



# Microsoft

## Exam Questions SC-100

Microsoft Cybersecurity Architect

#### NEW QUESTION 1

- (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 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 the VMAccess extension on all virtual machines.

Does this meet the goal?

- A. Yes
- B. No

**Answer:** B

#### Explanation:

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

<https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-network-security#ns-7-simplify>

#### NEW QUESTION 2

- (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 that allow traffic from the Front Door service tags. Does this meet the goal?

- A. Yes
- B. No

**Answer:** A

#### Explanation:

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

#### NEW QUESTION 3

- (Exam Topic 3)

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?

- 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>

#### NEW QUESTION 4

- (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

Deleted backups:

Disabled backups:

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area

Deleted backups:

Disabled backups:

NEW QUESTION 5

- (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

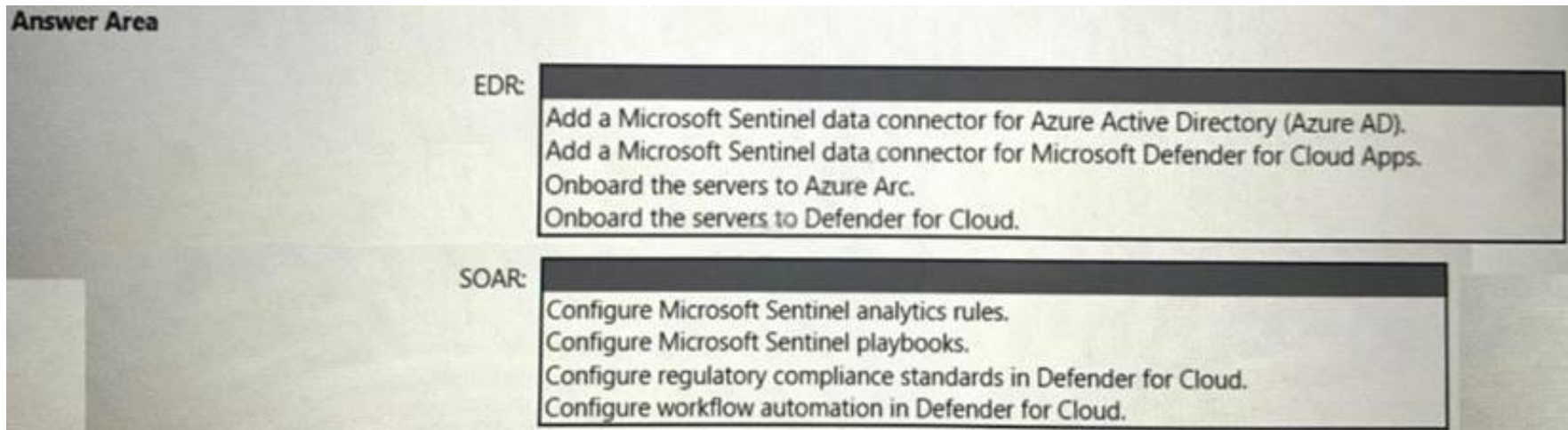
Explanation:

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 6

- (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

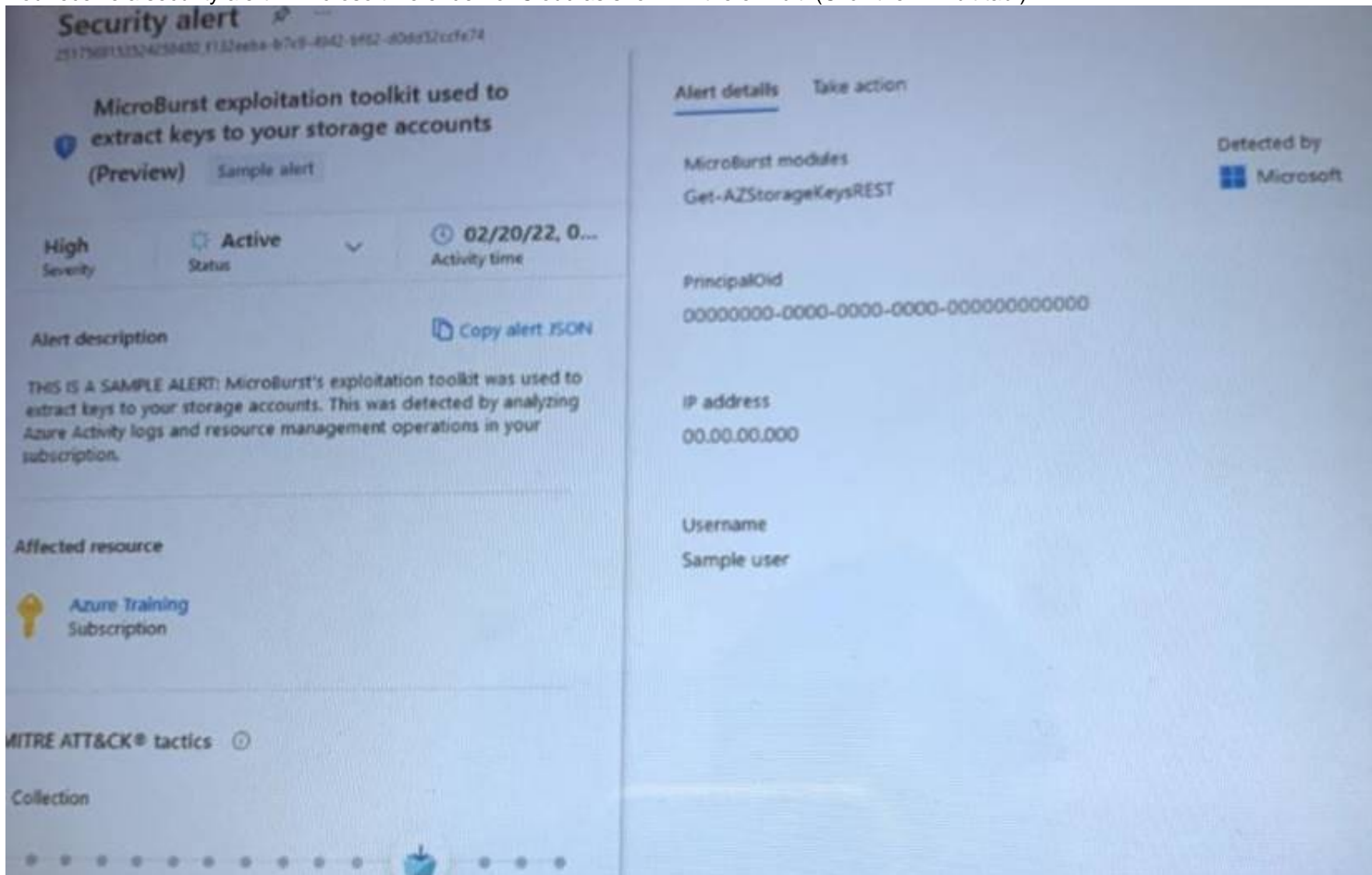
**Explanation:**

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 7**

- (Exam Topic 3)

You receive a security alert in Microsoft Defender for Cloud as shown in the exhibit. (Click the Exhibit tab.)



After remediating the threat which policy definition should you assign to prevent the threat from reoccurring?

- A. Storage account public access should be disallowed
- B. Azure Key Vault Managed HSM should have purge protection enabled
- C. Storage accounts should prevent shared key access
- D. Storage account keys should not be expired

**Answer:** A

**Explanation:**

<https://docs.microsoft.com/en-us/azure/storage/blobs/anonymous-read-access-prevent>

**NEW QUESTION 8**

- (Exam Topic 3)

You are designing a ransomware response plan that follows Microsoft Security Best Practices.

You need to recommend a solution to minimize the risk of a ransomware attack encrypting local user files. What should you include in the recommendation?

- A. Microsoft Defender for Endpoint
- B. Windows Defender Device Guard



- C. protected folders
- D. Azure Files
- E. BitLocker Drive Encryption (BitLocker)

**Answer:** E

#### NEW QUESTION 9

- (Exam Topic 3)

Your company is preparing for cloud adoption.

You are designing security for Azure landing zones.

Which two preventative controls can you implement to increase the secure score? Each NOTE: Each correct selection is worth one point.

- A. Azure Firewall
- B. Azure Web Application Firewall (WAF)
- C. Microsoft Defender for Cloud alerts
- D. Azure Active Directory (Azure AD Privileged Identity Management (PIM)
- E. Microsoft Sentinel

**Answer:** AB

#### Explanation:

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

#### NEW QUESTION 10

- (Exam Topic 3)

You have a Microsoft 365 tenant. Your company uses a third-party software as a service (SaaS) app named App1. App1 supports authenticating users by using Azure AD credentials. You need to recommend a solution to enable users to authenticate to App1 by using their Azure AD credentials. What should you include in the recommendation?

- A. an Azure AD enterprise application
- B. a retying party trust in Active Directory Federation Services (AD FS)
- C. Azure AD Application Proxy
- D. Azure AD B2C

**Answer:** A

#### NEW QUESTION 10

- (Exam Topic 3)

Your company has an on-premises network and an Azure subscription.

The company does NOT have a Site-to-Site VPN or an ExpressRoute connection to Azure.

You are designing the security standards for Azure App Service web apps. The web apps will access Microsoft SQL Server databases on the network.

You need to recommend security standards that will allow the web apps to access the databases. The solution must minimize the number of open internet-accessible endpoints to the on-premises network.

What should you include in the recommendation?

- A. a private endpoint
- B. hybrid connections
- C. virtual network NAT gateway integration
- D. virtual network integration

**Answer:** B

#### Explanation:

<https://docs.microsoft.com/en-us/azure/app-service/app-service-hybrid-connections>

#### NEW QUESTION 12

- (Exam Topic 3)

You have an Azure subscription that is used as an Azure landing zone for an application. You need to evaluate the security posture of all the workloads in the landing zone. What should you do first?

