

# Microsoft

## Exam Questions SC-100

Microsoft Cybersecurity Architect



**NEW QUESTION 1**

- (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 2**

- (Exam Topic 3)

You have an Azure subscription that has Microsoft Defender for Cloud enabled. You have an Amazon Web Services (AWS) implementation.

You plan to extend the Azure security strategy to the AWS implementation. The solution will NOT use Azure Arc. Which three services can you use to provide security for the AWS resources? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

- A. Azure Active Directory (Azure AD) Privileged Identity Management (PIM)
- B. Azure Active Directory (Azure AD) Conditional Access
- C. Microsoft Defender for servers
- D. Azure Policy
- E. Microsoft Defender for Containers

**Answer: BDE**

**Explanation:**

<https://docs.microsoft.com/en-us/azure/defender-for-cloud/supported-machines-endpoint-solutions-clouds-conta>

**NEW QUESTION 3**

- (Exam Topic 3)

You have an Azure subscription and an on-premises datacenter. The datacenter contains 100 servers that run Windows Server. All the servers are backed up to a Recovery Services vault by using Azure Backup and the Microsoft Azure Recovery Services (MARS) agent.

You need to design a recovery solution for ransomware attacks that encrypt the on-premises servers. The solution must follow Microsoft Security Best Practices and protect against the following risks:

- A compromised administrator account used to delete the backups from Azure Backup before encrypting the servers
- A compromised administrator account used to disable the backups on the MARS agent before encrypting the servers

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

Answer Area



- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

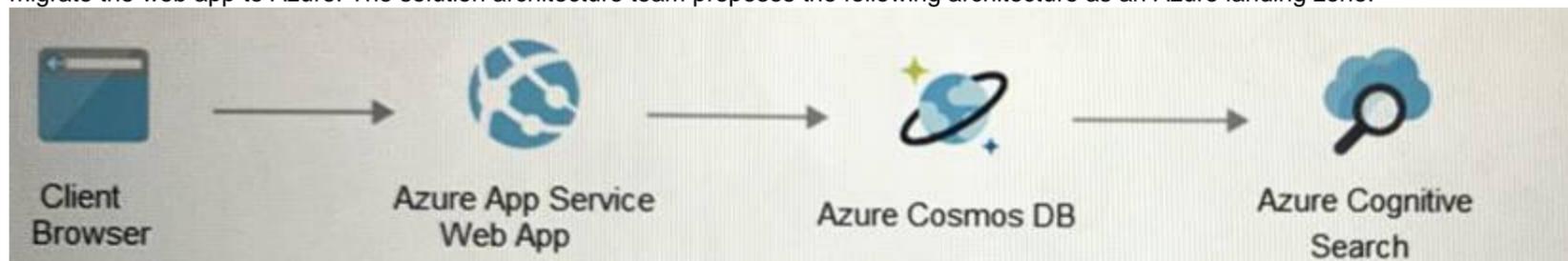
Answer Area



**NEW QUESTION 4**

- (Exam Topic 3)

Your on-premises network contains an e-commerce web app that was developed in Angular and Nodejs. 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:**

