



Microsoft

Exam Questions SC-100

Microsoft Cybersecurity Architect

About ExamBible

Your Partner of IT Exam

Found in 1998

ExamBible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, ExamBible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

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 new Azure environment based on the security best practices of the Microsoft Cloud Adoption Framework for Azure. The environment will contain one subscription for shared infrastructure components and three separate subscriptions for applications.

You need to recommend a deployment solution that includes network security groups (NSGs) Azure Key Vault, and Azure Bastion. The solution must minimize deployment effort and follow security best practices of the Microsoft Cloud Adoption Framework for Azure. What should you include in the recommendation?

- A. the Azure landing zone accelerator
- B. the Azure Well-Architected Framework
- C. Azure Security Benchmark v3
- D. Azure Advisor

Answer: A

NEW QUESTION 3

- (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 adaptive network hardening.

Does this meet the goal?

- A. Yes
- B. No

Answer: A

Explanation:

JIT:
<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 4

- (Exam Topic 3)

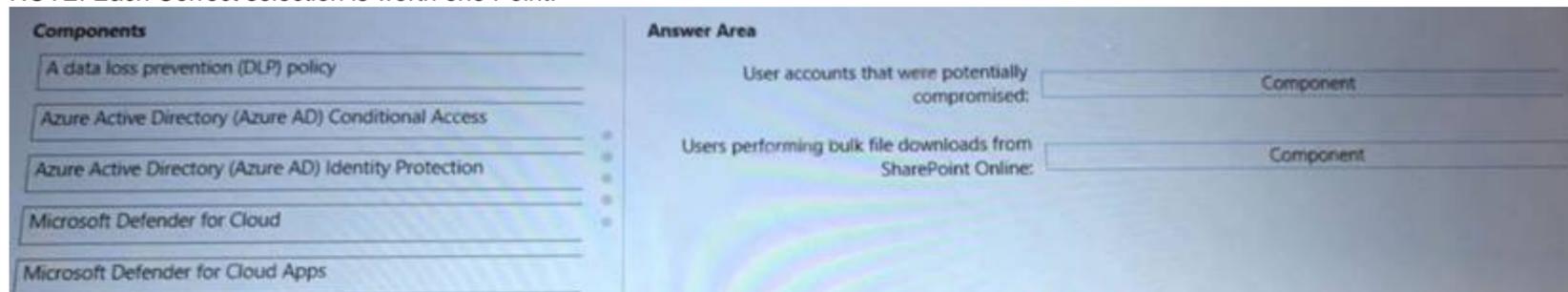
You have a Microsoft 365 subscription

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.



- 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 5

- (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

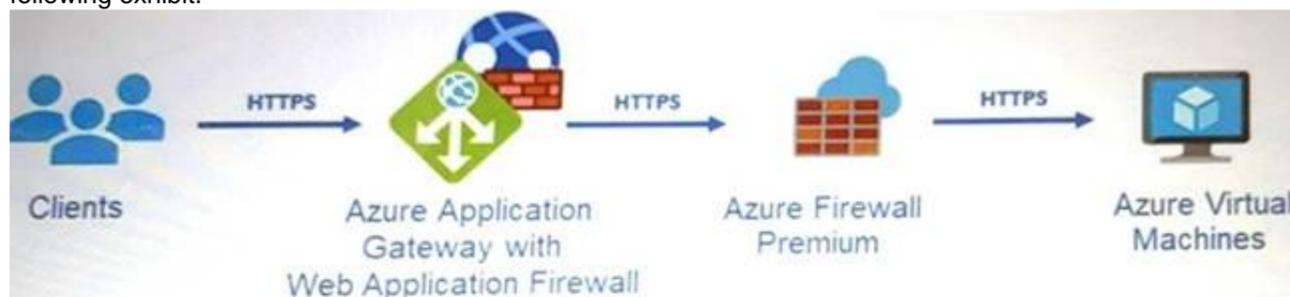
Explanation:

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

NEW QUESTION 6

- (Exam Topic 3)

Your company uses Microsoft Defender for Cloud and Microsoft Sentinel. The company is designing an application that will have the architecture shown in the following exhibit.



You are designing a logging and auditing solution for the proposed architecture. The solution must meet the following requirements-

- Integrate Azure Web Application Firewall (WAF) logs with Microsoft Sentinel.
- Use Defender for Cloud to review alerts from the virtual machines.

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

For WAF:	<input type="checkbox"/> The Azure Diagnostics extension <input type="checkbox"/> Azure Network Watcher <input type="checkbox"/> Data connectors <input type="checkbox"/> Workflow automation
For the virtual machines:	<input type="checkbox"/> The Azure Diagnostics extension <input type="checkbox"/> Azure Storage Analytics <input type="checkbox"/> Data connectors <input type="checkbox"/> The Log Analytics agent <input type="checkbox"/> Workflow automation

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Graphical user interface Description automatically generated

NEW QUESTION 7

- (Exam Topic 3)

You have an operational model based on the Microsoft Cloud Adoption framework for Azure.

You need to recommend a solution that focuses on cloud-centric control areas to protect resources such as endpoints, database, files, and storage accounts.

What should you include in the recommendation?

