

Microsoft.SC-100.vNov-2023.by.Lan.58q

Number: SC-100
Passing Score: 800
Time Limit: 120
File Version: 15.0

Exam Code: SC-100
Exam Name: Microsoft Cybersecurity Architect



Exam A

QUESTION 1

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

Correct Answer: B

Section:

Explanation:

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

QUESTION 2

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

Correct Answer: A

Section:

Explanation:

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

QUESTION 3

Your company has a third-party security information and event management (SIEM) solution that uses Splunk and Microsoft Sentinel. You plan to integrate Microsoft Sentinel with Splunk. You need to recommend a solution to send security events from Microsoft Sentinel to Splunk. What should you include in the recommendation?

- A. Azure Event Hubs
- B. Azure Data Factor

- C. a Microsoft Sentinel workbook
- D. a Microsoft Sentinel data connector

Correct Answer: D

Section:

Explanation:

<https://techcommunity.microsoft.com/t5/microsoft-sentinel-blog/azure-sentinel-side-by-side-with-splunk-via-eventhub/ba-p/2307029>

QUESTION 4



Your company has an Azure subscription that has enhanced security enabled for Microsoft Defender for Cloud. The company signs a contract with the United States government.



You need to review the current subscription for NIST 800-53 compliance.



What should you do first?

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

Correct Answer: D

Section:

Explanation:

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

QUESTION 5

HOTSPOT

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

You need to recommend which capabilities of Azure Backup and Azure Storage provide the strongest protection against ransomware attacks. The solution must follow Microsoft Security Best Practices. What should you recommend? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

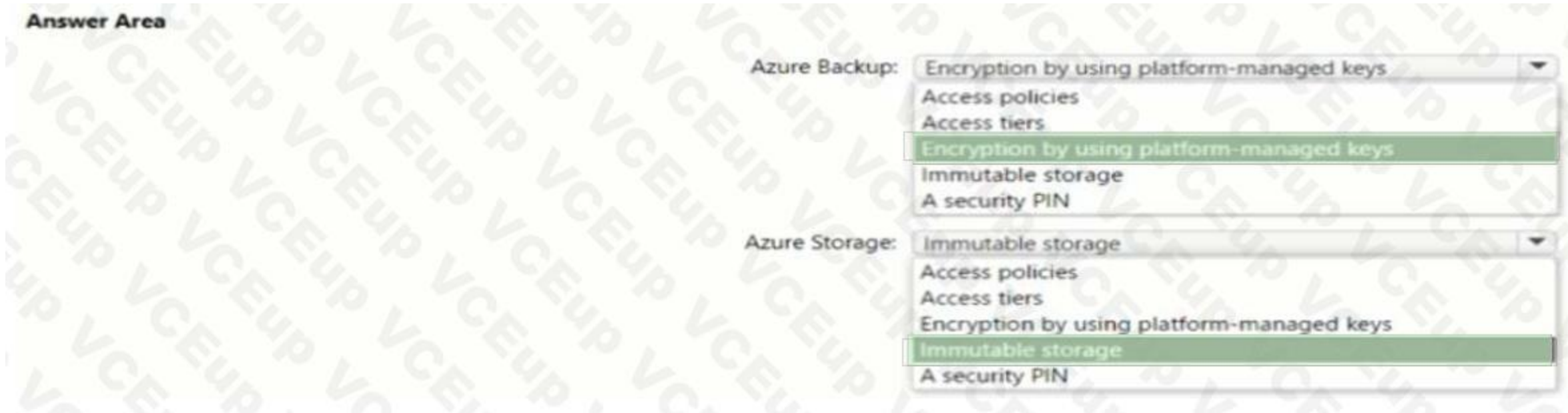
Hot Area:

Answer Area

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

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

Answer Area:



Section:

Explanation:

QUESTION 6

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



Correct Answer: B, D, E

Section:

Explanation:

<https://docs.microsoft.com/en-us/azure/defender-for-cloud/supported-machines-endpoint-solutions-clouds-containers?tabs=aws-eks>

QUESTION 7

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)

Correct Answer: A

Section:

Explanation:

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

QUESTION 8

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

Correct Answer: A

Section:

Explanation:

<https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-privileged-access#pa-2-avoid-standing-access-for-user-accounts-and-permissions> Adaptive Network Hardening: <https://docs.microsoft.com/en-us/security/benc>

QUESTION 9

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

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

Correct Answer: B, C

Section:

Explanation:



QUESTION 10

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

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

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

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

Correct Answer: D, E

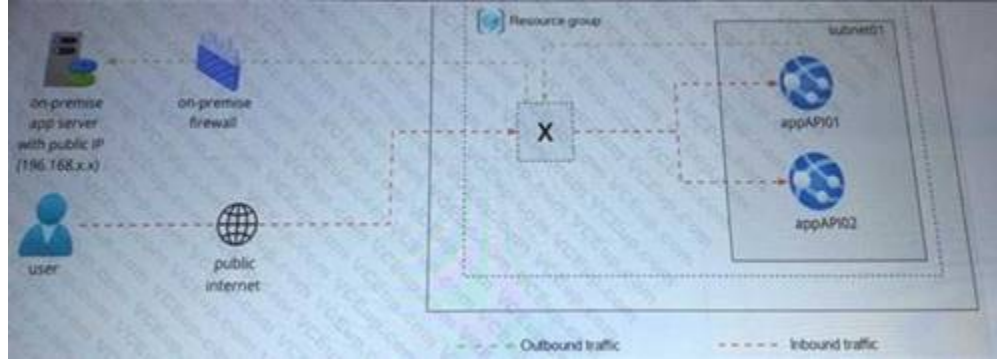
Section:

Explanation:

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

QUESTION 11

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

Correct Answer: C

Section:

Explanation:

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



QUESTION 12

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

Correct Answer: D

Section:

Explanation:

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

QUESTION 13

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

Correct Answer: C

Section:

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>

QUESTION 14

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

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

Correct Answer: B

Section:

Explanation:

Reference:

<https://docs.microsoft.com/en-us/azure/governance/blueprints/samples/iso27001-shared/control-mapping> <https://docs.microsoft.com/en-us/azure/defender-for-cloud/release-notes-archive> <https://docs.microsoft.com/en-us/azure/defender-for-cloud/prevent-misconfigurations>



QUESTION 15

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

Security alert

2517569153524258480_f132eeba-b7c9-4942-bf62-d0dd52ccfe74

MicroBurst exploitation toolkit used to extract keys to your storage accounts (Preview) [Sample alert](#)

High Severity Active Status 02/20/22, 0... Activity time

Alert description [Copy alert JSON](#)

THIS IS A SAMPLE ALERT: MicroBurst's exploitation toolkit was used to extract keys to your storage accounts. This was detected by analyzing Azure Activity logs and resource management operations in your subscription.

