Topic 2)

You need to recommend an identity security solution for the Azure AD tenant of Litware. The solution must meet the identity requirements and the regulatory compliance requirements.

What should you recommend? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

**Answer Area**

For the delegated management of users and groups, use:

- AD DS organizational units
- Azure AD administrative units
- Custom Azure AD roles

To ensure that you can perform leaked credential detection:

- Enable password hash synchronization in the Azure AD Connect deployment
- Enable Security defaults in the Azure AD tenant of Litware
- Replace pass-through authentication with Active Directory Federation Services

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

**Answer Area**

For the delegated management of users and groups, use:

- AD DS organizational units
- Azure AD administrative units
- Custom Azure AD roles

To ensure that you can perform leaked credential detection:

- Enable password hash synchronization in the Azure AD Connect deployment
- Enable Security defaults in the Azure AD tenant of Litware
- Replace pass-through authentication with Active Directory Federation Services

**NEW QUESTION 7**

- (Exam Topic 2)

You need to recommend a strategy for securing the litware.com forest. The solution must meet the identity requirements. What should you include in the recommendation? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

**Answer Area**

For Azure AD-targeted threats:

- Azure AD Identity Protection
- Azure AD Password Protection
- Microsoft Defender for Cloud

For AD DS-targeted threats:

- An account lockout policy in AD DS
- Microsoft Defender for Endpoint
- Microsoft Defender for Identity

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

\* 1. Azure AD Identity Protection Brute Force Detection:

<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/overview-identity-protection>

\* 2. Defender for Identity

MDI can detect brute force attacks: ref:

<https://docs.microsoft.com/en-us/defender-for-identity/compromised-credentials-alerts#suspected-brute-force-at>

**NEW QUESTION 8**

- (Exam Topic 3)

You have a Microsoft 365 E5 subscription and an Azure subscripts You need to evaluate the existing environment to increase the overall security posture for the following components:

- Windows 11 devices managed by Microsoft Intune
- Azure Storage accounts
- Azure virtual machines

What should you use to evaluate the components? To answer, select the appropriate options in the answer area.

Windows 11 devices:

Microsoft 365 compliance center
Microsoft 365 Defender
Microsoft Defender for Cloud
Microsoft Sentinel

Azure virtual machines:

Microsoft 365 compliance center
Microsoft 365 Defender
Microsoft Defender for Cloud
Microsoft Sentinel

Azure Storage accounts:

Microsoft 365 compliance center
Microsoft 365 Defender
Microsoft Defender for Cloud
Microsoft Sentinel

- A. Mastered  
 B. Not Mastered

**Answer:** A

**Explanation:**

Selection 1: Microsoft 365 Defender (Microsoft Defender for Endpoint is part of it). Selection 2: Microsoft Defender for Cloud.

Selection 3: Microsoft Defender for Cloud.

<https://docs.microsoft.com/en-us/learn/modules/design-strategy-for-secure-paas-iaas-saas-services/8-specify-sec>

**NEW QUESTION 9**

- (Exam Topic 3)

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?

- A. Azure Active Directory (Azure AD) Conditional Access App Control policies  
 B. OAuth app policies in Microsoft Defender for Cloud Apps  
 C. app protection policies in Microsoft Endpoint Manager  
 D. application control policies in Microsoft Defender for Endpoint

**Answer:** D

**Explanation:**

<https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/sele>

**NEW QUESTION 10**

- (Exam Topic 3)

You have an Azure subscription that contains several storage accounts. The storage accounts are accessed by legacy applications that are authenticated by using access keys.

You need to recommend a solution to prevent new applications from obtaining the access keys of the storage accounts. The solution must minimize the impact on the legacy applications.

What should you include in the recommendation?

- A. Apply read-only locks on the storage accounts.  
 B. Set the AllowSharcdKeyAccess property to false.  
 C. Set the AllowBlobPublicAcccss property to false.  
 D. Configure automated key rotation.

**Answer:** A

**Explanation:**

<https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources>

#### NEW QUESTION 10

- (Exam Topic 3)

You need to design a solution to provide administrators with secure remote access to the virtual machines. The solution must meet the following requirements:

- Prevent the need to enable ports 3389 and 22 from the internet.
- Only provide permission to connect the virtual machines when required.
- Ensure that administrators use the Azure portal to connect to the virtual machines.