- A. Add Microsoft Sentinel data connectors.
- B. Configure Continuous Integration/Continuous Deployment (CI/CD) vulnerability scanning.
- C. Enable the Defender plan for all resource types in Microsoft Defender for Cloud.
- D. Obtain Azure Active Directory Premium Plan 2 licenses.

**Answer:** A

#### NEW QUESTION 15

- (Exam Topic 3)

You are designing a ransomware response plan that follows Microsoft Security Best Practices

You need to recommend a solution to limit the scope of damage of ransomware attacks without being locked out.

What should you include in the recommendations?

- A. Privileged Access Workstations (PAWs)
- B. emergency access accounts
- C. device compliance policies
- D. Customer Lockbox for Microsoft Azure

Answer: B

#### NEW QUESTION 20

- (Exam Topic 3)

You are planning the security levels for a security access strategy.

You need to identify which job roles to configure at which security levels. The solution must meet security best practices of the Microsoft Cybersecurity Reference Architectures (MCRA).

Which security level should you configure for each job role? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Answer Area



Job Role	Selected Security Level
Developer	Specialized security
Standard user	Enterprise security
IT administrator	Privileged security

A. Mastered

B. Not Mastered

Answer: A

Explanation:

Answer Area



Job Role	Selected Security Level
Developer	Specialized security
Standard user	Enterprise security
IT administrator	Privileged security

#### NEW QUESTION 22

- (Exam Topic 3)

You have a Microsoft 365 E5 subscription and an Azure subscription. You are designing a Microsoft Sentinel deployment.

You need to recommend a solution for the security operations team. The solution must include custom views and a dashboard for analyzing security events. What should you recommend using in Microsoft Sentinel?

A. playbooks

B. workbooks

C. notebooks

D. threat intelligence

Answer: B

Explanation:

<https://docs.microsoft.com/en-us/azure/azure-monitor/visualize/workbooks-overview>

#### NEW QUESTION 25

- (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 28**

- (Exam Topic 3)

You have a Microsoft 365 E5 subscription.

You are designing a solution to protect confidential data in Microsoft SharePoint Online sites that contain more than one million documents.

You need to recommend a solution to prevent Personally Identifiable Information (PII) from being shared.

Which two components should you include in the recommendation? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

- A. data loss prevention (DLP) policies
- B. sensitivity label policies
- C. retention label policies
- D. eDiscovery cases

**Answer:** AB

**Explanation:**

Data loss prevention in Office 365. Data loss prevention (DLP) helps you protect sensitive information and prevent its inadvertent disclosure. Examples of sensitive information that you might want to prevent from leaking outside your organization include financial data or personally identifiable information (PII) such as credit card numbers, social security numbers, or health records. With a data loss prevention (DLP) policy, you can identify, monitor, and automatically protect sensitive information across Office 365.

Sensitivity labels from Microsoft Purview Information Protection let you classify and protect your organization's data without hindering the productivity of users and their ability to collaborate. Plan for integration into a broader information protection scheme. On top of coexistence with OME, sensitivity labels can be used alongside capabilities like Microsoft Purview Data Loss Prevention (DLP) and Microsoft Defender for Cloud Apps.

<https://motionwave.com.au/keeping-your-confidential-data-secure-with-microsoft-office-365/> <https://docs.microsoft.com/en-us/microsoft-365/solutions/information-protection-deploy-protect-information?vie>

**NEW QUESTION 33**

- (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 38**

- (Exam Topic 3)

You have a Microsoft 365 subscription.

You are designing a user access solution that follows the Zero Trust principles of the Microsoft Cybersecurity Reference Architectures (MCRA).

You need to recommend a solution that automatically restricts access to Microsoft Exchange Online, SharePoint Online, and Teams in near-real-time (NRT) in response to the following Azure AD events:

- A user account is disabled or deleted
- The password of a user is changed or reset.
- All the refresh tokens for a user are revoked
- Multi-factor authentication (MFA) is enabled for a user

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

- A. continuous access evaluation
- B. a sign-in risk policy
- C. Azure AD Privileged Identity Management (PIM)
- D. Conditional Access
- E. Azure AD Application Proxy

**Answer:** AD

**NEW QUESTION 42**

- (Exam Topic 3)

You have Windows 11 devices and Microsoft 365 E5 licenses.

You need to recommend a solution to prevent users from accessing websites that contain adult content such as gambling sites. What should you include in the recommendation?

- A. Microsoft Endpoint Manager
- B. Compliance Manager
- C. Microsoft Defender for Cloud Apps
- D. Microsoft Defender for Endpoint

**Answer:** D

**Explanation:**

<https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/web-content-filtering?view=o365-w>

#### NEW QUESTION 47

- (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 49

- (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 Azure security baseline for audit report.
- B. From Defender for Cloud, review the secure score recommendations.
- C. From Azure Policy, assign a built-in initiative that has a scope of the subscription.
- D. From Defender for Cloud, enable Defender for Cloud plans.