Affected resource



MITRE ATT&CK® tactics

• Collection

Alert details [Take action](#)

MicroBurst modules

Get-AZStorageKeysREST

Detected by

Microsoft

PrincipalOid

00000000-0000-0000-0000-000000000000

IP address

00.00.00.000

Username

Sample user

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

Correct Answer: A

Section:

Explanation:

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

QUESTION 16

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

Correct Answer: A, B

Section:

Explanation:

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

QUESTION 17

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

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

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

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

Correct Answer: A, C

Section:

Explanation:

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

QUESTION 18

Your company finalizes the adoption of Azure and is implementing Microsoft Defender for Cloud.

You receive the following recommendations in Defender for Cloud

- Access to storage accounts with firewall and virtual network configurations should be restricted,
- Storage accounts should restrict network access using virtual network rules.
- Storage account should use a private link connection.
- Storage account public access should be disallowed.

You need to recommend a service to mitigate identified risks that relate to the recommendations.

What should you recommend?

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

Correct Answer: D

Section:

Explanation:

<https://docs.microsoft.com/en-us/azure/defender-for-cloud/security-policy-concept> <https://docs.microsoft.com/en-us/security/benchmark/azure/baselines/storage-security-baseline>

QUESTION 19

You have 50 Azure subscriptions.

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

NOTE: Each correct selection is worth one point.

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



F. Assign a blueprint to a management group.

Correct Answer: A, F

Section:

Explanation:

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

QUESTION 20

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

Correct Answer: B

Section:

QUESTION 21

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

Correct Answer: A, C

Section:

Explanation:

<https://docs.microsoft.com/en-us/azure/active-directory-b2c/threat-management> [https://docs.microsoft.com/en-us/active-directory-b2c/conditional-access-user-flow?pivots=b2c-user-flow](https://docs.microsoft.com/en-us/azure/active-directory-b2c/conditional-access-user-flow?pivots=b2c-user-flow)

QUESTION 22

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

Correct Answer: C

Section:

Explanation:

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

QUESTION 23

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

Correct Answer: A, C

Section:**Explanation:**

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

QUESTION 24

You have an Azure subscription that has Microsoft Defender for Cloud enabled. You are evaluating the Azure Security Benchmark V3 report. In the Secure management ports controls, you discover that you have 0 out of a potential 8 points.

You need to recommend configurations to increase the score of the Secure management ports controls. Solution: You recommend onboarding all virtual machines to Microsoft Defender for Endpoint. Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section:**Explanation:**

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

QUESTION 25

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

Correct Answer: B

Section:**Explanation:**

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

QUESTION 26

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

Correct Answer: B

Section:

QUESTION 27

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

Correct Answer: A

Section:

Explanation:

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

QUESTION 28

A customer has a hybrid cloud infrastructure that contains a Microsoft 365 E5 subscription and an Azure subscription. All the on-premises servers in the perimeter network are prevented from connecting directly to the internet. The customer recently recovered from a ransomware attack.

The customer plans to deploy Microsoft Sentinel.

You need to recommend configurations to meet the following requirements:

- Ensure that the security operations team can access the security logs and the operation logs.
- Ensure that the IT operations team can access only the operations logs, including the event logs of the servers in the perimeter network. Which two configurations can you include in the recommendation? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

- A. Azure Active Directory (Azure AD) Conditional Access policies
- B. a custom collector that uses the Log Analytics agent
- C. resource-based role-based access control (RBAC)
- D. the Azure Monitor agent

Correct Answer: C, D

Section:

Explanation:

<https://docs.microsoft.com/en-us/azure/azure-monitor/agents/log-analytics-agent>

QUESTION 29

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.





 **vdumps**

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

Correct Answer: B

Section:

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.

QUESTION 30

HOTSPOT

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

[Home](#) > [Microsoft Defender for Cloud](#)

Recommendations

Showing subscription 'Subscription1'

[Download CSV report](#) [Guides & Feedback](#)

These recommendations directly affect your secure score. They're grouped into security controls, each representing a risk category. Focus your efforts on controls worth the most points, and fix all recommendations for all resources in a control to get the max points. [Learn more >](#)

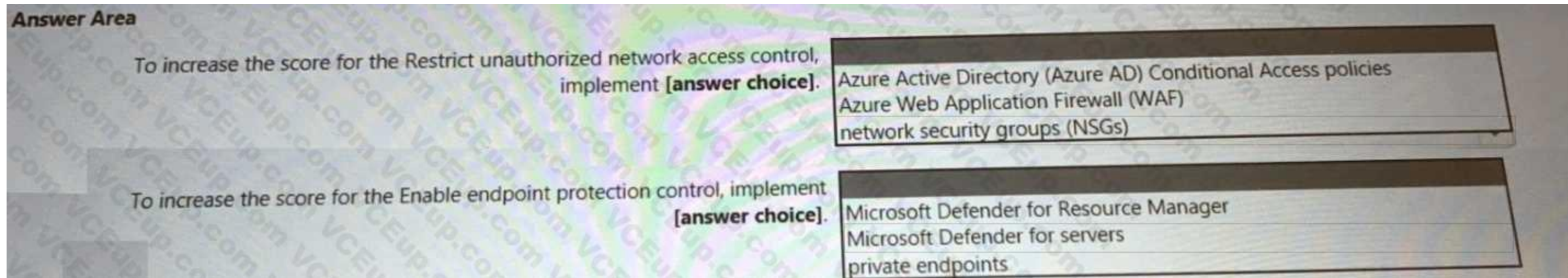
Control status : All
Recommendation status : 2 Selected
Recommendation maturity : All
Severity : All
Sort by max score