Which two actions should you include in the solution? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

- A. Enable Azure Active Directory (Azure AD) Privileged Identity Management (PIM) roles as virtual machine contributors.
- B. Configure Azure VPN Gateway.
- C. Enable Just Enough Administration (JEA).
- D. Enable just-in-time (JIT) VM access.
- E. Configure Azure Bastion.

**Answer:** DE

#### Explanation:

<https://docs.microsoft.com/en-us/powershell/scripting/learn/remoting/jea/overview?view=powershell-7.2> <https://docs.microsoft.com/en-us/azure/defender-for-cloud/just-in-time-access-usage> <https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles>

#### NEW QUESTION 14

- (Exam Topic 3)

Your company has a Microsoft 365 E5 subscription. The company wants to identify and classify data in Microsoft Teams, SharePoint Online, and Exchange Online. You need to recommend a solution to identify documents that contain sensitive information. What should you include in the recommendation?

- A. data classification content explorer
- B. data loss prevention (DLP)
- C. eDiscovery
- D. Information Governance

**Answer:** B

#### NEW QUESTION 16

- (Exam Topic 3)

Your company has a multi-cloud environment that contains a Microsoft 365 subscription, an Azure subscription, and Amazon Web Services (AWS) implementation. You need to recommend a security posture management solution for the following components:

- Azure IoT Edge devices
- AWS EC2 instances

Which services should you include in the recommendation? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

#### Answer Area

For the IoT Edge devices:	<input type="checkbox"/> Azure Arc <input type="checkbox"/> Microsoft Defender for Cloud <input type="checkbox"/> Microsoft Defender for Cloud Apps <input type="checkbox"/> Microsoft Defender for Endpoint <input type="checkbox"/> Microsoft Defender for IoT
For the AWS EC2 instances:	<input type="checkbox"/> Azure Arc only <input type="checkbox"/> Microsoft Defender for Cloud and Azure Arc <input type="checkbox"/> Microsoft Defender for Cloud Apps only <input type="checkbox"/> Microsoft Defender for Cloud only <input type="checkbox"/> Microsoft Defender for Endpoint and Azure Arc <input type="checkbox"/> Microsoft Defender for Endpoint only

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

<https://docs.microsoft.com/en-us/azure/defender-for-iot/organizations/architecture> <https://docs.microsoft.com/en-us/azure/defender-for-cloud/quickstart-onboard-aws?pivots=env-settings> <https://docs.microsoft.com/en-us/azure/azure-arc/servers/overview#supported-cloud-operations>

#### NEW QUESTION 17

- (Exam Topic 3)

You have an Azure subscription that has Microsoft Defender for Cloud enabled. You are evaluating the Azure Security Benchmark V3 report.

In the Secure management ports controls, you discover that you have 0 out of a potential 8 points.

You need to recommend configurations to increase the score of the Secure management ports controls. Solution: You recommend enabling just-in-time (JIT) VM access on all virtual machines.

Does this meet the goal?



- A. Yes
- B. No

**Answer:** A

**Explanation:**

<https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-privileged-access#pa-2-avoid-s>

**NEW QUESTION 19**

- (Exam Topic 3)

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

**Answer:** D

**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 21**

- (Exam Topic 3)

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

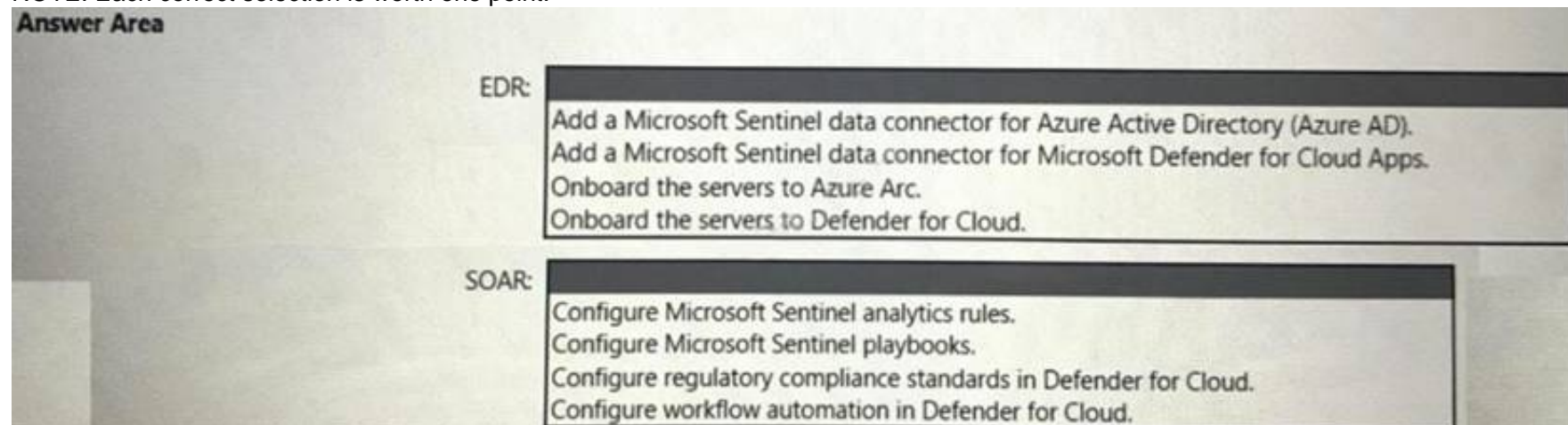
The Azure subscription contains a Microsoft Sentinel workspace. Microsoft Sentinel data connectors are configured for Microsoft 365, Microsoft 365 Defender, Defender for Cloud, and Azure.