- A. security baselines in the Microsoft Cloud Security Benchmark
- B. modern access control
- C. business resilience
- D. network isolation

Answer: A

NEW QUESTION 8

- (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 9

- (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: D

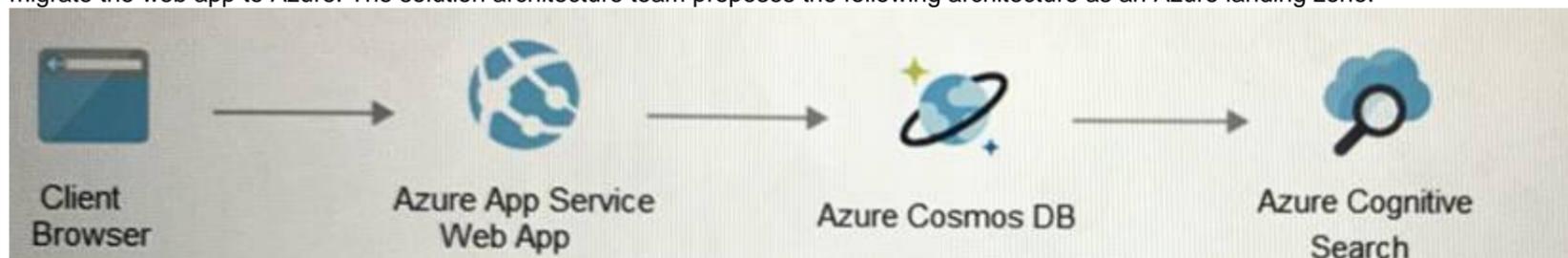
Explanation:

(<https://docs.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure>) <https://www.microsoft.com/en-us/security/business/identity-access/azure-active-directory-pricing?rtc=1>

NEW QUESTION 10

- (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

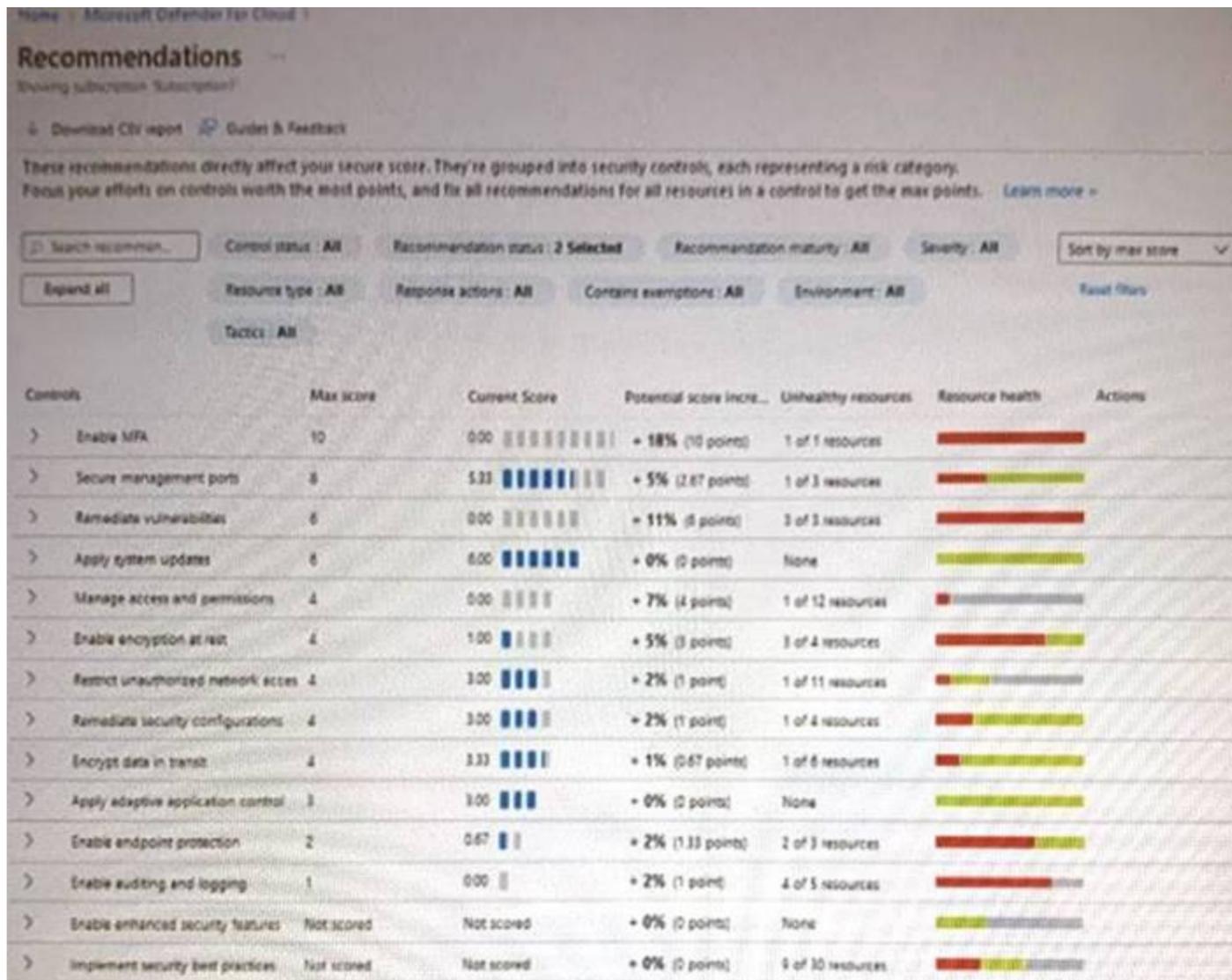
Explanation:

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 10

- (Exam Topic 3)