Expand all
Resource type : All
Response actions : All
Contains exemptions : All
Environment : All
Tactics : All
Reset filters

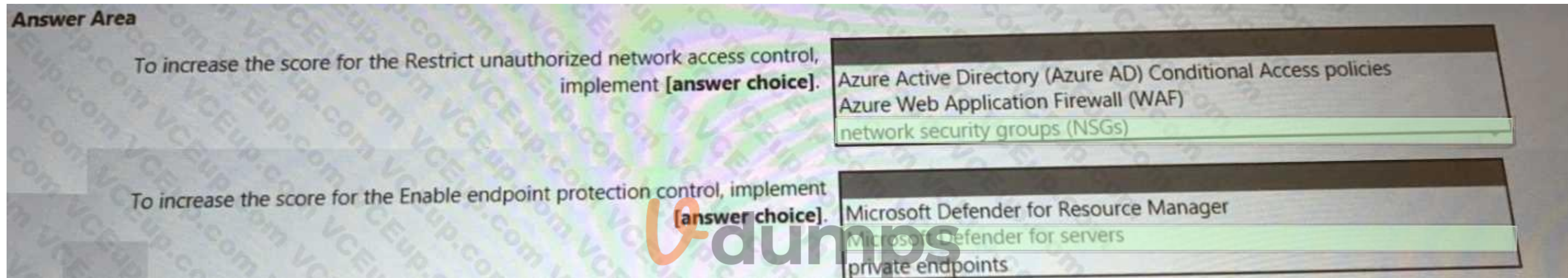
| Controls | Max score | Current Score | Potential score incre... | Unhealthy resources | Resource health | Actions |
|---------------------------------------|------------|---------------|--------------------------|---------------------|---|---------|
| > Enable MFA | 10 | 0.00 | + 18% (10 points) | 1 of 1 resources | <div style="width: 0%; background-color: red;"></div> | |
| > Secure management ports | 8 | 5.33 | + 5% (2.67 points) | 1 of 3 resources | <div style="width: 66.6%; background-color: red;"></div> | |
| > Remediate vulnerabilities | 6 | 0.00 | + 11% (6 points) | 3 of 3 resources | <div style="width: 0%; background-color: red;"></div> | |
| > Apply system updates | 6 | 6.00 | + 0% (0 points) | None | <div style="width: 100%; background-color: green;"></div> | |
| > Manage access and permissions | 4 | 0.00 | + 7% (4 points) | 1 of 12 resources | <div style="width: 0%; background-color: red;"></div> | |
| > Enable encryption at rest | 4 | 1.00 | + 5% (3 points) | 3 of 4 resources | <div style="width: 25%; background-color: red;"></div> | |
| > Restrict unauthorized network acces | 4 | 3.00 | + 2% (1 point) | 1 of 11 resources | <div style="width: 75%; background-color: red;"></div> | |
| > Remediate security configurations | 4 | 3.00 | + 2% (1 point) | 1 of 4 resources | <div style="width: 75%; background-color: red;"></div> | |
| > Encrypt data in transit | 4 | 3.33 | + 1% (0.67 points) | 1 of 6 resources | <div style="width: 55.5%; background-color: red;"></div> | |
| > Apply adaptive application control | 3 | 3.00 | + 0% (0 points) | None | <div style="width: 100%; background-color: green;"></div> | |
| > Enable endpoint protection | 2 | 0.67 | + 2% (1.33 points) | 2 of 3 resources | <div style="width: 33.3%; background-color: red;"></div> | |
| > Enable auditing and logging | 1 | 0.00 | + 2% (1 point) | 4 of 5 resources | <div style="width: 0%; background-color: red;"></div> | |
| > Enable enhanced security features | Not scored | Not scored | + 0% (0 points) | None | <div style="width: 0%; background-color: red;"></div> | |
| > Implement security best practices | Not scored | Not scored | + 0% (0 points) | 9 of 30 resources | <div style="width: 0%; background-color: red;"></div> | |

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.

Hot Area:



Answer Area:



Section:

Explanation:

Selection 1: NSG

<https://techcommunity.microsoft.com/t5/microsoft-defender-for-cloud/security-control-restrict-unauthorized-network-access/ba-p/1593833> Selection 2: Microsoft Defender for servers

Enable endpoint protection - Defender for Cloud checks your organization's endpoints for active threat detection and response solutions such as Microsoft Defender for Endpoint or any of the major solutions shown in this list.

When an Endpoint Detection and Response (EDR) solution isn't found, you can use these recommendations to deploy Microsoft Defender for Endpoint (included as part of Microsoft Defender for servers). Incorrect:

Not Microsoft Defender for Resource Manager:

Microsoft Defender for Resource Manager does not handle endpoint protection.

Microsoft Defender for Resource Manager automatically monitors the resource management operations in your organization, whether they're performed through the Azure portal, Azure REST APIs, Azure CLI, or other Azure programmatic clients. Defender for Cloud runs advanced security analytics to detect threats and alerts you about suspicious activity.

Reference:

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

QUESTION 31

HOTSPOT

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

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

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

Hot Area:

Answer Area

Windows 11 devices:

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

Azure virtual machines:

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

Azure Storage accounts:

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

Answer Area:

Answer Area

Windows 11 devices:

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

Azure virtual machines:

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

Azure Storage accounts:

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

Section:

Explanation:

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

Selection 2: Microsoft Defender for Cloud.

Selection 3: Microsoft Defender for Cloud. <https://docs.microsoft.com/en-us/learn/modules/design-strategy-for-secure-paas-iaas-saas-services/8-specify-security-requirements-for-storage-workloads>

QUESTION 32

HOTSPOT

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.

Hot 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

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

Section:

Explanation:

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

QUESTION 33

HOTSPOT

You are creating the security recommendations for an Azure App Service web app named App1.