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.



- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

For SOAR read this <https://docs.microsoft.com/en-us/azure/sentinel/automate-responses-with-playbooks> Endpoint detection and response (EDR) and eXtended detection and response (XDR) are both part of Microsoft Defender.

<https://docs.microsoft.com/en-us/microsoft-365/security/defender/eval-overview?view=o365-worldwide>

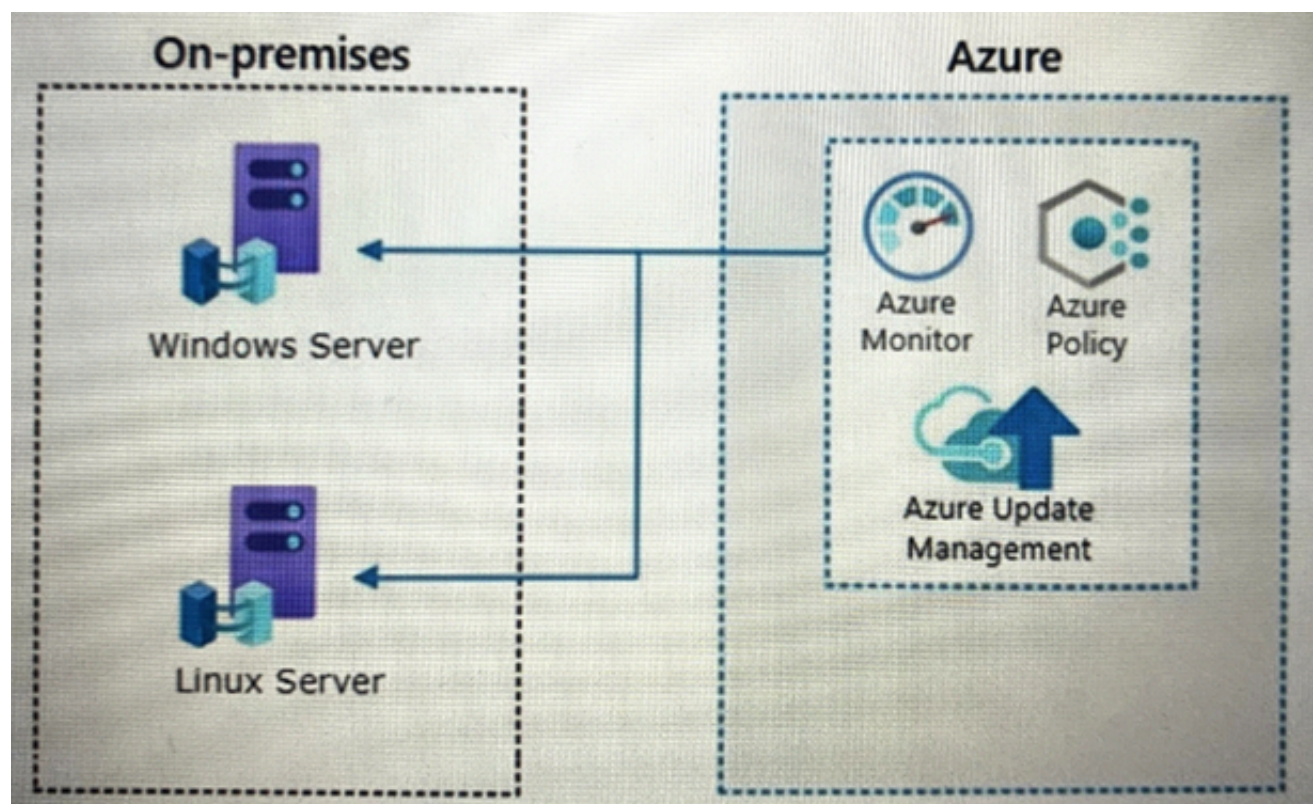
**NEW QUESTION 26**

- (Exam Topic 3)

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.