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



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

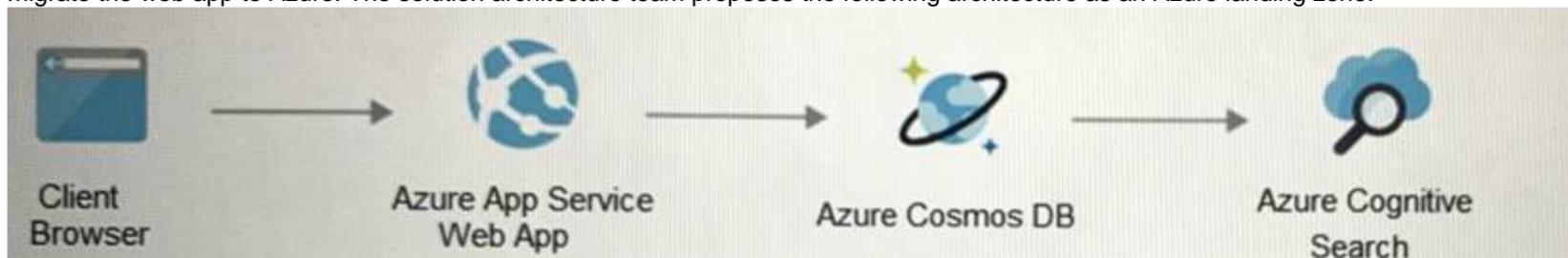
Explanation:

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 12

- (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 Front Door with Azure Web Application Firewall (WAF). Does this meet the goal?

- A. Yes
- B. No

Answer: B

Explanation:

<https://www.varonis.com/blog/securing-access-azure-webapps>

NEW QUESTION 17

- (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: AC

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 22

- (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 23

- (Exam Topic 3)

You have a customer that has a Microsoft 365 subscription and an Azure subscription. The customer has devices that run either Windows, iOS, Android, or macOS. The Windows devices are deployed on-premises and in Azure. You need to design a security solution to assess whether all the devices meet the customer's compliance rules. What should you include in the solution?

- A. Microsoft Information Protection
- B. Microsoft Defender for Endpoint
- C. Microsoft Sentinel
- D. Microsoft Endpoint Manager

Answer: D

Explanation:

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

NEW QUESTION 27

- (Exam Topic 3)

You are designing the security architecture for a cloud-only environment. You are reviewing the integration point between Microsoft 365 Defender and other Microsoft cloud services based on Microsoft Cybersecurity Reference Architectures (MCRA).

You need to recommend which Microsoft cloud services integrate directly with Microsoft 365 Defender and meet the following requirements:

- Enforce data loss prevention (DLP) policies that can be managed directly from the Microsoft 365 Defender portal.
- Detect and respond to security threats based on User and Entity Behavior Analytics (UEBA) with unified alerting.

What should you include in the recommendation for each requirement? 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 30

- (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 32

- (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



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 37

- (Exam Topic 3)

You have an Azure AD tenant that syncs with an Active Directory Domain Services (AD DS) domain. You have an on-premises datacenter that contains 100 servers. The servers run Windows Server and are backed up by using Microsoft Azure Backup Server (MABS).

You are designing a recovery solution for ransomware attacks. The solution follows Microsoft Security Best Practices.

You need to ensure that a compromised administrator account cannot be used to delete the backups. What should you do?

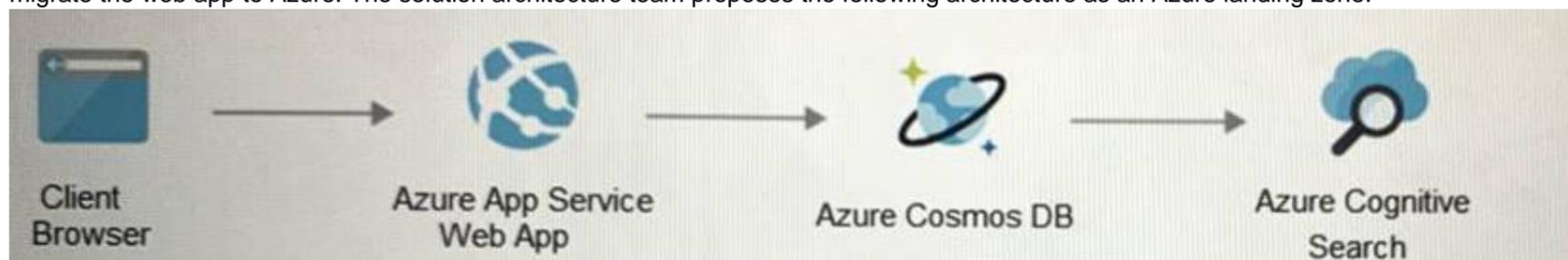
- A. From a Recovery Services vault generate a security PIN for critical operations.
- B. From Azure Backup, configure multi-user authorization by using Resource Guard.
- C. From Microsoft Azure Backup Setup, register MABS with a Recovery Services vault.
- D. From Azure AD Privileged Identity Management (PIM), create a role assignment for the Backup Contributor role.

Answer: B

NEW QUESTION 38

- (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 creating private endpoints for the web app and the database layer. Does this meet the goal?

- A. Yes
- B. No

Answer: A

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.

<https://docs.microsoft.com/en-us/azure/cosmos-db/how-to-configure-private-endpoints>

NEW QUESTION 42

- (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 45

- (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 46

- (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 47

- (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 52

- (Exam Topic 3)

You have a multi-cloud environment that contains an Azure subscription and an Amazon Web Services (AWS) account.

You need to implement security services in Azure to manage the resources in both subscriptions. The solution must meet the following requirements:

- Automatically identify threats found in AWS CloudTrail events.
- Enforce security settings on AWS virtual machines by using Azure policies.

What should you include in the solution for each requirement? 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 54

- (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 55

- (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 57

- (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.