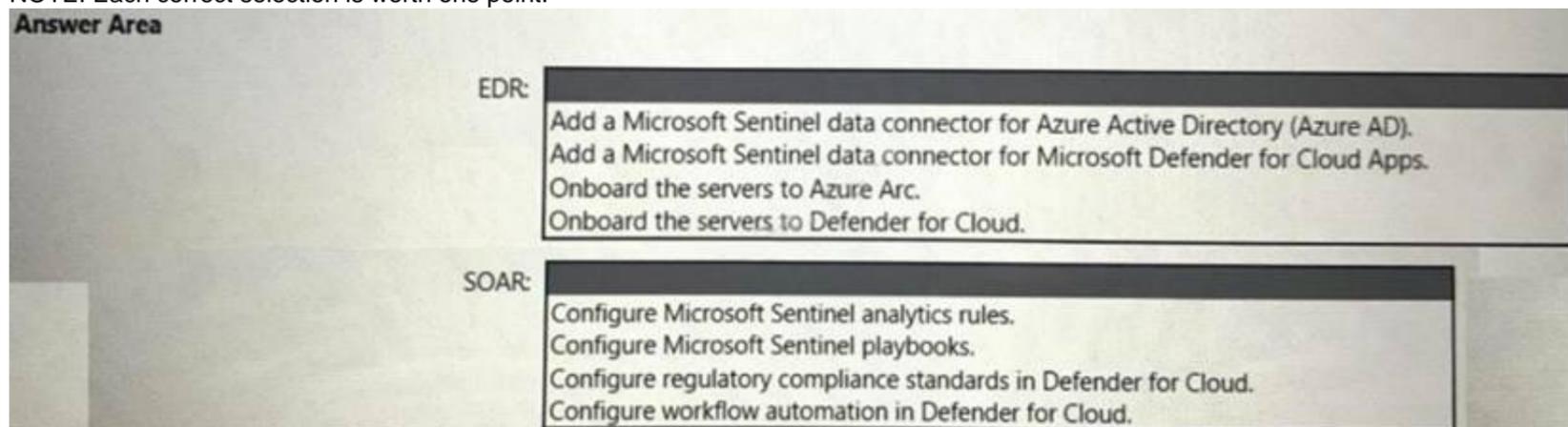
When using Azure-provided PaaS services (e.g., Azure Storage, Azure Cosmos DB, or Azure Web App, use the PrivateLink connectivity option to ensure all data exchanges are over the private IP space and the traffic never leaves the Microsoft network.

**NEW QUESTION 5**

- (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 6**

- (Exam Topic 3)

You open Microsoft Defender for Cloud as shown in the following exhibit.

Controls	Max score	Current Score	Potential score incre...	Unhealthy resources	Resource health	Actions
Enable MFA	10	0.00	+ 18% (10 points)	1 of 1 resources	Unhealthy	
Secure management ports	8	3.33	+ 5% (2.67 points)	1 of 3 resources	Unhealthy	
Remediate vulnerabilities	6	0.00	+ 11% (6 points)	3 of 3 resources	Unhealthy	
Apply system updates	6	6.00	+ 0% (0 points)	None	Healthy	
Manage access and permissions	4	0.00	+ 7% (4 points)	1 of 12 resources	Unhealthy	
Enable encryption at rest	4	1.00	+ 5% (3 points)	3 of 4 resources	Unhealthy	
Restrict unauthorized network access	4	3.00	+ 2% (1 point)	1 of 11 resources	Unhealthy	
Remediate security configurations	4	3.00	+ 2% (1 point)	1 of 4 resources	Unhealthy	
Encrypt data in transit	4	3.33	+ 1% (0.67 points)	1 of 6 resources	Unhealthy	
Apply adaptive application control	3	3.00	+ 0% (0 points)	None	Healthy	
Enable endpoint protection	2	0.67	+ 2% (1.33 points)	2 of 3 resources	Unhealthy	
Enable auditing and logging	1	0.00	+ 2% (1 point)	4 of 5 resources	Unhealthy	
Enable enhanced security features	Not scored	Not scored	+ 0% (0 points)	None	Healthy	
Implement security best practices	Not scored	Not scored	+ 0% (0 points)	9 of 30 resources	Unhealthy	

Use the drop-down menus to select the answer choice that complete each statements based on the information presented in the graphic.  
 NOTE: Each correct selection is worth one point.

**Answer Area**

To increase the score for the Restrict unauthorized network access control, implement [answer choice].

- Azure Active Directory (Azure AD) Conditional Access policies
- Azure Web Application Firewall (WAF)
- network security groups (NSGs)

To increase the score for the Enable endpoint protection control, implement [answer choice].

- Microsoft Defender for Resource Manager
- Microsoft Defender for servers
- private endpoints

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Selection 1: NSG Selection  
 Selection 2: Microsoft Defender for servers  
<https://docs.microsoft.com/en-us/azure/defender-for-cloud/secure-score-security-controls>

**NEW QUESTION 7**

- (Exam Topic 3)

A customer is deploying Docker images to 10 Azure Kubernetes Service (AKS) resources across four Azure subscriptions. You are evaluating the security posture of the customer.