- A. Azure VPN Gateway
- B. guest configuration in Azure Policy
- C. on-premises data gateway
- D. Azure Bastion
- E. Azure Arc

**Answer:** BE

**Explanation:**

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

### NEW QUESTION 30

- (Exam Topic 3)

Your company has a Microsoft 365 E5 subscription.

The Chief Compliance Officer plans to enhance privacy management in the working environment. You need to recommend a solution to enhance the privacy management. The solution must meet the following requirements:

- Identify unused personal data and empower users to make smart data handling decisions.
- Provide users with notifications and guidance when a user sends personal data in Microsoft Teams.
- Provide users with recommendations to mitigate privacy risks. What should you include in the recommendation?

- A. Microsoft Viva Insights
- B. Advanced eDiscovery
- C. Privacy Risk Management in Microsoft Priva
- D. communication compliance in insider risk management

**Answer:** C

**Explanation:**

Privacy Risk Management in Microsoft Priva gives you the capability to set up policies that identify privacy risks in your Microsoft 365 environment and enable easy remediation. Privacy Risk Management policies are meant to be internal guides and can help you: Detect overexposed personal data so that users can secure it. Spot and limit transfers of personal data across departments or regional borders. Help users identify and reduce the amount of unused personal data that you store.

<https://www.microsoft.com/en-us/security/business/privacy/microsoft-priva-risk-management>

### NEW QUESTION 34

- (Exam Topic 3)

You have an Azure subscription that has Microsoft Defender for Cloud enabled. Suspicious authentication activity alerts have been appearing in the Workload protections dashboard.

You need to recommend a solution to evaluate and remediate the alerts by using workflow automation. The solution must minimize development effort. What should you include in the recommendation?

- A. Azure Monitor webhooks
- B. Azure Logics Apps
- C. Azure Event Hubs
- D. Azure Functions apps

**Answer:** B

**Explanation:**

The workflow automation feature of Microsoft Defender for Cloud feature can trigger Logic Apps on security alerts, recommendations, and changes to regulatory compliance. Note: Azure Logic Apps is a cloud-based platform for creating and running automated workflows that integrate your apps, data, services, and systems.



With this platform, you can quickly develop highly scalable integration solutions for your enterprise and business-to-business (B2B) scenarios.

#### NEW QUESTION 36

- (Exam Topic 3)

You are designing security for an Azure landing zone. Your company identifies the following compliance and privacy requirements:

- Encrypt cardholder data by using encryption keys managed by the company.
- Encrypt insurance claim files by using encryption keys hosted on-premises.

Which two configurations meet the compliance and privacy requirements? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

- A. Store the insurance claim data in Azure Blob storage encrypted by using customer-provided keys.
- B. Store the cardholder data in an Azure SQL database that is encrypted by using keys stored in Azure Key Vault Managed HSM
- C. Store the insurance claim data in Azure Files encrypted by using Azure Key Vault Managed HSM.
- D. Store the cardholder data in an Azure SQL database that is encrypted by using Microsoft-managed Keys.

**Answer:** AC

#### Explanation:

<https://azure.microsoft.com/en-us/blog/customer-provided-keys-with-azure-storage-service-encryption/>

#### NEW QUESTION 39

- (Exam Topic 3)

You have an Azure subscription that has Microsoft Defender for Cloud enabled. You need to enforce ISO 2700V2013 standards for the subscription. The solution must ensure that noncompliant resources are remediated automatically

What should you use?

- A. the regulatory compliance dashboard in Defender for Cloud
- B. Azure Policy
- C. Azure Blueprints
- D. Azure role-based access control (Azure RBAC)

**Answer:** B

#### Explanation:

<https://azure.microsoft.com/en-us/blog/simplifying-your-environment-setup-while-meeting-compliance-needs-w>

#### NEW QUESTION 44

- (Exam Topic 3)

You have an Azure subscription that has Microsoft Defender for Cloud enabled. You are evaluating the Azure Security Benchmark V3 report.

