SC-100 Q&As

Microsoft Cybersecurity Architect

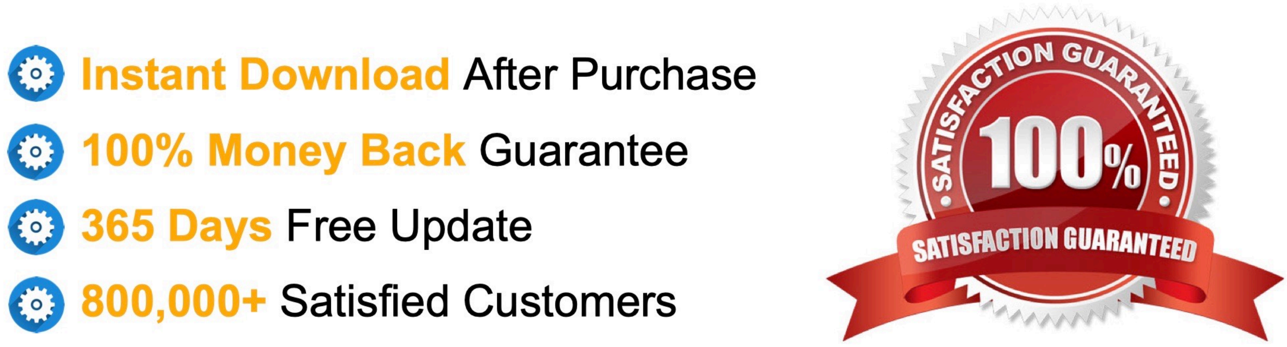
Pass Microsoft SC-100 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

https://www.leads4pass.com/sc-100.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Microsoft Official Exam Center


Instant Download After Purchase
100% Money Back Guarantee
365 Days Free Update
800,000+ Satisfied Customers
SATISFACTION GUARANTEED 100%
SATISFACTION GUARANTEED

QUESTION 1

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

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

You plan to remove all the domain accounts from the Administrators groups on the Windows computers.

You need to recommend a solution that will provide users with administrative access to the Windows computers only when access is required. The solution must minimize the lateral movement of ransomware attacks if an administrator

account on a computer is compromised.

What should you include in the recommendation?

A. Local Administrator Password Solution (LAPS)

B. Azure AD Identity Protection

C. Azure AD Privileged Identity Management (PIM)

D. Privileged Access Workstations (PAWs)

Correct Answer: A

Microsoft\\'s "Local Administrator Password Solution" (LAPS) provides management of local administrator account passwords for domain-joined computers. Passwords are randomized and stored in Active Directory (AD), protected by ACLs, so only eligible users can read it or request its reset.

Microsoft LAPS is short for Microsoft Local Administrator Password Solution. When installed and enabled on domain-joined computers it takes over the management of passwords of local accounts. Passwords are automatically changed to random characters that meet the domain\\'s password policy requirements at a frequency that you define through Group Policy.

The passwords are stored in a protected “confidential” attribute on the Computer object in AD. Unlike most other attributes which can be read by all domain users by default, the confidential attributes require extra privileges to be granted in order to read them, thus securing the managed passwords.

Incorrect: Not B: Integrate on-premises Active Directory domains with Azure Active Directory Validate security configuration and policy, Actively monitor Azure AD for signs of suspicious activity

Consider using Azure AD Premium P2 edition, which includes Azure AD Identity Protection. Identity Protection uses adaptive machine learning algorithms and heuristics to detect anomalies and risk events that may indicate that an identity has been compromised. For example, it can detect potentially unusual activity such as irregular sign-in activities, sign-ins from unknown sources or from IP addresses with suspicious activity, or sign-ins from devices that may be infected. Identity Protection uses this data to generate reports and alerts that enable you to investigate these risk events and take appropriate action.

Not C: Azure AD PIM is a service in Azure AD that enables you to manage, control, and monitor access to resources in Azure AD, Azure, and other Microsoft Online Services such as Microsoft 365 or Microsoft Intune.