App1 has the following specifications:

- Users will request access to App1 through the My Apps portal. A human resources manager will approve the requests.
- Users will authenticate by using Azure Active Directory (Azure AD) user accounts.

You need to recommend an access security architecture for App1.

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.

Hot Area:

To enable Azure AD authentication for App1, use:

| |
|--------------------------------|
| Azure AD application |
| Azure AD Application Proxy |
| Azure Application Gateway |
| A managed identity in Azure AD |
| Microsoft Defender for App |

To implement access requests for App1, use:

| |
|--|
| An access package in Identity Governance |
| An access policy in Microsoft Defender for Cloud Apps |
| An access review in Identity Governance |
| Azure AD Conditional Access App Control |
| An OAuth app policy in Microsoft Defender for Cloud Apps |

Answer Area:

To enable Azure AD authentication for App1, use:

| |
|--------------------------------|
| Azure AD application |
| Azure AD Application Proxy |
| Azure Application Gateway |
| A managed identity in Azure AD |
| Microsoft Defender for App |

To implement access requests for App1, use:

| |
|--|
| An access package in Identity Governance |
| An access policy in Microsoft Defender for Cloud Apps |
| An access review in Identity Governance |
| Azure AD Conditional Access App Control |
| An OAuth app policy in Microsoft Defender for Cloud Apps |

Section:

Explanation:

Azure AD application

(<https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/what-is-application-management>) An access package in identity governance

(<https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-access-package-create>)

QUESTION 34

DRAG DROP

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.

Select and Place:

| Components | Answer Area |
|---|---|
| A data loss prevention (DLP) policy | User accounts that were potentially compromised: <input type="text"/> Component |
| Azure Active Directory (Azure AD) Conditional Access | |
| Azure Active Directory (Azure AD) Identity Protection | Users performing bulk file downloads from SharePoint Online: <input type="text"/> Component |
| Microsoft Defender for Cloud | |
| Microsoft Defender for Cloud Apps | |

Correct Answer:

| Components | Answer Area |
|--|---|
| A data loss prevention (DLP) policy | User accounts that were potentially compromised: Azure Active Directory (Azure AD) Identity Protection |
| Azure Active Directory (Azure AD) Conditional Access | |
| <input type="text"/> | |
| <input type="text"/> | |
| Microsoft Defender for Cloud Apps | Users performing bulk file downloads from SharePoint Online: Microsoft Defender for Cloud |

Section:

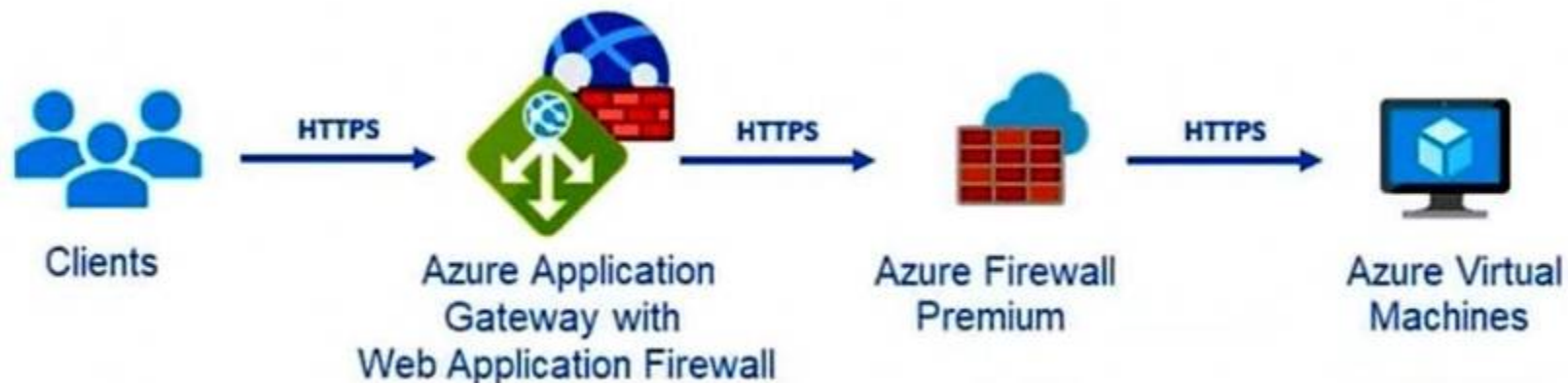
Explanation:

<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-exfiltration>
<https://docs.microsoft.com/en-us/microsoft-365/security/defender/investigate-users>

QUESTION 35

HOTSPOT

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.

Hot Area:

Answer Area

For WAF:

- The Azure Diagnostics extension
- Azure Network Watcher
- Data connectors
- Workflow automation

For the virtual machines:

- The Azure Diagnostics extension
- Azure Storage Analytics
- Data connectors
- The Log Analytics agent
- Workflow automation

Answer Area:

Answer Area

For WAF:

- The Azure Diagnostics extension
- Azure Network Watcher
- Data connectors
- Workflow automation

For the virtual machines:

- The Azure Diagnostics extension
- Azure Storage Analytics
- Data connectors
- The Log Analytics agent
- Workflow automation

Section:

Explanation:

Box 1: Data connectors -

Microsoft Sentinel connector streams security alerts from Microsoft Defender for Cloud into Microsoft Sentinel. Launch a WAF workbook (see step 7 below)

The WAF workbook works for all Azure Front Door, Application Gateway, and CDN WAFs. Before connecting the data from these resources, log analytics must be enabled on your resource. To enable log analytics for each resource, go to your individual Azure Front Door, Application Gateway, or CDN resource:

1. Select Diagnostic settings.
2. Select + Add diagnostic setting.
3. In the Diagnostic setting page (details skipped)
4. On the Azure home page, type Microsoft Sentinel in the search bar and select the Microsoft Sentinel resource.
5. Select an already active workspace or create a new workspace.
6. On the left side panel under Configuration select Data Connectors.
7. Search for Azure web application firewall and select Azure web application firewall (WAF). Select Open connector page on the bottom right.
8. Follow the instructions under Configuration for each WAF resource that you want to have log analytic data for if you haven't done so previously.
9. Once finished configuring individual WAF resources, select the Next steps tab. Select one of the recommended workbooks. This workbook will use all log analytic data that was enabled previously. A working WAF workbook should now exist for your WAF resources.