In the Secure management ports controls, you discover that you have 0 out of a potential 8 points. You need to recommend configurations to increase the score of the Secure management ports controls.

Solution: You recommend onboarding all virtual machines to Microsoft Defender for Endpoint. Does this meet the goal?

- A. Yes
- B. No

**Answer:** B

#### Explanation:

<https://docs.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls>

#### NEW QUESTION 48

- (Exam Topic 3)

Your company is developing an invoicing application that will use Azure Active Directory (Azure AD) B2C. The application will be deployed as an App Service web app. You need to recommend a solution to the application development team to secure the application from identity related attacks. Which two configurations should you recommend? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

- A. Azure AD Conditional Access integration with user flows and custom policies
- B. Azure AD workbooks to monitor risk detections
- C. custom resource owner password credentials (ROPC) flows in Azure AD B2C
- D. access packages in Identity Governance
- E. smart account logout in Azure AD B2C

**Answer:** AE

#### Explanation:

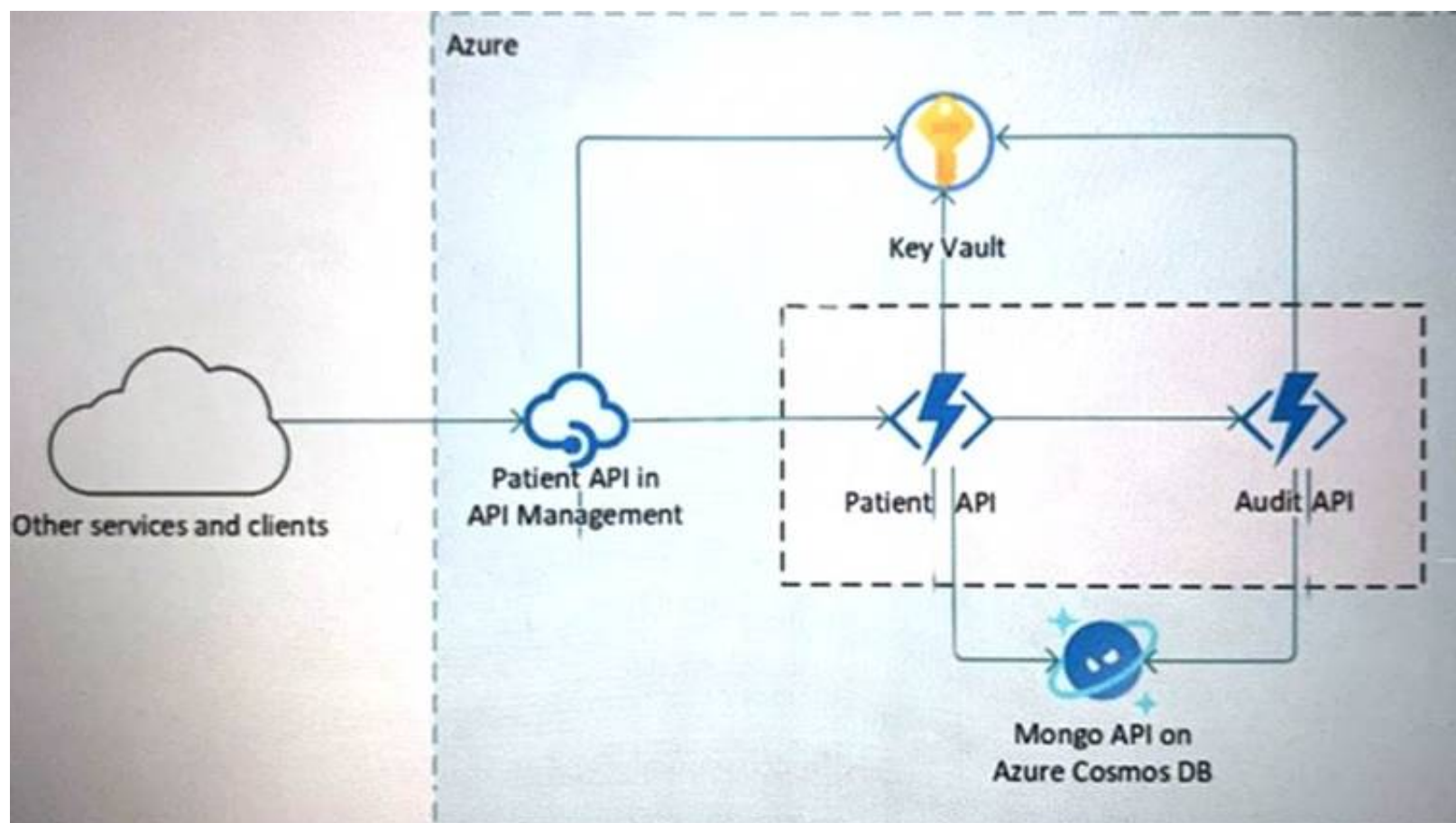
<https://docs.microsoft.com/en-us/azure/active-directory-b2c/threat-management>