Scopes

Files and emails

Groups and sites

Schematized data assets

Answer Area

SharePoint Online: Scope

Microsoft Teams: Scope

Exchange Online: Scope

- 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 61

- (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 65

- (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 66

- (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 67

- (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 68

- (Exam Topic 2)

You need to design a strategy for securing the SharePoint Online and Exchange Online data. The solution must meet the application security requirements.

Which two services should you leverage in the strategy? Each correct answer presents part of the solution. NOTE; Each correct selection is worth one point.

- A. Azure AD Conditional Access
- B. Microsoft Defender for Cloud Apps
- C. Microsoft Defender for Cloud
- D. Microsoft Defender for Endpoint
- E. access reviews in Azure AD

Answer: AB

Explanation:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-session#c> <https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-integrate-with-microsoft-cl>

NEW QUESTION 73

- (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 76

- (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>

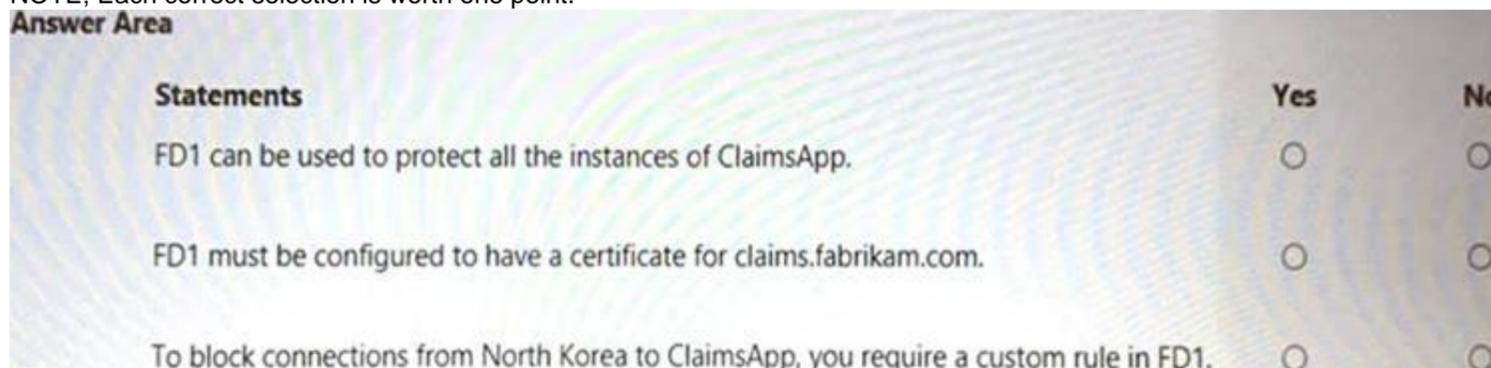
NEW QUESTION 81

- (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.



- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

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 83

- (Exam Topic 1)

What should you create in Azure AD to meet the Contoso developer requirements?

Account type for the developers:

- A guest account in the contoso.onmicrosoft.com tenant
- A guest account in the fabrikam.onmicrosoft.com tenant
- A synced user account in the corp.fabrikam.com domain
- A user account in the fabrikam.onmicrosoft.com tenant

Component in Identity Governance:

- A connected organization
- An access package
- An access review
- An Azure AD role
- An Azure resource role

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Box 1: A synced user account - Need to use a synced user account.

Box 2: An access review

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

NEW QUESTION 88

- (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 90

- (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 95

- (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 99

- (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 100

- (Exam Topic 3)

Your company is developing a modern application that will run as an Azure App Service web app. You plan to perform threat modeling to identify potential security issues by using the Microsoft Threat Modeling Tool. Which type of diagram should you create?

- A. data flow
- B. system flow
- C. process flow
- D. network flow

Answer: A

Explanation:

<https://docs.microsoft.com/en-us/learn/modules/tm-create-a-threat-model-using-foundational-data-flow-diagram> <https://docs.microsoft.com/en-us/azure/security/develop/threat-modeling-tool-getting-started?source=recommen>

NEW QUESTION 104

- (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 105

- (Exam Topic 3)

You have an Azure AD tenant that syncs with an Active Directory Domain Services (AD DS) domain. You are designing an Azure DevOps solution to deploy applications to an Azure subscription by using continuous integration and continuous deployment (CI/CD) pipelines.

You need to recommend which types of identities to use for the deployment credentials of the service connection. The solution must follow DevSecOps best practices from the Microsoft Cloud Adoption Framework for Azure.

What should you recommend?

- A. an Azure AD user account that has a password stored in Azure Key Vault
- B. a group managed service account (gMSA)
- C. an Azure AD user account that has role assignments in Azure AD Privileged Identity Management(PIM)
- D. a managed identity in Azure

Answer: D

NEW QUESTION 110

- (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 114

- (Exam Topic 3)

Your company is moving all on-premises workloads to Azure and Microsoft 365. You need to design a security orchestration, automation, and response (SOAR) strategy in Microsoft Sentinel that meets the following requirements:

- Minimizes manual intervention by security operation analysts
- Supports Waging alerts within Microsoft Teams channels What should you include in the strategy?

A. data connectors

B. playbooks

C. workbooks

D. KQL

Answer: B

Explanation:

<https://docs.microsoft.com/en-us/azure/sentinel/tutorial-respond-threats-playbook?tabs=LAC>

NEW QUESTION 115

- (Exam Topic 3)

Your company develops several applications that are accessed as custom enterprise applications in Azure Active Directory (Azure AD). You need to recommend a solution to prevent users on a specific list of countries from connecting to the applications. What should you include in the recommendation?