**Answer:** C

**Explanation:**

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

#### NEW QUESTION 51

- (Exam Topic 2)

You need to recommend a multi-tenant and hybrid security solution that meets to the business requirements and the hybrid 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 centralize subscription management:

- Azure AD B2B
- Azure AD B2C
- Azure Lighthouse

To enable the management of on-premises resources:

- Azure Arc
- Azure Stack Edge
- Azure Stack Hub

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**



**Answer Area**

To centralize subscription management:

- Azure AD B2B
- Azure AD B2C**
- Azure Lighthouse

To enable the management of on-premises resources:

- Azure Arc**
- Azure Stack Edge
- Azure Stack Hub

#### NEW QUESTION 54

- (Exam Topic 3)

Your company has a Microsoft 365 E5 subscription.

The company plans to deploy 45 mobile self-service kiosks that will run Windows 10. You need to provide recommendations to secure the kiosks. The solution must meet the following requirements:

- Ensure that only authorized applications can run on the kiosks.
- Regularly harden the kiosks against new threats.

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

- A. Onboard the kiosks to Azure Monitor.
- B. Implement Privileged Access Workstation (PAW) for the kiosks.
- C. Implement Automated Investigation and Remediation (AIR) in Microsoft Defender for Endpoint.
- D. Implement threat and vulnerability management in Microsoft Defender for Endpoint.
- E. Onboard the kiosks to Microsoft Intune and Microsoft Defender for Endpoint.

**Answer:** DE

#### Explanation:

(<https://docs.microsoft.com/en-us/microsoft-365/security/defender-vulnerability-management/defender-vulnerab>)

#### NEW QUESTION 57

- (Exam Topic 2)

You need to recommend a solution to evaluate regulatory compliance across the entire managed environment. The solution must meet the regulatory compliance requirements and the business 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**

Evaluate regulatory compliance of cloud resources by assigning:

- Azure Policy definitions to management groups
- Azure Policy initiatives to management groups**
- Azure Policy initiatives to subscriptions

Evaluate regulatory compliance of on-premises resources by using:

- Azure Arc**
- Group Policy
- PowerShell Desired State Configuration (DSC)

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

**Answer Area**

Evaluate regulatory compliance of cloud resources by assigning:

- Azure Policy definitions to management groups
- Azure Policy initiatives to management groups**
- Azure Policy initiatives to subscriptions

Evaluate regulatory compliance of on-premises resources by using:

- Azure Arc**
- Group Policy
- PowerShell Desired State Configuration (DSC)

#### NEW QUESTION 59

- (Exam Topic 2)

You need to recommend a solution for securing the landing zones. The solution must meet the landing zone requirements and the business requirements.

What should you configure for each landing zone?

- A. Azure DDoS Protection Standard
- B. an Azure Private DNS zone
- C. Microsoft Defender for Cloud
- D. an ExpressRoute gateway

Answer: D

Explanation:

One of the stipulations is to meet the business requirements of minimizing costs. ExpressRoute is expensive. Given the landing zone requirements of

- 1) "Use a DNS namespace of litware.com"
- 2) "Ensure that the Azure virtual machines in each landing zone communicate with Azure App Service web apps in the same zone over the Microsoft backbone network, rather than over public endpoints"

NEW QUESTION 60

- (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

Segment Microsoft Sentinel workspaces by:

Azure AD tenant

Enterprise

Region and Azure AD tenant

Integrate Azure subscriptions by using:

Self-service sign-up user flows for Azure AD B2B

Self-service sign-up user flows for Azure AD B2C

The Azure Lighthouse subscription onboarding process

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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

NEW QUESTION 62

- (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

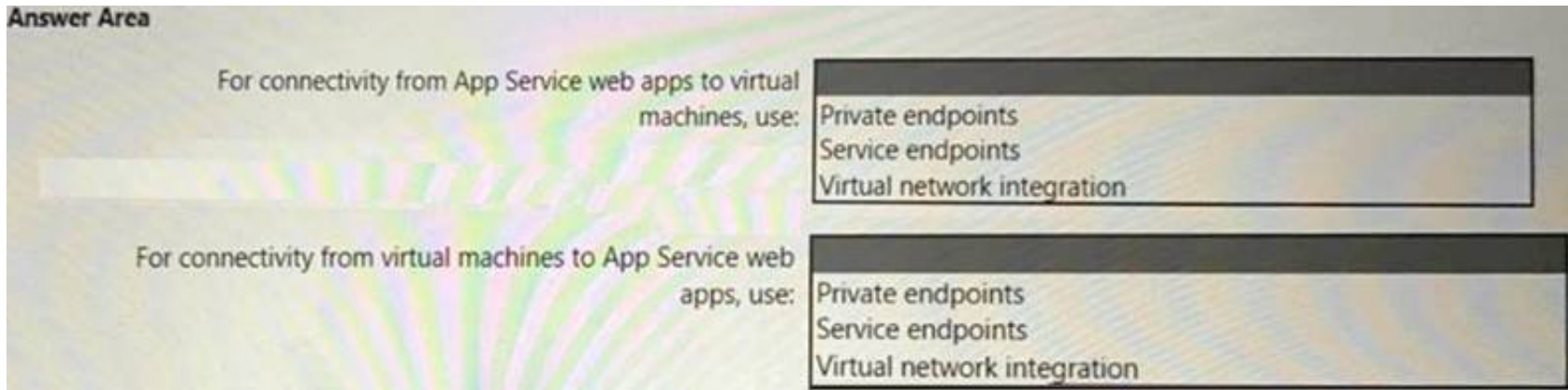
Enable Security defaults in the Azure AD tenant of Litware

Replace pass-through authentication with Active Directory Federation Services

NEW QUESTION 65

- (Exam Topic 2)

You need to recommend a strategy for App Service web app connectivity. The solution must meet the landing zone requirements. What should you recommend? 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:

Box 1: Virtual Network Integration - correct

Virtual network integration gives your app access to resources in your virtual network, but it doesn't grant inbound private access to your app from the virtual network.