<https://docs.microsoft.com/en-us/azure/active-directory-b2c/conditional-access-user-flow?pivots=b2c-user-flow>

#### NEW QUESTION 52

- (Exam Topic 3)

Your company is developing a serverless application in Azure that will have the architecture shown in the following exhibit.



You need to recommend a solution to isolate the compute components on an Azure virtual network. What should you include in the recommendation?

- A. Azure Active Directory (Azure AD) enterprise applications
- B. an Azure App Service Environment (ASE)
- C. Azure service endpoints
- D. an Azure Active Directory (Azure AD) application proxy

**Answer: B**

**Explanation:**

App Service environments (ASEs) are appropriate for application workloads that require:

Very high scale, Isolation and secure network access, High memory utilization. This capability can host your: Windows web apps, Linux web apps, Docker containers, Mobile apps, Functions.

<https://docs.microsoft.com/en-us/azure/app-service/environment/overview>

**NEW QUESTION 53**

- (Exam Topic 3)

You are designing the security standards for containerized applications onboarded to Azure. You are evaluating the use of Microsoft Defender for Containers.

In which two environments can you use Defender for Containers to scan for known vulnerabilities? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

- A. Linux containers deployed to Azure Container Registry
- B. Linux containers deployed to Azure Kubernetes Service (AKS)
- C. Windows containers deployed to Azure Container Registry
- D. Windows containers deployed to Azure Kubernetes Service (AKS)
- E. Linux containers deployed to Azure Container Instances

**Answer: AB**

**Explanation:**

<https://docs.microsoft.com/en-us/learn/modules/design-strategy-for-secure-paas-iaas-saas-services/9-specify-sec> <https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-containers-introduction#view-vulnerabi>

**NEW QUESTION 54**

- (Exam Topic 3)

You are designing security for a runbook in an Azure Automation account. The runbook will copy data to Azure Data Lake Storage Gen2.

You need to recommend a solution to secure the components of the copy process.

What should you include in the recommendation for each component? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Data security:

Access keys stored in Azure Key Vault
Automation Contributor built-in role
Azure Private Link with network service tags
Azure Web Application Firewall rules with network service tags

Network access control:

Access keys stored in Azure Key Vault
Automation Contributor built-in role
Azure Private Link with network service tags
Azure Web Application Firewall rules with network service tags

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Data Security = Access Keys stored in Azure Key Vault

Network access control = Azure Private Link with network service tags

<https://docs.microsoft.com/en-us/azure/automation/automation-security-guidelines#data-security>

**NEW QUESTION 58**

- (Exam Topic 3)

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 blob containers in Azure Storage, you recommend encryption that uses customer-managed keys (CMKs).

Does this meet the goal?

- A. Yes
- B. No

**Answer:** A

**NEW QUESTION 59**

- (Exam Topic 3)

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?

- 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 in 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>

**NEW QUESTION 60**

- (Exam Topic 3)

A customer follows the Zero Trust model and explicitly verifies each attempt to access its corporate applications.

The customer discovers that several endpoints are infected with malware. The customer suspends access attempts from the infected endpoints.

The malware is removed from the end point.

Which two conditions must be met before endpoint users can access the corporate applications again? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Microsoft Defender for Endpoint reports the endpoints as compliant.
- B. Microsoft Intune reports the endpoints as compliant.
- C. A new Azure Active Directory (Azure AD) Conditional Access policy is enforced.
- D. The client access tokens are refreshed.

**Answer:** CD



**Explanation:**

<https://www.microsoft.com/security/blog/2022/02/17/4-best-practices-to-implement-a-comprehensive-zero-trust> <https://docs.microsoft.com/en-us/azure/active-directory/develop/refresh-tokens>

**NEW QUESTION 62**

- (Exam Topic 3)

You use Azure Pipelines with Azure Repos to implement continuous integration and continuous deployment (CI/CO) workflows.