You discover that the AKS resources are excluded from the secure score recommendations. You need to produce accurate recommendations and update the secure score.

Which two actions should you recommend in Microsoft Defender for Cloud? Each correct answer presents part of the solution. NOTE: Each correct selection is worth one point.

- A. Configure auto provisioning.
- B. Assign regulatory compliance policies.
- C. Review the inventory.
- D. Add a workflow automation.
- E. Enable Defender plans.

**Answer: AE**

**Explanation:**

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

**NEW QUESTION 8**

- (Exam Topic 3)

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?

- 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.

**NEW QUESTION 9**

- (Exam Topic 3)

A customer has a hybrid cloud infrastructure that contains a Microsoft 365 E5 subscription and an Azure subscription.

All the on-premises servers in the perimeter network are prevented from connecting directly to the internet. The customer recently recovered from a ransomware attack.

The customer plans to deploy Microsoft Sentinel.

You need to recommend configurations to meet the following requirements:

- Ensure that the security operations team can access the security logs and the operation logs.
- Ensure that the IT operations team can access only the operations logs, including the event logs of the servers in the perimeter network.

Which two configurations can you include in the recommendation? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

- A. Configure Azure Active Directory (Azure AD) Conditional Access policies.
- B. Use the Azure Monitor agent with the multi-homing configuration.
- C. Implement resource-based role-based access control (RBAC) in Microsoft Sentinel.
- D. Create a custom collector that uses the Log Analytics agent.

**Answer: BC**

**NEW QUESTION 10**

- (Exam Topic 3)

Your company plans to evaluate the security of its Azure environment based on the principles of the Microsoft Cloud Adoption Framework for Azure.

You need to recommend a cloud-based service to evaluate whether the Azure resources comply with the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF).

What should you recommend?

- A. Compliance Manager in Microsoft Purview
- B. Microsoft Defender for Cloud
- C. Microsoft Sentinel
- D. Microsoft Defender for Cloud Apps

**Answer: D**

**NEW QUESTION 10**

- (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 14**

- (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 18**

- (Exam Topic 3)

Your company has a Microsoft 365 E5 subscription.

Users use Microsoft Teams, Exchange Online, SharePoint Online, and OneDrive for sharing and collaborating. The company identifies protected health information (PHI) within stored documents and communications. What should you recommend using to prevent the PHI from being shared outside the company?

- A. insider risk management policies
- B. data loss prevention (DLP) policies
- C. sensitivity label policies
- D. retention policies

**Answer: C**

**Explanation:**

<https://docs.microsoft.com/en-us/microsoft-365/compliance/create-test-tune-dlp-policy?view=o365-worldwide>