Box 2: Private Endpoints. - correct

You can use Private Endpoint for your Azure Web App to allow clients located in your private network to securely access the app over Private Link.

NEW QUESTION 67

- (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 70

- (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.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:





### NEW QUESTION 73

- (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:** D

**Explanation:**

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

### NEW QUESTION 78

- (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 80

- (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 lockout in Azure AD B2C

**Answer:** AC

**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 84

- (Exam Topic 3)

You are creating an application lifecycle management process based on the Microsoft Security Development Lifecycle (SDL).

You need to recommend a security standard for onboarding applications to Azure. The standard will include recommendations for application design, development, and deployment

What should you include during the application design phase?

- A. static application security testing (SAST) by using SonarQube
- B. dynamic application security testing (DAST) by using Veracode
- C. threat modeling by using the Microsoft Threat Modeling Tool



D. software decomposition by using Microsoft Visual Studio Enterprise

**Answer:** C

**Explanation:**

<https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling>

#### NEW QUESTION 85

- (Exam Topic 3)

Your company has an on-premises network, an Azure subscription, and a Microsoft 365 E5 subscription. The company uses the following devices:

- Computers that run either Windows 10 or Windows 11
- Tablets and phones that run either Android or iOS

You need to recommend a solution to classify and encrypt sensitive Microsoft Office 365 data regardless of where the data is stored. What should you include in the recommendation?

- A. eDiscovery
- B. retention policies
- C. Compliance Manager
- D. Microsoft Information Protection

**Answer:** D

**Explanation:**

<https://docs.microsoft.com/en-us/microsoft-365/compliance/information-protection> <https://docs.microsoft.com/en-us/microsoft-365/compliance/ediscovery?view=o365-worldwide>

#### NEW QUESTION 89

- (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

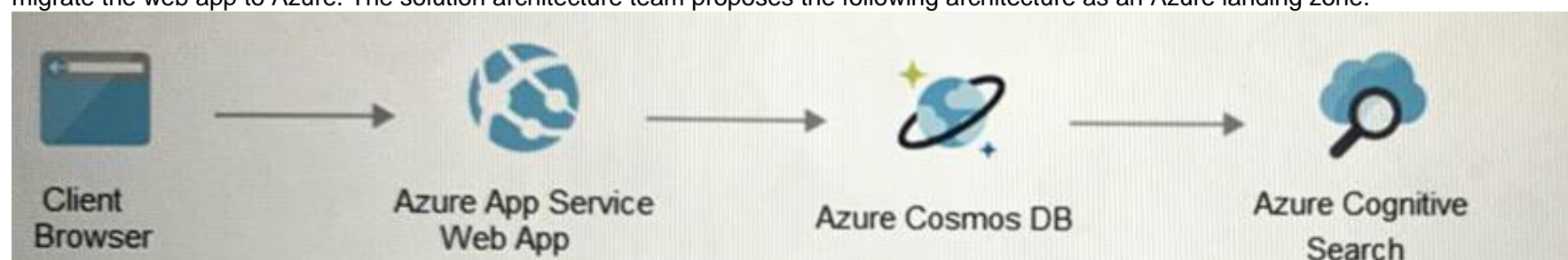
**Explanation:**

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

#### NEW QUESTION 91

- (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 Application Gateway with Azure Web Application Firewall (WAF).

Does this meet the goal?

- 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 93

- (Exam Topic 3)

You have a Microsoft 365 tenant.

Your company uses a third-party software as a service (SaaS) app named App1 that is integrated with an Azure AD tenant. You need to design a security strategy to meet the following requirements:

- Users must be able to request access to App1 by using a self-service request.
- When users request access to App1, they must be prompted to provide additional information about their request.
- Every three months, managers must verify that the users still require access to App1. What should you include in the design?

- A. Azure AD Application Proxy
- B. connected apps in Microsoft Defender for Cloud Apps
- C. Microsoft Entra Identity Governance
- D. access policies in Microsoft Defender for Cloud Apps

**Answer:** C

#### NEW QUESTION 94

- (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 96

- (Exam Topic 3)

Your company wants to optimize using Microsoft Defender for Endpoint to protect its resources against ransomware based on Microsoft Security Best Practices.

You need to prepare a post-breach response plan for compromised computers based on the Microsoft Detection and Response Team (DART) approach in Microsoft Security Best Practices.