You need to recommend best practices to secure the stages of the CI/CD workflows based on the Microsoft Cloud Adoption Framework for Azure.

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

NOTE: Each correct selection is worth one point.

**Answer Area**

Git workflow:

Secure deployment credentials:

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

**Answer Area**

Git workflow:

Secure deployment credentials:

**NEW QUESTION 64**

- (Exam Topic 3)

You have a Microsoft 365 subscription

You need to recommend a security solution to monitor the following activities:

- User accounts that were potentially compromised
- Users performing bulk file downloads from Microsoft SharePoint Online

What should you include in the recommendation for each activity? To answer, drag the appropriate components to the correct activities. Each component 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.

**Components**

- A data loss prevention (DLP) policy
- Azure Active Directory (Azure AD) Conditional Access
- Azure Active Directory (Azure AD) Identity Protection
- Microsoft Defender for Cloud
- Microsoft Defender for Cloud Apps

**Answer Area**

User accounts that were potentially compromised:

Users performing bulk file downloads from SharePoint Online:

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

<https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks> <https://docs.microsoft.com/en-us/defender-cloud-apps/policies-threat-protection#detect-mass-download-data-exf> <https://docs.microsoft.com/en-us/microsoft-365/security/defender/investigate-users>

**NEW QUESTION 65**

- (Exam Topic 3)

Your company is developing a new Azure App Service web app. You are providing design assistance to verify the security of the web app.

You need to recommend a solution to test the web app for vulnerabilities such as insecure server configurations, cross-site scripting (XSS), and SQL injection.

What should you include in the recommendation?

- A. interactive application security testing (IAST)
- B. static application security testing (SAST)

- C. runtime application self-protection (RASP)
- D. dynamic application security testing (DAST)

**Answer:** D

**Explanation:**

<https://docs.microsoft.com/en-us/azure/security/develop/secure-develop#test-your-application-in-an-operating-st>

**NEW QUESTION 69**

- (Exam Topic 3)

Your company has Microsoft 365 E5 licenses and Azure subscriptions.

The company plans to automatically label sensitive data stored in the following locations:

- Microsoft SharePoint Online
- Microsoft Exchange Online
- Microsoft Teams

You need to recommend a strategy to identify and protect sensitive data.

Which scope should you recommend for the sensitivity label policies? To answer, drag the appropriate scopes to the correct locations. Each scope 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.



- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Box 1: Groups and sites

Box 2: Groups and sites

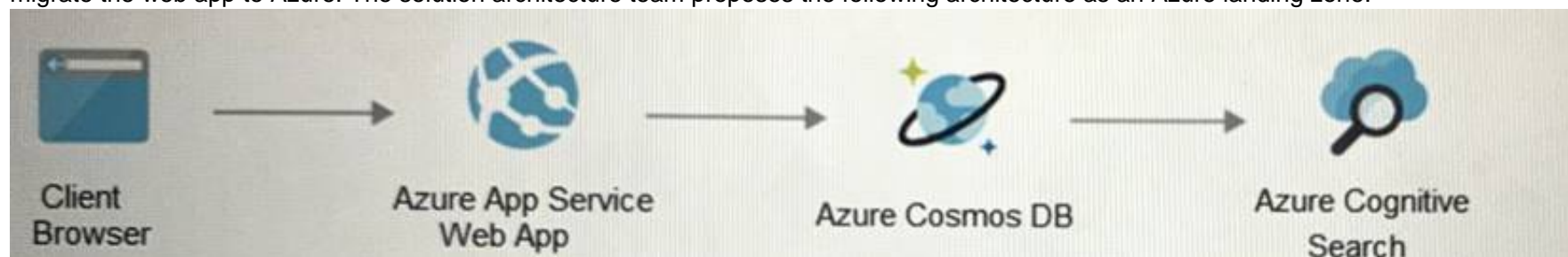
Box 3: Files and emails –

<https://docs.microsoft.com/en-us/microsoft-365/compliance/sensitivity-labels?view=o365-worldwide> Go to label scopes

**NEW QUESTION 74**

- (Exam Topic 3)

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 Key Vault to store credentials.

- A. Yes
- B. No

**Answer:** B

**Explanation:**

When using Azure-provided PaaS services (e.g., Azure Storage, Azure Cosmos DB, or Azure Web App, use the PrivateLink connectivity option to ensure all data exchanges are over the private IP space and the traffic never leaves the Microsoft network.