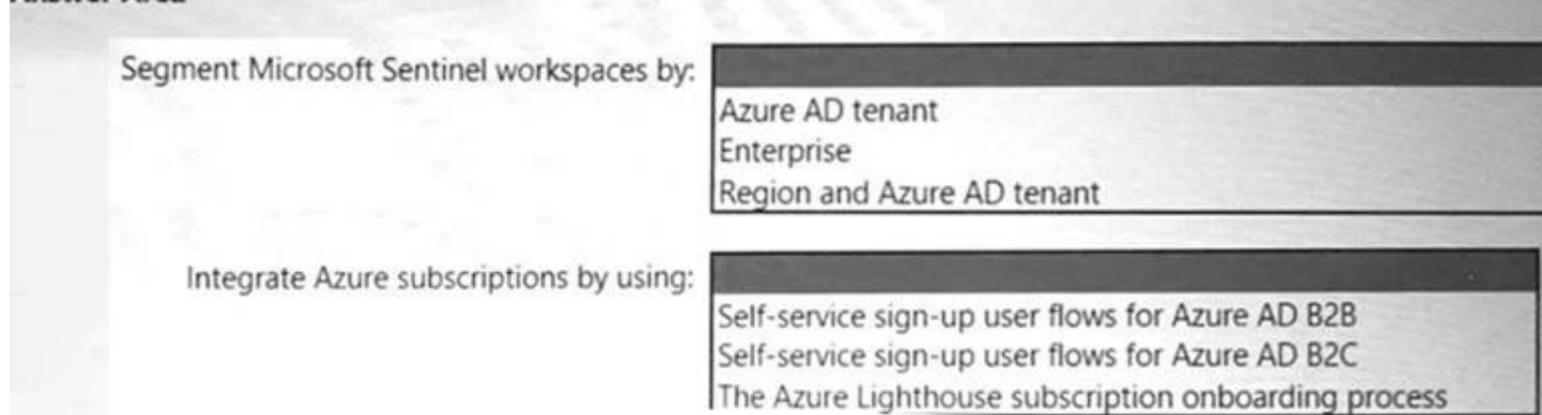
**NEW QUESTION 21**

- (Exam Topic 2)

You need to recommend a SIEM and SOAR strategy that meets the hybrid requirements, the Microsoft Sentinel 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**



- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

Segment Microsoft Sentinel workspaces by: Region and Azure AD tenant Lighthouse subscription

**NEW QUESTION 22**

- (Exam Topic 1)

You need to recommend a solution to scan the application code. The solution must meet the application development requirements. What should you include in the recommendation?

- A. Azure Key Vault
- B. GitHub Advanced Security
- C. Application Insights in Azure Monitor
- D. Azure DevTest Labs

**Answer: B**

**Explanation:**

<https://docs.microsoft.com/en-us/learn/modules/introduction-github-advanced-security/2-what-is-github-advanc>

**NEW QUESTION 23**

- (Exam Topic 1)

You need to recommend a solution to meet the security requirements for the virtual machines. What should you include in the recommendation?

- A. an Azure Bastion host
- B. a network security group (NSG)
- C. just-in-time (JIT) VM access
- D. Azure Virtual Desktop

**Answer: A**

**Explanation:**

The security requirement this question wants us to meet is "The secure host must be provisioned from a custom operating system image."

<https://docs.microsoft.com/en-us/azure/virtual-desktop/set-up-golden-image>

**NEW QUESTION 27**

- (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 configuring gateway-required virtual network integration. Does this meet the goal?

- A. Yes
- B. No

**Answer: B**

**Explanation:**

<https://docs.microsoft.com/en-us/azure/app-service/app-service-ip-restrictions#restrict-access-to-a-specific-azure>

**NEW QUESTION 29**

- (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 31**

- (Exam Topic 3)

You have a Microsoft 365 E5 subscription that uses Microsoft Exchange Online.

You need to recommend a solution to prevent malicious actors from impersonating the email addresses of internal senders.

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**

Service: 

- Azure AD Identity Protection
- Microsoft Defender for DNS
- Microsoft Defender for Office 365**
- Microsoft Purview

Policy type: 

- Anti-phishing**
- Anti-spam
- Data loss prevention (DLP)
- Insider risk management

- A. Mastered
- B. Not Mastered

**Answer: A**

**Explanation:**

**Answer Area**

Service: 

- Azure AD Identity Protection
- Microsoft Defender for DNS
- Microsoft Defender for Office 365**
- Microsoft Purview

Policy type: 

- Anti-phishing**
- Anti-spam
- Data loss prevention (DLP)
- Insider risk management

**NEW QUESTION 35**

- (Exam Topic 3)

You have a Microsoft 365 E5 subscription and an Azure subscription. 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:

Azure virtual machines:

Azure Storage accounts:

- 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 37**

- (Exam Topic 3)

You have an on-premises network and a Microsoft 365 subscription. You are designing a Zero Trust security strategy. Which two security controls should you include as part of the Zero Trust solution? Each correct answer part of the solution. NOTE: Each correct answer is worth one point.

- A. Block sign-attempts from unknown location.
- B. Always allow connections from the on-premises network.
- C. Disable passwordless sign-in for sensitive account.
- D. Block sign-in attempts from noncompliant devices.