What should you include in the response plan?

- A. controlled folder access
- B. application isolation
- C. memory scanning
- D. machine isolation
- E. user isolation

**Answer:** D

#### NEW QUESTION 97

- (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:	<div><div>Microsoft Defender for Office 365</div><div>Azure AD Identity Protection</div><div>Microsoft Defender for DNS</div><div>Microsoft Defender for Office 365</div><div>Microsoft Purview</div></div>
Policy type:	<div><div>Anti-phishing</div><div>Anti-phishing</div><div>Anti-spam</div><div>Data loss prevention (DLP)</div><div>Insider risk management</div></div>

- A. Mastered
- B. Not Mastered

**Answer:** A

#### Explanation:

## Answer Area

Service:

Policy type:

### NEW QUESTION 100

- (Exam Topic 3)

You design cloud-based software as a service (SaaS) solutions.

You need to recommend ransomware attacks. The solution must follow Microsoft Security Best Practices. What should you recommend doing first?

- A. Implement data protection.
- B. Develop a privileged access strategy.
- C. Prepare a recovery plan.
- D. Develop a privileged identity strategy.

Answer: C

### NEW QUESTION 102

- (Exam Topic 3)

You have a Microsoft 365 subscription that is protected by using Microsoft 365 Defender

You are designing a security operations strategy that will use Microsoft Sentinel to monitor events from Microsoft 365 and Microsoft 365 Defender

You need to recommend a solution to meet the following requirements:

- Integrate Microsoft Sentinel with a third-party security vendor to access information about known malware
- Automatically generate incidents when the IP address of a command-and-control server is detected in the events

What should you configure in Microsoft Sentinel to meet each requirement? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

## Answer Area

Integrate Microsoft Sentinel with a third-party security vendor:

Automatically generate incidents:

- A. Mastered
- B. Not Mastered

Answer: A

### Explanation:

## Answer Area

Integrate Microsoft Sentinel with a third-party security vendor:

Automatically generate incidents:

### NEW QUESTION 106

- (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 f 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

Manage NSG rules by using:

Just-in-time (JIT) VM access  
 Azure Automation  
 Azure Bastion  
 Just-in-time (JIT) VM access

Only allow SSH connections to the jump servers from:

Any public IP addresses provided before the connection is established  
 Any public IP addresses provided before the connection is established  
 AzureBastionSubnet  
 GatewaySubnet

- A. Mastered  
 B. Not Mastered

Answer: A

Explanation:

Answer Area

Manage NSG rules by using:

Just-in-time (JIT) VM access  
 Azure Automation  
 Azure Bastion  
 Just-in-time (JIT) VM access

Only allow SSH connections to the jump servers from:

Any public IP addresses provided before the connection is established  
 Any public IP addresses provided before the connection is established  
 AzureBastionSubnet  
 GatewaySubnet

### NEW QUESTION 107

- (Exam Topic 3)

Your company has a hybrid cloud infrastructure that contains an on-premises Active Directory Domain Services (AD DS) forest, a Microsoft B65 subscription, and an Azure subscription.

The company's on-premises network contains internal web apps that use Kerberos authentication. Currently, the web apps are accessible only from the network.

You have remote users who have personal devices that run Windows 11.

You need to recommend a solution to provide the remote users with the ability to access the web apps. The solution must meet the following requirements:

- Prevent the remote users from accessing any other resources on the network.
- Support Azure Active Directory (Azure AD) Conditional Access.
- Simplify the end-user experience.

What should you include in the recommendation?

- A. Azure AD Application Proxy  
 B. Azure Virtual WAN  
 C. Microsoft Tunnel  
 D. web content filtering in Microsoft Defender for Endpoint

Answer: A

Explanation:

<https://docs.microsoft.com/en-us/learn/modules/configure-azure-ad-application-proxy/2-explore>