Not D: Privileged Access Workstations (PAWs) provide a dedicated operating system for sensitive tasks that is protected from Internet attacks and threat vectors. Separating these sensitive tasks and accounts from the daily use workstations and devices provides very strong protection from phishing attacks, application and OS vulnerabilities, various impersonation attacks, and credential theft attacks such as keystroke logging, Pass-the-Hash, and Pass-The-Ticket.

Reference: https://craighays.com/microsoft-laps/ https://learn.microsoft.com/en-us/azure/architecture/reference-architectures/identity/azure-ad

QUESTION 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. access reviews in Azure AD

C. Microsoft Defender for Cloud

D. Microsoft Defender for Cloud Apps

E. Microsoft Defender for Endpoint

Correct Answer: BD

Scenario: Litware identifies the following application security requirements:

Monitor and control access to Microsoft SharePoint Online and Exchange Online data in real time.

B: Azure Active Directory (Azure AD) access reviews enable organizations to efficiently manage group memberships, access to enterprise applications, and role assignments. User\\'s access can be reviewed on a regular basis to make sure only the right people have continued access.

D: The Defender for Cloud Apps framework Discover and control the use of Shadow IT: Identify the cloud apps, IaaS, and PaaS services used by your organization. Investigate usage patterns, assess the risk levels and business readiness of more than 25,000 SaaS apps against more than 80 risks. Start managing them to ensure security and compliance.

Protect your sensitive information anywhere in the cloud: Understand, classify, and protect the exposure of sensitive information at rest. Leverage out-of-the box policies and automated processes to apply controls in real time across all your cloud apps.

Etc.

Reference: https://docs.microsoft.com/en-us/azure/active-directory/governance/access-reviews-overview https://docs.microsoft.com/en-us/defender-cloud-apps/what-is-defender-for-cloud-apps

QUESTION 3

You have 50 Azure subscriptions.

You need to monitor the 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.

What are two ways to achieve the goal? Each correct answer presents a complete solution.

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: AF

An Azure Management group is logical containers that allow Azure Administrators to manage access, policy, and compliance across multiple Azure Subscriptions en masse.

If your organization has many Azure subscriptions, you may need a way to efficiently manage access, policies, and compliance for those subscriptions. Management groups provide a governance scope above subscriptions. You organize subscriptions into management groups the governance conditions you apply cascade by inheritance to all associated subscriptions.

F: Blueprint definition locations

When creating a blueprint definition, you\\'ll define where the blueprint is saved. Blueprints can be saved to a management group or subscription that you have Contributor access to. If the location is a management group, the blueprint is

available to assign to any child subscription of that management group.

A: Create and assign an initiative definition

With an initiative definition, you can group several policy definitions to achieve one overarching goal. An initiative evaluates resources within scope of the assignment for compliance to the included policies.

Note: The Azure Policy Regulatory Compliance built-in initiative definition maps to compliance domains and controls in ISO 27001:2013.

The Azure Policy control mapping provides details on policy definitions included within this blueprint and how these policy definitions map to the compliance domains and controls in ISO 27001. When assigned to an architecture, resources

are evaluated by Azure Policy for non-compliance with assigned policy definitions.

Incorrect:

Not B, D, E: If you plan to apply this policy definition to multiple subscriptions, the location must be a management group that contains the subscriptions you assign the policy to. The same is true for an initiative definition.

Reference: 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 4

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

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Need to use customer-managed keys instead.

Note: Automated key rotation in Key Vault allows users to configure Key Vault to automatically generate a new key version at a specified frequency. You can use rotation policy to configure rotation for each individual key. Our recommendation is to rotate encryption keys at least every two years to meet cryptographic best practices. This feature enables end-to-end zero-touch rotation for encryption at rest for Azure services with customer-managed key (CMK) stored in Azure Key Vault. Please refer to specific Azure service documentation to see if the service covers end

to-end rotation.

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

QUESTION 5

Your company has a Microsoft 365 ES subscription.

The Chief Compliance Officer plans to enhance privacy management in the working environment.