**NEW QUESTION 76**

- (Exam Topic 3)

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?

- A. role-based authorization
- B. Azure AD Privileged Identity Management (PIM)
- C. resource-based authorization
- D. Azure AD Multi-Factor Authentication

**Answer:** B

**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>

#### NEW QUESTION 77

- (Exam Topic 3)

Your company has an Azure subscription that has enhanced security enabled for Microsoft Defender for Cloud. The company signs a contract with the United States government. You need to review the current subscription for NIST 800-53 compliance. What should you do first?

- A. From Defender for Cloud, review the secure score recommendations.
- B. From Microsoft Sentinel, configure the Microsoft Defender for Cloud data connector.
- C. From Defender for Cloud, review the Azure security baseline for audit report.
- D. From Defender for Cloud, add a regulatory compliance standard.

**Answer:** D

#### Explanation:

<https://docs.microsoft.com/en-us/azure/defender-for-cloud/update-regulatory-compliance-packages#what-regula>

#### NEW QUESTION 79

- (Exam Topic 3)

You are evaluating an Azure environment for compliance.

You need to design an Azure Policy implementation that can be used to evaluate compliance without changing any resources.

Which effect should you use in Azure Policy?

- A. Deny
- B. Disabled
- C. Modify
- D. Append

**Answer:** B

#### Explanation:

Before looking to manage new or updated resources with your new policy definition, it's best to see how it evaluates a limited subset of existing resources, such as a test resource group. Use the enforcement mode Disabled (DoNotEnforce) on your policy assignment to prevent the effect from triggering or activity log entries from being created.

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

#### NEW QUESTION 83

- (Exam Topic 3)

You are designing a security strategy for providing access to Azure App Service web apps through an Azure Front Door instance.

You need to recommend a solution to ensure that the web apps only allow access through the Front Door instance.

Solution: You recommend access restrictions to allow traffic from the backend IP address of the Front Door instance.

Does this meet the goal?

- A. Yes
- B. No

**Answer:** B

#### NEW QUESTION 87

- (Exam Topic 3)

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?

- A. Microsoft 365 Defender
- B. Microsoft Defender for Cloud
- C. Microsoft Defender for Cloud Apps
- D. Microsoft Sentinel

**Answer:** D

#### NEW QUESTION 88

- (Exam Topic 3)

Your company has devices that run either Windows 10, Windows 11, or Windows Server. You are in the process of improving the security posture of the devices.

You plan to use security baselines from the Microsoft Security Compliance Toolkit.

What should you recommend using to compare the baselines to the current device configurations?

- A. Microsoft Intune
- B. Policy Analyzer
- C. Local Group Policy Object (LGPO)
- D. Windows Autopilot

**Answer:** B

#### Explanation:

<https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-security-configuration-framework>



#### NEW QUESTION 93

- (Exam Topic 3)

You have an on-premises network that has several legacy applications. The applications perform LDAP queries against an existing directory service. You are migrating the on-premises infrastructure to a cloud-only infrastructure.

You need to recommend an identity solution for the infrastructure that supports the legacy applications. The solution must minimize the administrative effort to maintain the infrastructure.

Which identity service should you include in the recommendation?

A. Azure Active Directory Domain Services (Azure AD DS)

B. Azure Active Directory (Azure AD) B2C

C. Azure Active Directory (Azure AD)

D. Active Directory Domain Services (AD DS)

**Answer:** A

**Explanation:**

<https://docs.microsoft.com/en-us/azure/active-directory-domain-services/overview>

#### NEW QUESTION 94

- (Exam Topic 3)

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 blob containers in Azure Storage, you recommend encryption that uses Microsoft-managed keys within an encryption scope.

Does this meet the goal?

A. Yes

B. No

**Answer:** B

**Explanation:**

<https://docs.microsoft.com/en-us/azure/key-vault/keys/how-to-configure-key-rotation>

#### NEW QUESTION 99

.....

## THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual SC-100 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the SC-100 Product From:

<https://www.2passeasy.com/dumps/SC-100/>

## Money Back Guarantee

### SC-100 Practice Exam Features:

- \* SC-100 Questions and Answers Updated Frequently
- \* SC-100 Practice Questions Verified by Expert Senior Certified Staff
- \* SC-100 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- \* SC-100 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year