**Answer:** AD

**NEW QUESTION 38**

- (Exam Topic 3)

Your company has a hybrid cloud infrastructure.

The company plans to hire several temporary employees within a brief period. The temporary employees will need to access applications and data on the company' premises network.

The company's security policy prevents the use of personal devices for accessing company data and applications.

You need to recommend a solution to provide the temporary employee with access to company resources. The solution must be able to scale on demand. What should you include in the recommendation?

- A. Migrate the on-premises applications to cloud-based applications.
- B. Redesign the VPN infrastructure by adopting a split tunnel configuration.
- C. Deploy Microsoft Endpoint Manager and Azure Active Directory (Azure AD) Conditional Access.
- D. Deploy Azure Virtual Desktop, Azure Active Directory (Azure AD) Conditional Access, and Microsoft Defender for Cloud Apps.

**Answer:** D

**Explanation:**

<https://docs.microsoft.com/en-us/azure/architecture/example-scenario/wvd/windows-virtual-desktop> <https://docs.microsoft.com/en-us/azure/virtual-desktop/security-guide> <https://techcommunity.microsoft.com/t5/security-compliance-and-identity/announcing-microsoft-defender-for-c>

**NEW QUESTION 40**

- (Exam Topic 3)

You plan to deploy a dynamically scaling, Linux-based Azure Virtual Machine Scale Set that will host jump servers. The jump servers will be used by support staff who connect from personal and kiosk devices via the internet. The subnet of the jump servers will be associated to a network security group (NSG).

You need to design an access solution for the Azure Virtual Machine Scale Set. The solution must meet the following requirements:

- Ensure that each time the support staff connects to a jump server; they must request access to the server.
- Ensure that only authorized support staff can initiate SSH connections to the jump servers.
- Maximize protection against brute-force attacks from internal networks and the internet.
- Ensure that users can only connect to the jump servers from the internet.
- Minimize administrative effort.

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

Answer Area



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area



**NEW QUESTION 45**

- (Exam Topic 3)

Note: This question is part of a series of questions that present the same scenario. Each question in the series contains a unique solution that might meet the stated goals. Some question sets might have more than one correct solution, while others might not have a correct solution.

After you answer a question in this section, you will NOT be able to return to it. As a result, these questions will not appear in the review screen.

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 Microsoft-managed keys.

Does this meet the goal?

- A. Yes
- B. No

Answer: B

**NEW QUESTION 48**

- (Exam Topic 3)

Your company has an on-premise network in Seattle and an Azure subscription. The on-premises network contains a Remote Desktop server.

The company contracts a third-party development firm from France to develop and deploy resources to the virtual machines hosted in the Azure subscription.

Currently, the firm establishes an RDP connection to the Remote Desktop server. From the Remote Desktop connection, the firm can access the virtual machines hosted in Azure by using custom administrative tools installed on the Remote Desktop server. All the traffic to the Remote Desktop server is captured by a firewall, and the firewall only allows specific connections from France to the server.

You need to recommend a modern security solution based on the Zero Trust model. The solution must minimize latency for developers.

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

- A. Configure network security groups (NSGs) to allow access from only specific logical groupings of IP address ranges.
- B. Implement Azure Firewall to restrict host pool outbound access.
- C. Configure Azure Active Directory (Azure AD) Conditional Access with multi-factor authentication (MFA) and named locations.
- D. Migrate from the Remote Desktop server to Azure Virtual Desktop.
- E. Deploy a Remote Desktop server to an Azure region located in France.

Answer: BCD

Explanation:

<https://docs.microsoft.com/en-us/azure/firewall/protect-azure-virtual-desktop>

**NEW QUESTION 51**

- (Exam Topic 3)

Your company has an office in Seattle.

The company has two Azure virtual machine scale sets hosted on different virtual networks. The company plans to contract developers in India.

You need to recommend a solution provide the developers with the ability to connect to the virtual machines over SSL from the Azure portal. The solution must meet the following requirements:

- Prevent exposing the public IP addresses of the virtual machines.

- Provide the ability to connect without using a VPN.
- Minimize costs.