Box 2: The Log Analytics agent -

Use the Log Analytics agent to integrate with Microsoft Defender for cloud.

QUESTION 36

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 customermanaged keys (CMKs). Does this meet the goal?

- A. Yes
- B. No

Correct Answer: A

Section:



QUESTION 37

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 Microsoftmanaged keys within an encryption scope. Does this meet the goal?

- A. Yes
- B. No

Correct Answer: B

Section:

Explanation:

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

QUESTION 38

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

Correct Answer: B

Section:

Explanation:

<https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-privilegedaccess#pa-2-avoid-standing-access-for-user-accounts-and-permissions> Adaptive Network Hardening:

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

QUESTION 39

HOTSPOT

You use Azure Pipelines with Azure Repos to implement continuous integration and continuous deployment (CI/CO) workflows. You need to recommend best practices to secure the stages of the CI/CD workflows based on the Microsoft Cloud Adoption Framework for Azure. What should you include in the recommendation for each stage? To answer, select the appropriate options in the answer area. NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

Git workflow: Azure Key Vault
Azure Key Vault
Custom roles for build agents
Protected branches
Resource locks in Azure

Secure deployment credentials: Protected branches
Azure Key Vault
Custom roles for build agents
Protected branches
Resource locks in Azure

Answer Area:

Answer Area

Git workflow: Azure Key Vault
Azure Key Vault
Custom roles for build agents
Protected branches
Resource locks in Azure

Secure deployment credentials: Protected branches
Azure Key Vault
Custom roles for build agents
Protected branches
Resource locks in Azure

Section:

Explanation:

QUESTION 40

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

Correct Answer: B

Section:

QUESTION 41

You use Azure Pipelines with Azure Repos to implement continuous integration and continuous deployment (O/CD) workflows for the deployment of applications to Azure. You need to recommend what to include in dynamic application security testing (DAST) based on the principles of the Microsoft Cloud Adoption Framework for Azure. What should you recommend?

- A. unit testing
- B. penetration testing
- C. dependency checks
- D. threat modeling

Correct Answer: C

Section:

QUESTION 42

HOTSPOT

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.

Hot Area:

Answer Area

The screenshot shows two dropdown menus. The first menu is labeled 'Infrastructure scanning:' and has a dropdown arrow pointing to 'Go to production'. The second menu is labeled 'Static application security testing:' and has a dropdown arrow pointing to 'Build and test'. Both menus have a list of options: 'Go to production', 'Operate', and 'Plan and develop'. The 'Go to production' option in the first menu and the 'Build and test' option in the second menu are highlighted with a dark background, indicating they are the selected answers.

Answer Area:



Section:

Explanation:

QUESTION 43

For a Microsoft cloud environment, you are designing a security architecture based on the Microsoft Cloud Security Benchmark. What are three best practices for identity management based on the Azure Security Benchmark?

Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

- A. Manage application identities securely and automatically.
- B. Manage the lifecycle of identities and entitlements
- C. Protect identity and authentication systems.
- D. Enable threat detection for identity and access management.
- E. Use a centralized identity and authentication system.



Correct Answer: A, C, E

Section:

QUESTION 44

Your company plans to follow DevSecOps best practices of the Microsoft Cloud Adoption Framework for Azure. You need to perform threat modeling by using a top-down approach based on the Microsoft Cloud Adoption Framework for Azure. What should you use to start the threat modeling process?

- A. the STRIDE model
- B. the DREAD model
- C. OWASP threat modeling
- D. Other options

Correct Answer: C

Section:

QUESTION 45

HOTSPOT

Your company, named Contoso. Ltd... has an Azure AD tenant named contoso.com. Contoso has a partner company named Fabrikam. Inc. that has an Azure AD tenant named fabrikam.com. You need to ensure that helpdesk

users at Fabrikam can reset passwords for specific users at Contoso. The solution must meet the following requirements:

- * Follow the principle of least privilege.
- * Minimize administrative effort.

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

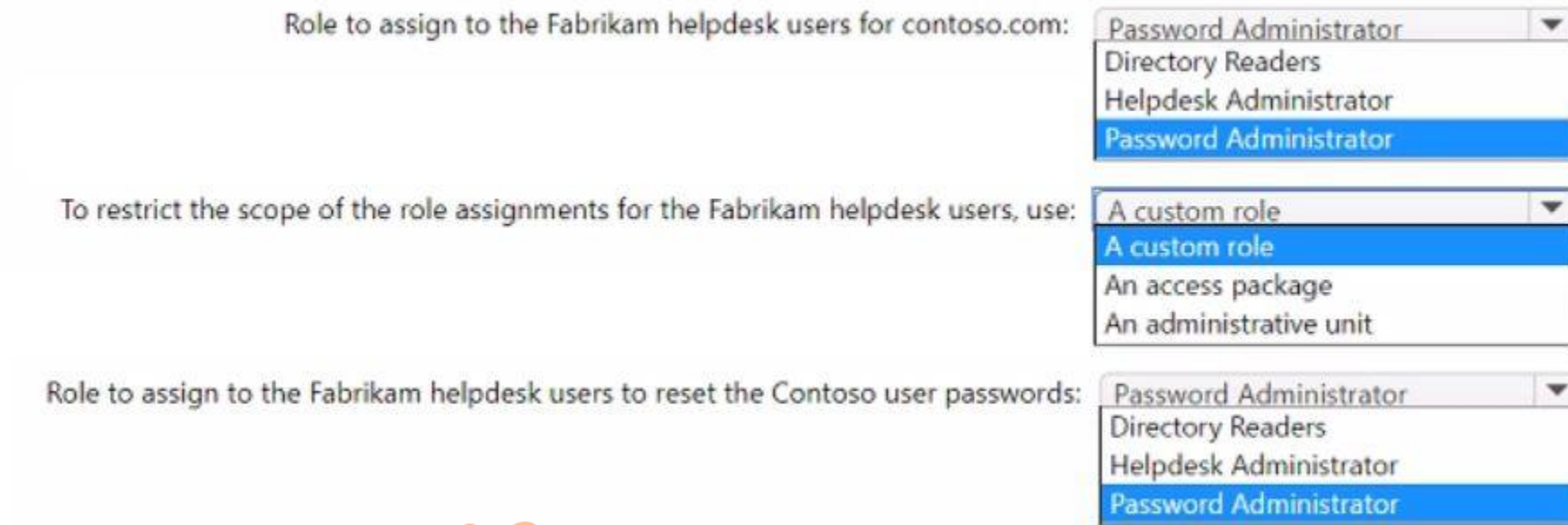
Hot Area:

Answer Area

Role to assign to the Fabrikam helpdesk users for contoso.com:

To restrict the scope of the role assignments for the Fabrikam helpdesk users, use:

Role to assign to the Fabrikam helpdesk users to reset the Contoso user passwords:



The screenshot shows a hot spot question interface with three dropdown menus. The first dropdown is labeled 'Role to assign to the Fabrikam helpdesk users for contoso.com:' and has 'Password Administrator' selected. The second dropdown is labeled 'To restrict the scope of the role assignments for the Fabrikam helpdesk users, use:' and has 'A custom role' selected. The third dropdown is labeled 'Role to assign to the Fabrikam helpdesk users to reset the Contoso user passwords:' and has 'Password Administrator' selected. The selected options are highlighted in blue.

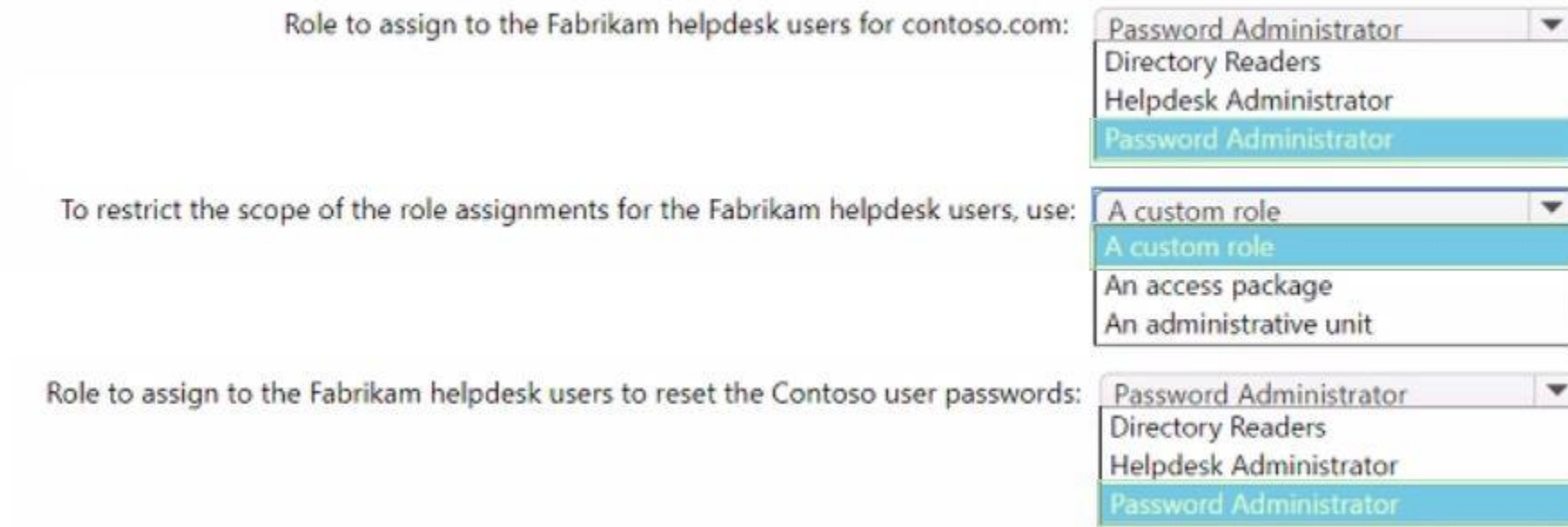
Answer Area:

Answer Area

Role to assign to the Fabrikam helpdesk users for contoso.com:

To restrict the scope of the role assignments for the Fabrikam helpdesk users, use:

Role to assign to the Fabrikam helpdesk users to reset the Contoso user passwords:



The screenshot shows a hot spot question interface with three dropdown menus. The first dropdown is labeled 'Role to assign to the Fabrikam helpdesk users for contoso.com:' and has 'Password Administrator' selected. The second dropdown is labeled 'To restrict the scope of the role assignments for the Fabrikam helpdesk users, use:' and has 'A custom role' selected. The third dropdown is labeled 'Role to assign to the Fabrikam helpdesk users to reset the Contoso user passwords:' and has 'Password Administrator' selected. The selected options are highlighted in blue.

Section:

Explanation:

QUESTION 46

HOTSPOT

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

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

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

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

Hot Area:
Answer Area

Manage NSG rules by using:

- Azure Bastion
- 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

Answer Area:
Answer Area

Manage NSG rules by using:

- Azure Bastion
- 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

Section:
Explanation:

QUESTION 47

HOTSPOT

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.

Hot Area:

Answer Area

To automate vulnerability code scanning:

- GitHub Enterprise Cloud
- GitHub Enterprise Server
- GitHub Team

To automatically generate pull requests:

- Codespaces
- Dependabot
- Dependency Tracker

Answer Area:

Answer Area

To automate vulnerability code scanning:

- GitHub Enterprise Cloud
- GitHub Enterprise Server
- GitHub Team

To automatically generate pull requests:

- Codespaces
- Dependabot
- Dependency Tracker

Section:

Explanation:

QUESTION 48

You have an Azure subscription. The subscription contains 50 virtual machines that run Windows Server and 50 virtual machines that run Linux. You need to perform vulnerability assessments on the virtual machines. The solution must meet the following requirements:

- * Identify missing updates and insecure configurations.
- * Use the Qualys engine.

What should you use?