You need to recommend a solution to enhance the privacy management. The solution must meet the following requirements:

1.

Identify unused personal data and empower users to make smart data handling decisions.

2.

Provide users with notifications and guidance when a user sends personal data in Microsoft Teams.

3.

Provide users with recommendations to mitigate privacy risks. What should you include in the recommendation?

A. communication compliance in insider risk management

B. Microsoft Viva Insights

C. Privacy Risk Management in Microsoft Priva

D. Advanced eDiscovery

Correct Answer: C

Privacy Risk Management in Microsoft Priva gives you the capability to set up policies that identify privacy risks in your Microsoft 365 environment and enable easy remediation. Privacy Risk Management policies are meant to be internal

guides and can help you:

Detect overexposed personal data so that users can secure it.

Spot and limit transfers of personal data across departments or regional borders.

Help users identify and reduce the amount of unused personal data that you store.

Incorrect:

Not B: Microsoft Viva Insights provides personalized recommendations to help you do your best work. Get insights to build better work habits, such as following through on commitments made to collaborators and protecting focus time in the

day for uninterrupted, individual work.

Not D: The Microsoft Purview eDiscovery (Premium) solution builds on the existing Microsoft eDiscovery and analytics capabilities. eDiscovery (Premium) provides an end-to-end workflow to preserve, collect, analyze, review, and export

content that\\'s responsive to your organization\\'s internal and external investigations.

Reference: https://docs.microsoft.com/en-us/privacy/priva/risk-management

QUESTION 6

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 Firewall, 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

Correct Answer: A

Explanation:

About Azure Bastion host and jumpboxes

The most simple solution is to host a jumpbox on the virtual network of the data management landing zone or data landing zone to connect to the data services through private endpoints.

Azure Bastion provides a few other core security benefits, including:

*

The service integrates with native security appliances for an Azure virtual network, such as Azure Firewall.

Note:

*

Platform landing zones: Subscriptions deployed to provide centralized services, often operated by a central team, or a number of central teams split by function (e.g. networking, identity), which will be used by various workloads and applications. Platform landing zones represent key services that often benefit from being consolidated for efficiency and ease of operations. Examples include networking, identity, and management services.

*

The Azure App Service landing zone accelerator is an open-source collection of architectural guidance and reference implementation to accelerate deployment of Azure App Service at scale. It can provide a specific architectural approach and reference implementation via infrastructure as code templates to prepare your landing zones. The landing zones adhere to the architecture and best practices of the Cloud Adoption Framework.

Incorrect:

Not B: The Azure Well-Architected Framework is a set of guiding tenets that can be used to improve the quality of a workload. The framework consists of five pillars of architectural excellence:

Reliability Security Cost Optimization Operational Excellence Performance Efficiency

Not C: The Azure Security Benchmark (ASB) provides prescriptive best practices and recommendations to help improve the security of workloads, data, and services on Azure. This benchmark is part of a set of holistic security guidance that also includes:

*

Cloud Adoption Framework: Guidance on security, including strategy, roles and responsibilities, Azure Top 10 Security Best Practices, and reference implementation.

*

Azure Well-Architected Framework: Guidance on securing your workloads on Azure.

*

Microsoft Security Best Practices: Recommendations with examples on Azure.

Microsoft Cybersecurity Reference Architectures (MCRA): Visual diagrams and guidance for security components and relationships

*

The Azure Security Benchmark focuses on cloud-centric control areas. These controls are consistent with well-known security benchmarks, such as those described by the Center for Internet Security (CIS) Controls, National Institute of

Standards and Technology (NIST), and Payment Card Industry Data Security Standard (PCI-DSS).

Reference:

https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/scenarios/cloud-scale-analytics/architectures/connect-to-environments-privately

https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/ready/landing-zone/

https://learn.microsoft.com/en-us/security/benchmark/azure/overview-v3

https://learn.microsoft.com/en-us/azure/architecture/framework/

QUESTION 7

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:

1.

Windows 11 devices managed by Microsoft Intune

2.