### NEW QUESTION 111

- (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 112

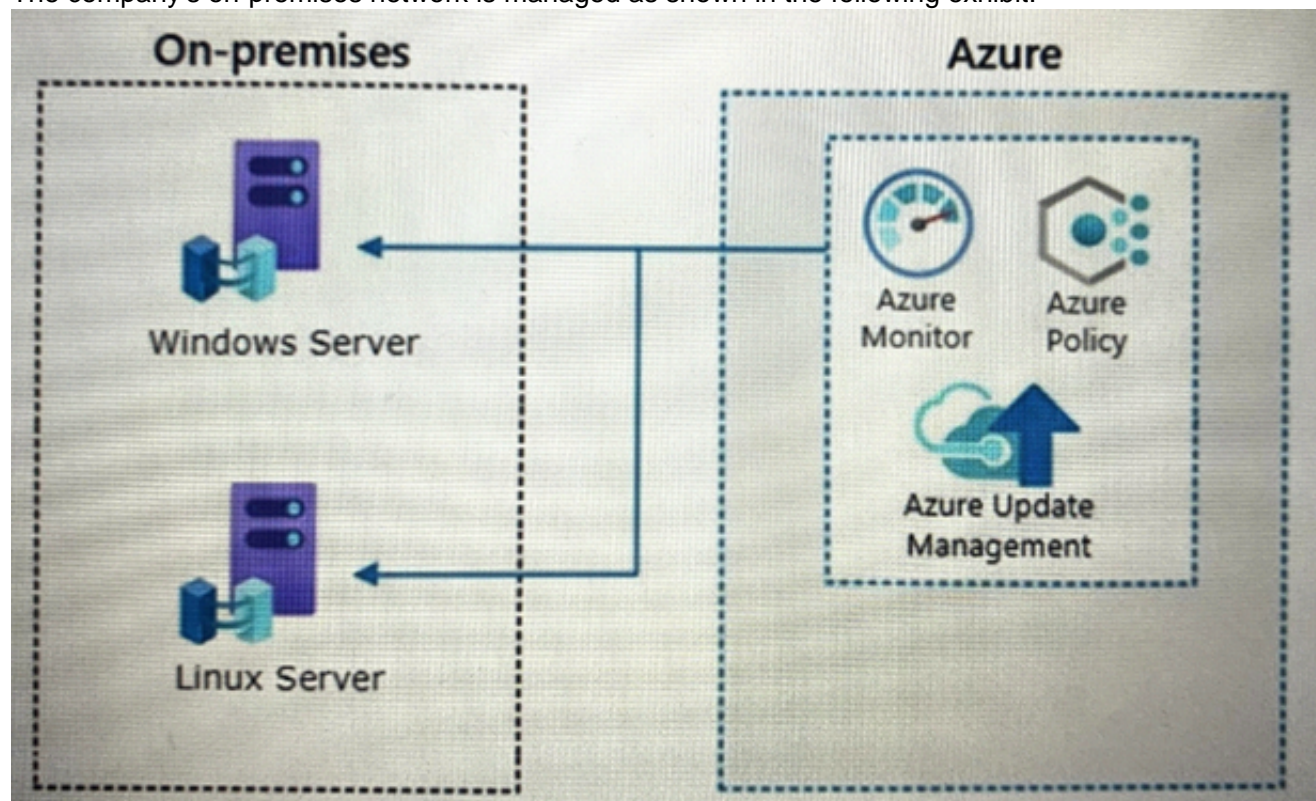
- (Exam Topic 3)

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 117

- (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's 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 119

- (Exam Topic 3)

You have an Active Directory Domain Services (AD DS) domain that contains a virtual desktop infrastructure (VDI). The VDI uses non-persistent images and cloned virtual machine templates. VDI devices are members of the domain.

You have an Azure subscription that contains an Azure Virtual Desktop environment. The environment contains host pools that use a custom golden image. All the Azure Virtual Desktop deployments are members of a single Azure Active Directory Domain Services (Azure AD DS) domain.

You need to recommend a solution to deploy Microsoft Defender for Endpoint to the hosts. The solution must meet the following requirements:

- Ensure that the hosts are onboarded to Defender for Endpoint during the first startup sequence.
- Ensure that the Microsoft Defender 365 portal contains a single entry for each deployed VDI host.
- Minimize administrative effort.

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 VDI:

- Add the Defender for Endpoint onboarding script to the virtual machine template.
- Deploy Defender for Endpoint by using a custom Group Policy Object (GPO).
- Onboard the virtual machine template to Defender for Endpoint.**

For Azure Virtual Desktop:

- Add the Defender for Endpoint onboarding script to the golden image.
- Deploy Defender for Endpoint by using a custom Group Policy Object (GPO).
- Onboard the golden image to Defender for Endpoint.**

- A. Mastered
- B. Not Mastered

**Answer:** A

**Explanation:**

Answer Area

For the VDI:

- Add the Defender for Endpoint onboarding script to the virtual machine template.
- Deploy Defender for Endpoint by using a custom Group Policy Object (GPO).
- Onboard the virtual machine template to Defender for Endpoint.**

For Azure Virtual Desktop:

- Add the Defender for Endpoint onboarding script to the golden image.
- Deploy Defender for Endpoint by using a custom Group Policy Object (GPO).
- Onboard the golden image to Defender for Endpoint.**

#### NEW QUESTION 121

- (Exam Topic 3)

For of an Azure deployment you are designing a security architecture based on the Microsoft Cloud Security Benchmark. You need to recommend a best practice for implementing service accounts for Azure API management What should you include in the recommendation?

- A. device registrations in Azure AD
- B. application registrations m Azure AD
- C. Azure service principals with certificate credentials
- D. Azure service principals with usernames and passwords
- E. managed identities in Azure

**Answer:** E

#### NEW QUESTION 124

- (Exam Topic 3)

You have an Azure AD tenant that syncs with an Active Directory Domain Services (AD DS) domain. Client computers run Windows and are hybrid-joined to Azure AD.

You are designing a strategy to protect endpoints against ransomware. The strategy follows Microsoft Security Best Practices.

You plan to remove all the domain accounts from the Administrators group on the Windows computers. You need to recommend a solution that will provide users with administrative access to the Windows computers only when access is required. The solution must minimize the lateral movement of ransomware attacks if an administrator account on a computer is compromised.