A. activity policies in Microsoft Defender for Cloud Apps

B. sign-in risk policies in Azure AD Identity Protection

C. device compliance policies in Microsoft Endpoint Manager

D. Azure AD Conditional Access policies

E. user risk policies in Azure AD Identity Protection

Answer: A

Explanation:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-loc> <https://docs.microsoft.com/en-us/power-platform/admin/restrict-access-online-trusted-ip-rules>

NEW QUESTION 118

- (Exam Topic 3)

You have an Azure subscription that has Microsoft Defender for Cloud enabled.

You are evaluating the Azure Security Benchmark V3 report as shown in the following exhibit.

Home > Microsoft Defender for Cloud

Microsoft Defender for Cloud

Showing subscription 'Subscription1'

Download report Manage compliance policies Open query Audit reports

You can now fully customize the standards you track in the dashboard. Update your dashboard by selecting 'Manage compliance policies' above.

Azure Security Benchmark V3 ISO 27001 PCI DSS 3.2.1 SOC TSP HIPAA HITRUST

Under each applicable compliance control is the set of assessments run by Defender for Cloud that are associated with that control. If they are all green, it means those assessments are currently passing; this does not ensure you are fully compliant with that control. Furthermore, not all controls for any particular regulation are covered by Defender for Cloud assessments, and therefore this report is only a partial view of your overall compliance status.

Azure Security Benchmark is applied to the subscription Subscription1

Expand all compliance controls

- NS. Network Security
- IM. Identity Management
- PA. Privileged Access
- DP. Data Protection
- AM. Asset Management
- LT. Logging and Threat Detection
- IR. Incident Response
- PV. Posture and Vulnerability Management
- ES. Endpoint Security
- BR. Backup and Recovery
- DS. DevOps Security

You need to verify whether Microsoft Defender for servers is installed on all the virtual machines that run Windows. Which compliance control should you evaluate?

- A. Data Protection
- B. Incident Response
- C. Posture and Vulnerability Management
- D. Asset Management
- E. Endpoint Security

Answer: E

Explanation:

<https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-endpoint-security>

NEW QUESTION 119

- (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 122

- (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 123

- (Exam Topic 3)

You have a Microsoft 365 E5 subscription.

You need to recommend a solution to add a watermark to email attachments that contain sensitive data. What should you include in the recommendation?

- A. Microsoft Defender for Cloud Apps
- B. insider risk management
- C. Microsoft Information Protection
- D. Azure Purview

Answer: C

Explanation:

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

You can use sensitivity labels to: Provide protection settings that include encryption and content markings. For example, apply a "Confidential" label to a document or email, and that label encrypts the content and applies a "Confidential" watermark. Content markings include headers and footers as well as watermarks, and encryption can also restrict what actions authorized people can take on the content. Protect content in Office apps across different platforms and devices. Supported by Word, Excel, PowerPoint, and Outlook on the Office desktop apps and Office on the web. Supported on Windows, macOS, iOS, and Android. Protect content in third-party apps and services by using Microsoft Defender for Cloud Apps. With Defender for Cloud Apps, you can detect, classify, label, and protect content in third-party apps and services, such as Salesforce, Box, or DropBox, even if the third-party app or service does not read or support sensitivity labels.

NEW QUESTION 127

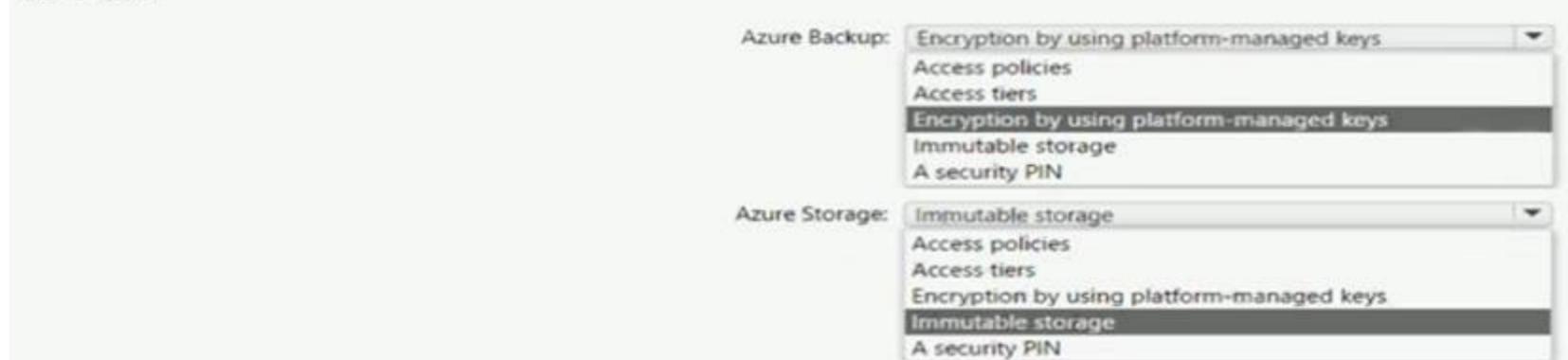
- (Exam Topic 3)