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

- A. Deploy Azure Bastion to one virtual network.
- B. Deploy Azure Bastion to each virtual network.
- C. Enable just-in-time VM access on the virtual machines.
- D. Create a hub and spoke network by using virtual network peering.
- E. Create NAT rules and network rules in Azure Firewall.

**Answer:** AD

**Explanation:**

<https://docs.microsoft.com/en-us/learn/modules/connect-vm-with-azure-bastion/2-what-is-azure-bastion>

**NEW QUESTION 55**

- (Exam Topic 3)

Your company plans to follow DevSecOps best practices of the Microsoft Cloud Adoption Framework for Azure to integrate DevSecOps processes into continuous integration and continuous deployment (CI/CD) DevOps pipelines

You need to recommend which security-related tasks to integrate into each stage of the DevOps pipelines. What should recommend? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

**Answer Area**



- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

**Answer Area**



**NEW QUESTION 59**

- (Exam Topic 3)

You have an Azure SQL database named DB1 that contains customer information. A team of database administrators has full access to DB1.

To address customer inquiries, operators in the customer service department use a custom web app named App1 to view the customer information.

You need to design a security strategy for D81. The solution must meet the following requirements:

- When the database administrators access DB1 by using SQL management tools, they must be prevented from viewing the content of the Credit Card attribute of each customer record.
- When the operators view customer records in App1, they must view only the last four digits of the Credit Card attribute.

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

**Answer Area**

For the database administrators:

For the operators:

- A. Mastered
- B. Not Mastered

**Answer:** A

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

For the database administrators:

For the operators:

**NEW QUESTION 61**

- (Exam Topic 3)

For a Microsoft cloud environment, you are designing a security architecture based on the Microsoft Cybersecurity Reference Architectures (MCRA). You need to protect against the following external threats of an attack chain:

- An attacker attempts to exfiltrate data to external websites.
- An attacker attempts lateral movement across domain-joined computers.

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

**Answer Area**

An attacker attempts to exfiltrate data to external websites:

An attacker attempts lateral movement across domain-joined computers:

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

**Answer Area**

An attacker attempts to exfiltrate data to external websites:

Microsoft Defender for Identity  
 Microsoft Defender for Cloud Apps  
**Microsoft Defender for Identity**  
 Microsoft Defender for Office 365

An attacker attempts lateral movement across domain-joined computers:

Microsoft Defender for Identity  
 Microsoft Defender for Cloud Apps  
**Microsoft Defender for Identity**  
 Microsoft Defender for Office 365

**NEW QUESTION 64**

- (Exam Topic 3)

Your company plans to move all on-premises virtual machines to Azure. A network engineer proposes the Azure virtual network design shown in the following table.

Virtual network name	Description	Peering connection
Hub VNet	Linux and Windows virtual machines	VNet1, VNet2
VNet1	Windows virtual machines	Hub VNet
VNet2	Linux virtual machines	Hub VNet
VNet3	Windows virtual machine scale sets	VNet4
VNet4	Linux virtual machine scale sets	VNet3

You need to recommend an Azure Bastion deployment to provide secure remote access to all the virtual machines. Based on the virtual network design, how many Azure Bastion subnets are required?

- A. 1
- B. 2
- C. 3
- D. 4
- E. 5

**Answer: C**

**Explanation:**

<https://docs.microsoft.com/en-us/azure/bastion/vnet-peering>

<https://docs.microsoft.com/en-us/learn/modules/connect-vm-with-azure-bastion/2-what-is-azure-bastion>

**NEW QUESTION 69**

- (Exam Topic 3)

You are designing an auditing solution for Azure landing zones that will contain the following components:

- SQL audit logs for Azure SQL databases
- Windows Security logs from Azure virtual machines
- Azure App Service audit logs from App Service web apps

You need to recommend a centralized logging solution for the landing zones. The solution must meet the following requirements:

- Log all privileged access.
- Retain logs for at least 365 days.
- Minimize costs.