What should you include in the recommendation?

- A. Local Administrator Password Solution (LAPS)
- B. Privileged Access Workstations (PAWs)
- C. Azure AD Privileged Identity Management (PIM)
- D. Azure AD identity Protection

**Answer:** A

#### NEW QUESTION 128

- (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 129

- (Exam Topic 3)

Your company has an Azure App Service plan that is used to deploy containerized web apps. You are designing a secure DevOps strategy for deploying the web apps to the App Service plan. You need to recommend a strategy to integrate code scanning tools into a secure software development lifecycle. The code must be scanned during the following two phases:

Uploading the code to repositories Building containers

Where should you integrate code scanning for each phase? To answer, select the appropriate options in the answer area.

**Answer Area**

Uploading code to repositories:

- ☐ Azure Boards
- ☐ Azure Pipelines
- ☐ GitHub Enterprise
- ☐ Microsoft Defender for Cloud

Building containers:

- ☐ Azure Boards
- ☐ Azure Pipelines
- ☐ GitHub Enterprise
- ☐ Microsoft Defender for Cloud

- A. Mastered
- B. Not Mastered

**Answer: A**

#### Explanation:

<https://docs.github.com/en/enterprise-cloud@latest/get-started/learning-about-github/about-github-advanced-sec> <https://microsoft.github.io/code-with-engineering-playbook/automated-testing/tech-specific-samples/azdo-conta>

#### NEW QUESTION 133

- (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 134

- (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 135

- (Exam Topic 3)

Your company is migrating data to Azure. The data contains Personally Identifiable Information (PII). The

company plans to use Microsoft Information Protection for the PII data store in Azure. You need to recommend a solution to discover PII data at risk in the Azure resources.

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.

To connect the Azure data sources to  
 Microsoft Information Protection:

Azure Purview

Endpoint data loss prevention

Microsoft Defender for Cloud Apps

Microsoft Information Protection

To triage security alerts related to  
 resources that contain PII data:

Azure Monitor

Endpoint data loss prevention

Microsoft Defender for Cloud

Microsoft Defender for Cloud Apps

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface, text, application Description automatically generated  
 Prioritize security actions by data sensitivity,  
<https://docs.microsoft.com/en-us/azure/defender-for-cloud/information-protection>. As to Azure SQL Database Azure SQL Managed Instance Azure Synapse Analytics (Azure resources as well): <https://docs.microsoft.com/en-us/azure/azure-sql/database/data-discovery-and-classification-overview?view=azu>

NEW QUESTION 140

- (Exam Topic 3)  
 You are designing a security operations strategy based on the Zero Trust framework.  
 You need to increase the operational efficiency of the Microsoft Security Operations Center (SOC).  
 Based on the Zero Trust framework, which three deployment objectives should you prioritize in sequence? To answer, move the appropriate objectives from the list of objectives to the answer area and arrange them in the correct order.

Actions

Establish ransomware recovery readiness.

Implement disaster recovery.

Establish visibility.

Enable additional protection and detection controls.

Enable automation.

Answer Area

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Actions

Establish ransomware recovery readiness.

Implement disaster recovery.

Establish visibility.

Enable additional protection and detection controls.

Enable automation.

Answer Area

Establish visibility.

Enable additional protection and detection controls.

Enable automation.

NEW QUESTION 145

- (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 149**

- (Exam Topic 3)

You have an Azure subscription that contains a Microsoft Sentinel workspace.

Your on-premises network contains firewalls that support forwarding event logs in the Common Event Format (CEF). There is no built-in Microsoft Sentinel connector for the firewalls.

You need to recommend a solution to ingest events from the firewalls into Microsoft Sentinel. What should you include in the recommendation?

- A. an Azure logic app
- B. an on-premises Syslog server
- C. an on-premises data gateway
- D. Azure Data Factory

**Answer: B**

**NEW QUESTION 151**

- (Exam Topic 3)

You plan to automate the development and deployment of a Node.js-based app by using GitHub. You need to recommend a DevSecOps solution for the app. The solution must meet the following requirements:

- Automate the generation of pull requests that remediate identified vulnerabilities.
- Automate vulnerability code scanning for public and private repositories.
- Minimize administrative effort.
- Minimize costs.

What should you recommend using? 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:**

A close up of a text Description automatically generated

**NEW QUESTION 153**

- (Exam Topic 3)

Your company plans to deploy several Azure App Service web apps. The web apps will be deployed to the West Europe Azure region. The web apps will be accessed only by customers in Europe and the United States.

You need to recommend a solution to prevent malicious bots from scanning the web apps for vulnerabilities. The solution must minimize the attack surface. What should you include in the recommendation?

- A. Azure Firewall Premium
- B. Azure Application Gateway Web Application Firewall (WAF)
- C. network security groups (NSGs)
- D. Azure Traffic Manager and application security groups

**Answer: D**

**Explanation:**

<https://docs.microsoft.com/en-us/azure/web-application-firewall/ag/bot-protection>

**NEW QUESTION 154**

- (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 159

.....

## 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](#)**