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

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

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

Answer Area



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

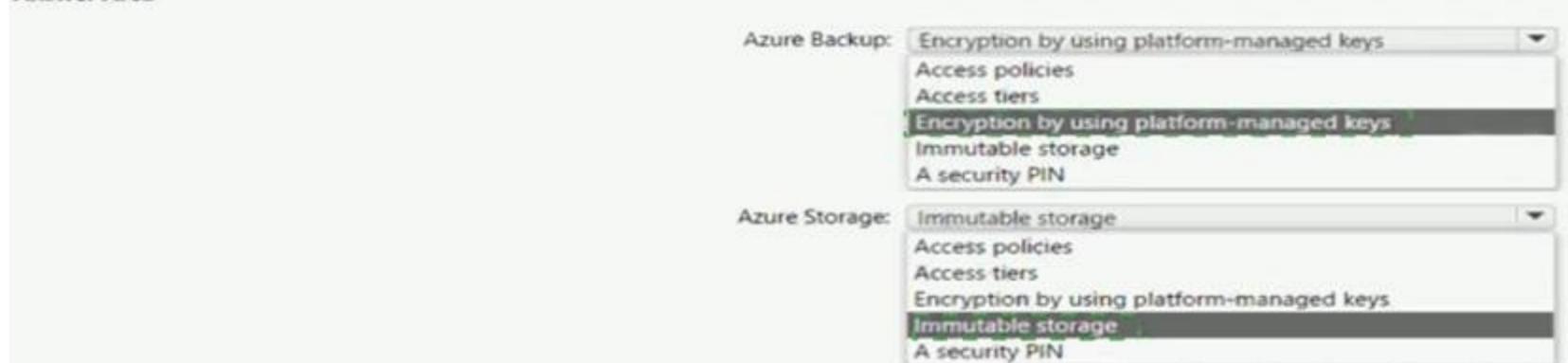
Azure Storage: Immutable storage
 Access policies
 Access tiers
 Encryption by using platform-managed keys
 Immutable storage
 A security PIN

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area



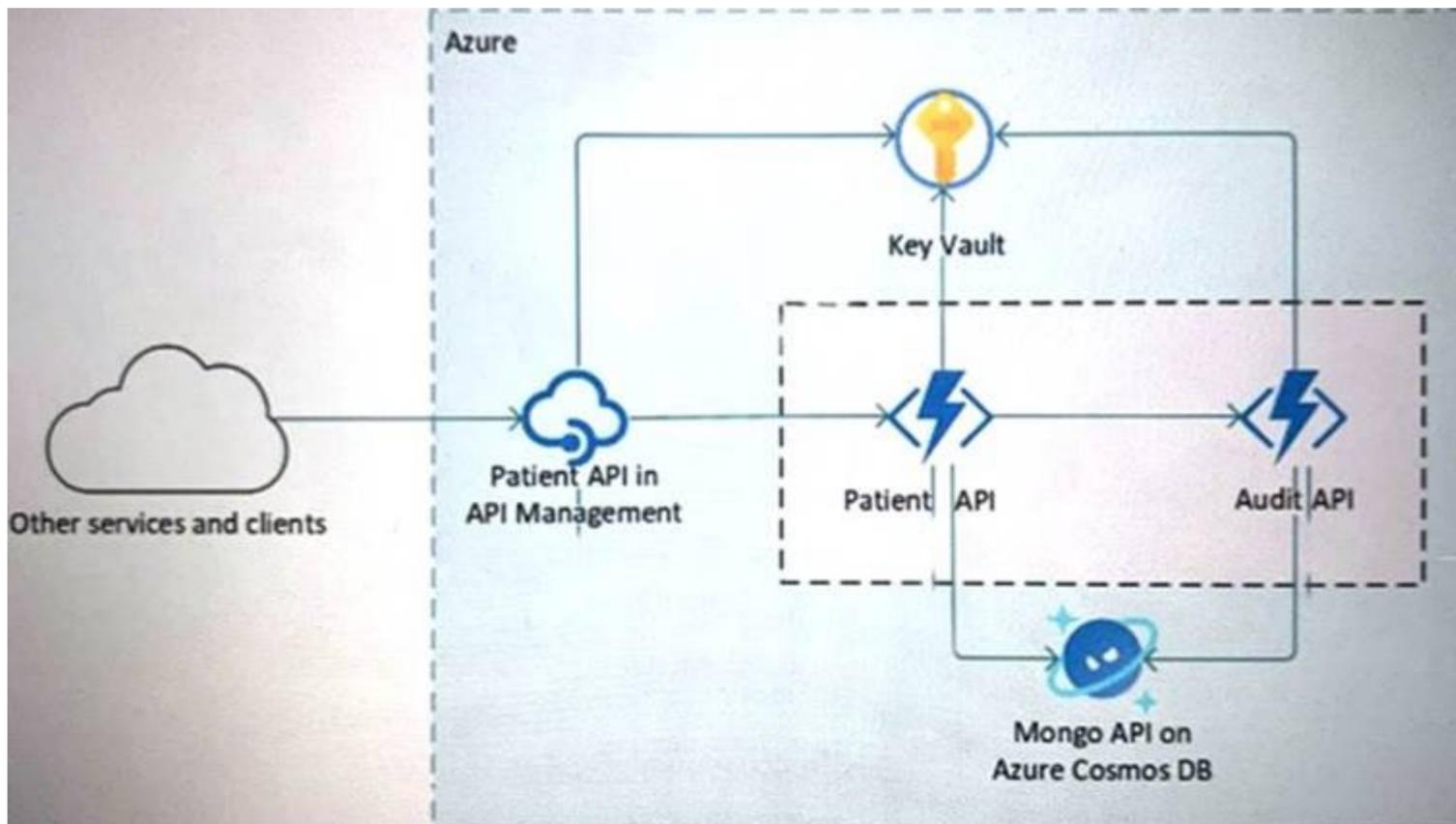
Azure Backup: Encryption by using platform-managed keys
 Access policies
 Access tiers
 Encryption by using platform-managed keys
 Immutable storage
 A security PIN

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

NEW QUESTION 129

- (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 131

- (Exam Topic 3)

You have an Azure subscription.

Your company has a governance requirement that resources must be created in the West Europe or North Europe Azure regions.

What should you recommend using to enforce the governance requirement?