- A. Microsoft Defender for Servers
- B. Microsoft Defender Threat Intelligence (Defender TI)
- C. Microsoft Defender for Endpoint
- D. Microsoft Defender External Attack Surface Management (Defender EASM)

Correct Answer: A

Section:

Case Study 01

Topic 1, Fabrikam, Inc Case Study 1

OverView

Fabrikam, Inc. is an insurance company that has a main office in New York and a branch office in Paris.

On-premises Environment

The on-premises network contains a single Active Directory Domain Services (AD DS) domain named corp.fabrikam.com.

Azure Environment

Fabrikam has the following Azure resources:

- An Azure Active Directory (Azure AD) tenant named fabrikam.onmicrosoft.com that syncs with corp.fabnkam.com
- A single Azure subscription named Sub1
- A virtual network named Vnet1 in the East US Azure region
- A virtual network named Vnet2 in the West Europe Azure region
- An instance of Azure Front Door named FD1 that has Azure Web Application Firewall (WAR enabled
- A Microsoft Sentinel workspace
- An Azure SQL database named ClaimsDB that contains a table named ClaimDetails
- 20 virtual machines that are configured as application servers and are NOT onboarded to Microsoft Defender for Cloud
- A resource group named TestRG that is used for testing purposes only
- An Azure Virtual Desktop host pool that contains personal assigned session hosts All the resources in Sub1 are in either the East US or the West Europe region.

Partners

Fabrikam has contracted a company named Contoso, Ltd. to develop applications. Contoso has the following infrastructure-

- An Azure AD tenant named contoso.onmicrosoft.com
- An Amazon Web Services (AWS) implementation named ContosoAWS1 that contains AWS EC2 instances used to host test workloads for the applications of Fabrikam Developers at Contoso will connect to the resources of Fabrikam to test or update applications. The developers will be added to a security Group named Contoso Developers in fabrikam.onmicrosoft.com that will be assigned to roles in Sub1.

The ContosoDevelopers group is assigned the db.owner role for the ClaimsDB database.

Compliance Event

Fabrikam deploys the following compliance environment:

- Defender for Cloud is configured to assess all the resources in Sub1 for compliance to the HIPAA HITRUST standard.
- Currently, resources that are noncompliant with the HIPAA HITRUST standard are remediated manually.
- Qualys is used as the standard vulnerability assessment tool for servers.

Problem Statements

The secure score in Defender for Cloud shows that all the virtual machines generate the following recommendation-. Machines should have a vulnerability assessment solution.

All the virtual machines must be compliant in Defender for Cloud.

ClaimApp Deployment

Fabrikam plans to implement an internet-accessible application named ClaimsApp that will have the following specification

- ClaimsApp will be deployed to Azure App Service instances that connect to Vnet1 and Vnet2.
- Users will connect to ClaimsApp by using a URL of https://claims.fabrikam.com.
- ClaimsApp will access data in ClaimsDB.
- ClaimsDB must be accessible only from Azure virtual networks.
- The app services permission for ClaimsApp must be assigned to ClaimsDB.

Application Development Requirements

Fabrikam identifies the following requirements for application development:

- Azure DevTest labs will be used by developers for testing.
- All the application code must be stored in GitHub Enterprise.
- Azure Pipelines will be used to manage application deployments.
- All application code changes must be scanned for security vulnerabilities, including application code or configuration files that contain secrets in clear text. Scanning must be done at the time the code is pushed to a repository.

Security Requirement

Fabrikam identifies the following security requirements:

- Internet-accessible applications must prevent connections that originate in North Korea.
- Only members of a group named InfraSec must be allowed to configure network security groups

(NSGs) and instances of Azure Firewall, VJM. And Front Door in Sub1.

- Administrators must connect to a secure host to perform any remote administration of the virtual machines. The secure host must be provisioned from a custom operating system image.

AWS Requirements

Fabrikam identifies the following security requirements for the data hosted in ContosoAWSV.

- Notify security administrators at Fabrikam if any AWS EC2 instances are noncompliant with secure score recommendations.
- Ensure that the security administrators can query AWS service logs directly from the Azure environment.

Contoso Developer Requirements

Fabrikam identifies the following requirements for the Contoso developers;

- Every month, the membership of the ContosoDevelopers group must be verified.
- The Contoso developers must use their existing contoso.onmicrosoft.com credentials to access the resources in Sub1.
- The Comoro developers must be prevented from viewing the data in a column named MedicalHistory in the ClaimDetails table.

Compliance Requirement

Fabrikam wants to automatically remediate the virtual machines in Sub1 to be compliant with the HIPPA HITRUST standard. The virtual machines in TestRG must be excluded from the compliance assessment.

QUESTION 1

HOTSPOT

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.

Hot Area:

Answer Area

| Statements | Yes | No |
|---|----------------------------------|-----------------------|
| FD1 can be used to protect all the instances of ClaimsApp. | <input checked="" type="radio"/> | <input 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"/> |

Answer Area:

Answer Area

| Statements | Yes | No |
|---|----------------------------------|-----------------------|
| FD1 can be used to protect all the instances of ClaimsApp. | <input checked="" type="radio"/> | <input 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"/> |

Section:

Explanation:

QUESTION 2

HOTSPOT

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.