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 SQL audit logs: [A Log Analytics workspace, Azure Application Insights, Microsoft Defender for SQL, Microsoft Sentinel]

For the Security logs: [A Log Analytics workspace, Application Insights, Microsoft Defender for servers, Microsoft Sentinel]

For the App Service audit logs: [A Log Analytics workspace, Application Insights, Microsoft Defender for App Service, Microsoft Sentinel]

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

**Answer Area**

For the SQL audit logs: [A Log Analytics workspace, Azure Application Insights, Microsoft Defender for SQL, Microsoft Sentinel]

For the Security logs: [A Log Analytics workspace, Application Insights, Microsoft Defender for servers, Microsoft Sentinel]

For the App Service audit logs: [A Log Analytics workspace, Application Insights, Microsoft Defender for App Service, Microsoft Sentinel]

**NEW QUESTION 70**

- (Exam Topic 3)

You have a Microsoft 365 subscription that syncs with Active Directory Domain Services (AD DS).

You need to define the recovery steps for a ransomware attack that encrypted data in the subscription. The solution must follow Microsoft Security Best Practices.

What is the first step in the recovery plan?

- A. Disable Microsoft OneDrive sync and Exchange ActiveSync.
- B. Recover files to a cleaned computer or device.
- C. Contact law enforcement.
- D. From Microsoft Defender for Endpoint perform a security scan.

**Answer:** A

**NEW QUESTION 71**

- (Exam Topic 3)

You have 50 Azure subscriptions.

You need to monitor resource in the subscriptions for compliance with the ISO 27001:2013 standards. The solution must minimize the effort required to modify the list of monitored policy definitions for the subscriptions.

NOTE: Each correct selection is worth one point.

- A. Assign an initiative to a management group.
- B. Assign a policy to each subscription.
- C. Assign a policy to a management group.
- D. Assign an initiative to each subscription.
- E. Assign a blueprint to each subscription.
- F. Assign a blueprint to a management group.

**Answer:** AF

**Explanation:**

<https://docs.microsoft.com/en-us/azure/governance/management-groups/overview> <https://docs.microsoft.com/en-us/azure/governance/blueprints/overview>

<https://docs.microsoft.com/en-us/azure/governance/policy/samples/iso-27001> <https://docs.microsoft.com/en-us/azure/governance/policy/tutorials/create-and-manage>

#### NEW QUESTION 72

- (Exam Topic 3)

You have the following on-premises servers that run Windows Server:

- Two domain controllers in an Active Directory Domain Services (AD DS) domain
- Two application servers named Server1 and Server2 that run ASP.NET web apps
- A VPN server named Server3 that authenticates by using RADIUS and AD DS. End users use a VPN to access the web apps over the internet.

You need to redesign a user access solution to increase the security of the connections to the web apps. The solution must minimize the attack surface and follow the Zero Trust principles of the Microsoft Cybersecurity Reference Architectures (MCRA).

What should you include in the recommendation?

- A. Configure connectors and rules in Microsoft Defender for Cloud Apps.
- B. Configure web protection in Microsoft Defender for Endpoint.
- C. Publish the web apps by using Azure AD Application Proxy.
- D. Configure the VPN to use Azure AD authentication.

**Answer: C**

#### NEW QUESTION 73

- (Exam Topic 3)

You are planning the security requirements for Azure Cosmos DB Core (SQL) API accounts. You need to recommend a solution to audit all users that access the data in the Azure Cosmos DB accounts. Which two configurations should you include in the recommendation? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. Enable Microsoft Defender for Cosmos DB.
- B. Send the Azure Active Directory (Azure AD) sign-in logs to a Log Analytics workspace.
- C. Disable local authentication for Azure Cosmos DB.
- D. Enable Microsoft Defender for Identity.
- E. Send the Azure Cosmos DB logs to a Log Analytics workspace.

**Answer: BC**

#### Explanation:

<https://docs.microsoft.com/en-us/azure/cosmos-db/audit-control-plane-logs>

#### NEW QUESTION 75

.....

## **Thank You for Trying Our Product**

### **We offer two products:**

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

### **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

**100% Actual & Verified — Instant Download, Please Click**  
**[Order The SC-100 Practice Test Here](#)**