- A. regulatory compliance standards in Microsoft Defender for Cloud
- B. custom Azure roles
- C. Azure Policy assignments
- D. Azure management groups

Answer: C

NEW QUESTION 133

- (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.

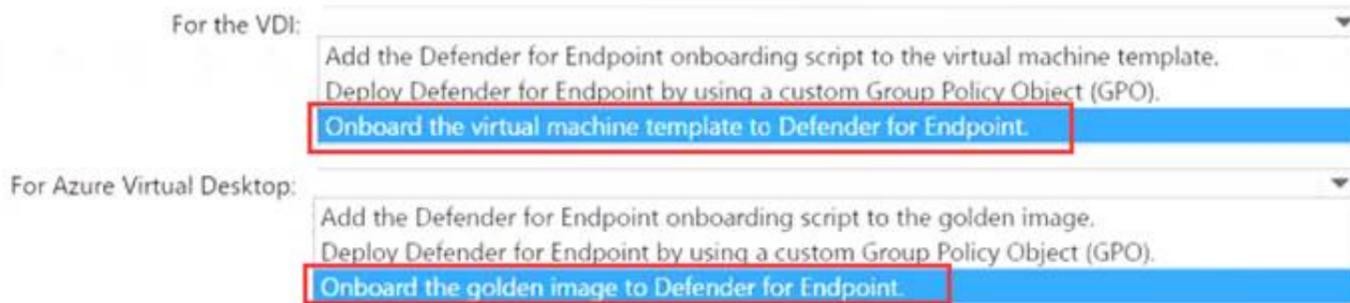
For Azure Virtual Desktop: Add the Defender for Endpoint onboarding script to the golden image.
 Deploy Defender for Endpoint by using a custom Group Policy Object (GPO).
 Onboard the golden image to Defender for Endpoint.

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Answer Area



NEW QUESTION 137

- (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 139

- (Exam Topic 3)

Your company has a Microsoft 365 subscription and uses Microsoft Defender for Identity. You are informed about incidents that relate to compromised identities.

You need to recommend a solution to expose several accounts for attackers to exploit. When the attackers attempt to exploit the accounts, an alert must be triggered. Which Defender for Identity feature should you include in the recommendation?

- A. standalone sensors
- B. honeypot entity tags
- C. sensitivity labels
- D. custom user tags

Answer: B

Explanation:

<https://docs.microsoft.com/en-us/advanced-threat-analytics/suspicious-activity-guide#honeypot-activity> The Sensitive tag is used to identify high value assets.(user / devices / groups)Honeypot entities are used as traps for malicious actors. Any authentication associated with these honeypot entities triggers an alert. and Defender for Identity considers Exchange servers as high-value assets and automatically tags them as Sensitive

NEW QUESTION 141

- (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 142

- (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

Infrastructure scanning: 

- Build and test
- Commit the code
- Go to production**
- Operate
- Plan and develop

Static application security testing: 

- Build and test**
- Commit the code
- Go to production
- Operate
- Plan and develop

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:
Answer Area

Infrastructure scanning: 

- Build and test
- ~~Commit the code~~
- Go to production**
- Operate
- Plan and develop

Static application security testing: 

- Build and test**
- Commit the code
- Go to production
- Operate
- Plan and develop**

NEW QUESTION 143

- (Exam Topic 3)

You have a hybrid cloud infrastructure.

You plan to deploy the Azure applications shown in the following table.

Name	Type	Requirement
App1	An Azure App Service web app accessed from Windows 11 devices on the on-premises network	Protect against attacks that use cross-site scripting (XSS).
App2	An Azure App Service web app accessed from mobile devices	Allow users to authenticate to App2 by using their LinkedIn account.

What should you use to meet the requirement of each app? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Answer Area

App1: Azure AD B2B authentication with Conditional Access

App2: Azure AD B2C custom policies with Conditional Access

Azure Application Gateway Web Application Firewall policies

Azure Firewall

Azure VPN Gateway with network security group rules

Azure VPN Point-to-Site connections

App2: Azure AD B2B authentication with Conditional Access

Azure AD B2C custom policies with Conditional Access

Azure Application Gateway Web Application Firewall policies

Azure Firewall

Azure VPN Gateway with network security group rules

Azure VPN Point-to-Site connections

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

Text Description automatically generated with medium confidence

NEW QUESTION 148

- (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

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

Answer Area

- Establish visibility.
- Enable additional protection and detection controls.
- Enable automation.

NEW QUESTION 150

- (Exam Topic 3)

You plan to automate the development and deployment of a Nodejs-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

To automate vulnerability code scanning:

- GitHub Enterprise Cloud
- GitHub Enterprise Cloud
- GitHub Enterprise Server
- GitHub Team

To automatically generate pull requests:

- Dependabot
- Codespaces
- Dependabot
- Dependency Tracker

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

A close up of a text Description automatically generated

NEW QUESTION 154

- (Exam Topic 3)

You are designing a security operations strategy based on the Zero Trust framework.

You need to minimize the operational load on Tier 1 Microsoft Security Operations Center (SOC) analysts. What should you do?

- A. Enable built-in compliance policies in Azure Policy.
- B. Enable self-healing in Microsoft 365 Defender.
- C. Automate data classification.
- D. Create hunting queries in Microsoft 365 Defender.