Hot Area:

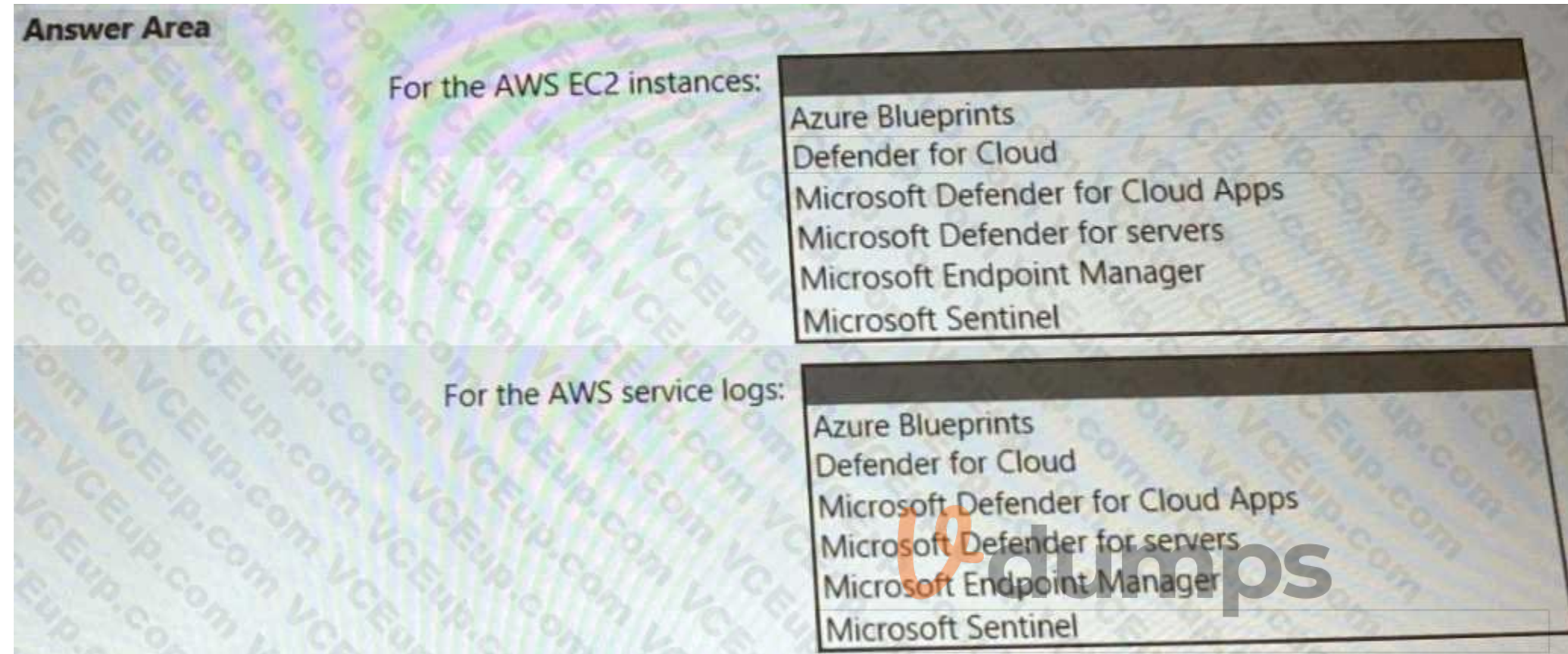
Answer Area

For the AWS EC2 instances:

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

For the AWS service logs:

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



Answer Area:

Answer Area

For the AWS EC2 instances:

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

For the AWS service logs:

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

Section:

Explanation:

QUESTION 3

HOTSPOT

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

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

Hot Area:



Answer Area

ClaimsDB must be accessible only from Azure virtual networks:

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

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

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

Answer Area:

Answer Area



ClaimsDB must be accessible only from Azure virtual networks:

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

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

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

Section:

Explanation:

QUESTION 4

You need to recommend a solution to meet the security requirements for the InfraSec group. What should you use to delegate the access?

- A. a subscription
- B. a custom role-based access control (RBAC) role
- C. a resource group
- D. a management group

Correct Answer: B

Section:

QUESTION 5

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

Correct Answer: B

Section:

Explanation:

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

QUESTION 6

You need to recommend a solution to resolve the virtual machine issue. What should you include in the recommendation? (Choose Two)

- A. Onboard the virtual machines to Microsoft Defender for Endpoint.
- B. Onboard the virtual machines to Azure Arc.
- C. Create a device compliance policy in Microsoft Endpoint Manager.
- D. Enable the Qualys scanner in Defender for Cloud.

Correct Answer: A, D

Section:

Explanation:

<https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/switch-to-mde-phase-3?view=o365-worldwide>

QUESTION 7

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

Correct Answer: B

Section:

Explanation:

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

QUESTION 8

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

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

Correct Answer: A

Section:

Explanation:

The security requirement this question wants us to meet is "The secure host must be provisioned from a custom operating system image." <https://docs.microsoft.com/en-us/azure/virtual-desktop/set-up-golden-image>

QUESTION 9

HOTSPOT

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

Hot Area:

The screenshot shows a hot spot area for a question. It contains two dropdown menus. The first dropdown is titled "Account type for the developers:" and has four options: "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", and "A user account in the fabrikam.onmicrosoft.com tenant". The second dropdown is titled "Component in Identity Governance:" and has four options: "A connected organization", "An access package", "An access review", "An Azure AD role", and "An Azure resource role".

Answer Area:

Answer Area

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

Section:

Explanation:

QUESTION 10

HOTSPOT

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

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

NOTE: Each correct selection is worth one point.



Hot Area:

Answer Area

To enforce compliance to the regulatory standard, create:

- An Azure Automation account
- A blueprint
- A managed identity
- Workflow automation

To exclude TestRG from the compliance assessment:

- Edit an Azure blueprint
- Modify a Defender for Cloud workflow automation
- Modify an Azure policy definition
- Update an Azure policy assignment

Answer Area:

Answer Area

To enforce compliance to the regulatory standard, create:

- An Azure Automation account
- A blueprint
- A managed identity
- Workflow automation

To exclude TestRG from the compliance assessment:

- Edit an Azure blueprint
- Modify a Defender for Cloud workflow automation
- Modify an Azure policy definition
- Update an Azure policy assignment

Section:

Explanation:

Box 1 = A Blueprint

Box 2 = Update an Azure Policy assignment

<https://learn.microsoft.com/en-us/azure/governance/policy/tutorials/create-and-manage#update-assignment-with-exclusion> [https://docs.microsoft.com/en-us/azure/governance/policy/concepts/definition-structurewhile it is in policy assignment-https://docs.microsoft.com/en-us/azure/governance/policy/concepts/assignment-structure](https://docs.microsoft.com/en-us/azure/governance/policy/concepts/definition-structurewhile-it-is-in-policy-assignment-https://docs.microsoft.com/en-us/azure/governance/policy/concepts/assignment-structure)