Answer: C

NEW QUESTION 155

- (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:	<input type="checkbox"/> A Log Analytics workspace <input type="checkbox"/> Azure Application Insights <input type="checkbox"/> Microsoft Defender for SQL <input type="checkbox"/> Microsoft Sentinel
For the Security logs:	<input type="checkbox"/> A Log Analytics workspace <input type="checkbox"/> Application Insights <input type="checkbox"/> Microsoft Defender for servers <input type="checkbox"/> Microsoft Sentinel
For the App Service audit logs:	<input type="checkbox"/> A Log Analytics workspace <input type="checkbox"/> Application Insights <input type="checkbox"/> Microsoft Defender for App Service <input type="checkbox"/> Microsoft Sentinel

- A. Mastered
- B. Not Mastered

Answer: A

Explanation:

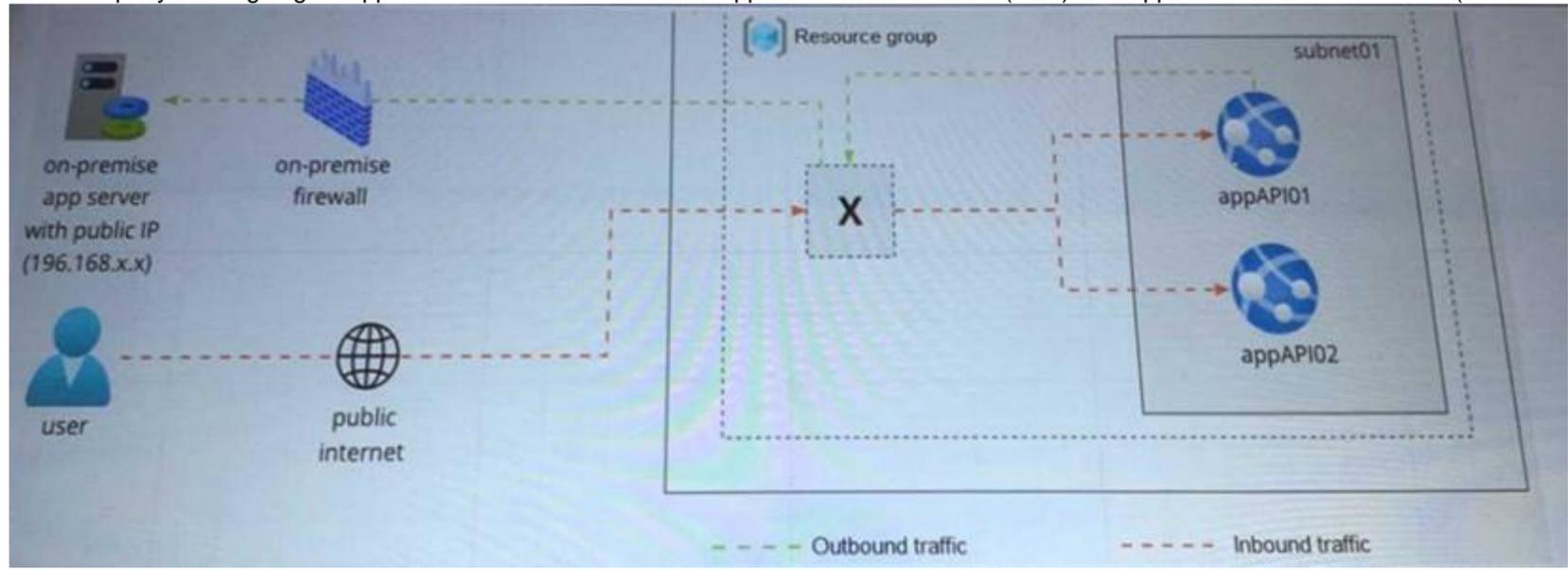
Answer Area

For the SQL audit logs:	<input type="checkbox"/> A Log Analytics workspace <input type="checkbox"/> Azure Application Insights <input checked="" type="checkbox"/> Microsoft Defender for SQL <input type="checkbox"/> Microsoft Sentinel
For the Security logs:	<input checked="" type="checkbox"/> A Log Analytics workspace <input type="checkbox"/> Application Insights <input type="checkbox"/> Microsoft Defender for servers <input type="checkbox"/> Microsoft Sentinel
For the App Service audit logs:	<input type="checkbox"/> A Log Analytics workspace <input type="checkbox"/> Application Insights <input type="checkbox"/> Microsoft Defender for App Service <input checked="" type="checkbox"/> Microsoft Sentinel

NEW QUESTION 157

- (Exam Topic 3)

Your company is designing an application architecture for Azure App Service Environment (ASE) web apps as shown in the exhibit. (Click the Exhibit tab.)



Communication between the on-premises network and Azure uses an ExpressRoute connection.

You need to recommend a solution to ensure that the web apps can communicate with the on-premises application server. The solution must minimize the number of public IP addresses that are allowed to access the on-premises network.

What should you include in the recommendation?

- A. Azure Traffic Manager with priority traffic-routing methods
- B. Azure Application Gateway v2 with user-defined routes (UDRs).
- C. Azure Front Door with Azure Web Application Firewall (WAF)
- D. Azure Firewall with policy rule sets

Answer: C

Explanation:

<https://docs.microsoft.com/en-us/azure/web-application-firewall/afds/afds-overview>

NEW QUESTION 160

- (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 162

- (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 167

- (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 based on HTTP headers that have the Front Door ID. Does this meet the goal?

- A. Yes
- B. No

Answer: A

Explanation:

<https://docs.microsoft.com/en-us/azure/frontdoor/front-door-faq#how-do-i-lock-down-the-access-to-my-backend>

NEW QUESTION 172

- (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 AllowSharedKeyAccess property to false.
- C. Set the AllowBlobPublicAccess 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 174

.....

Relate Links

100% Pass Your SC-100 Exam with Exam Bible Prep Materials

<https://www.exambible.com/SC-100-exam/>

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - <https://www.exambible.com/>