Azure Storage accounts

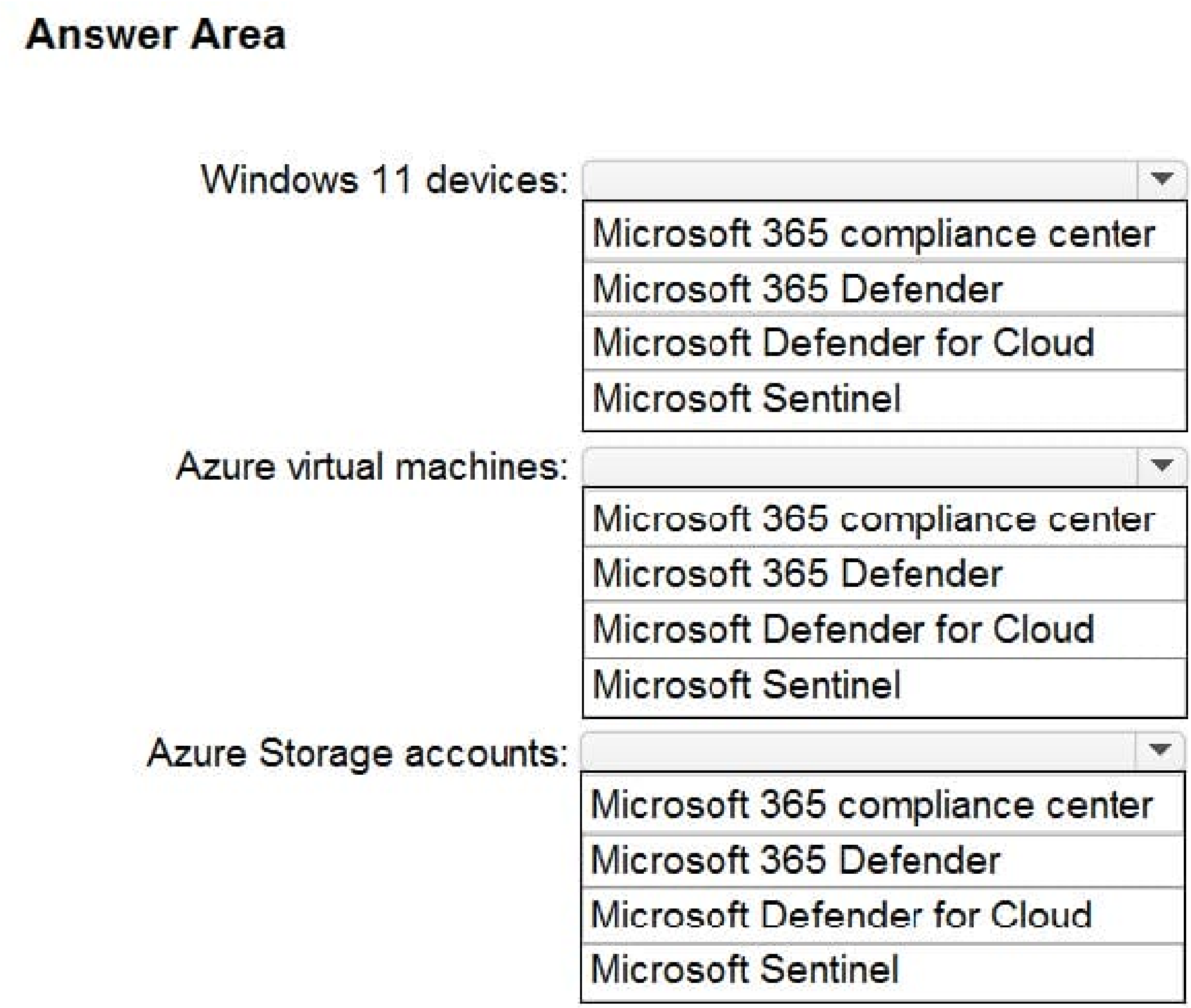
3.

Azure virtual machines

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

NOTE: Each correct selection is worth one point.

Hot Area:



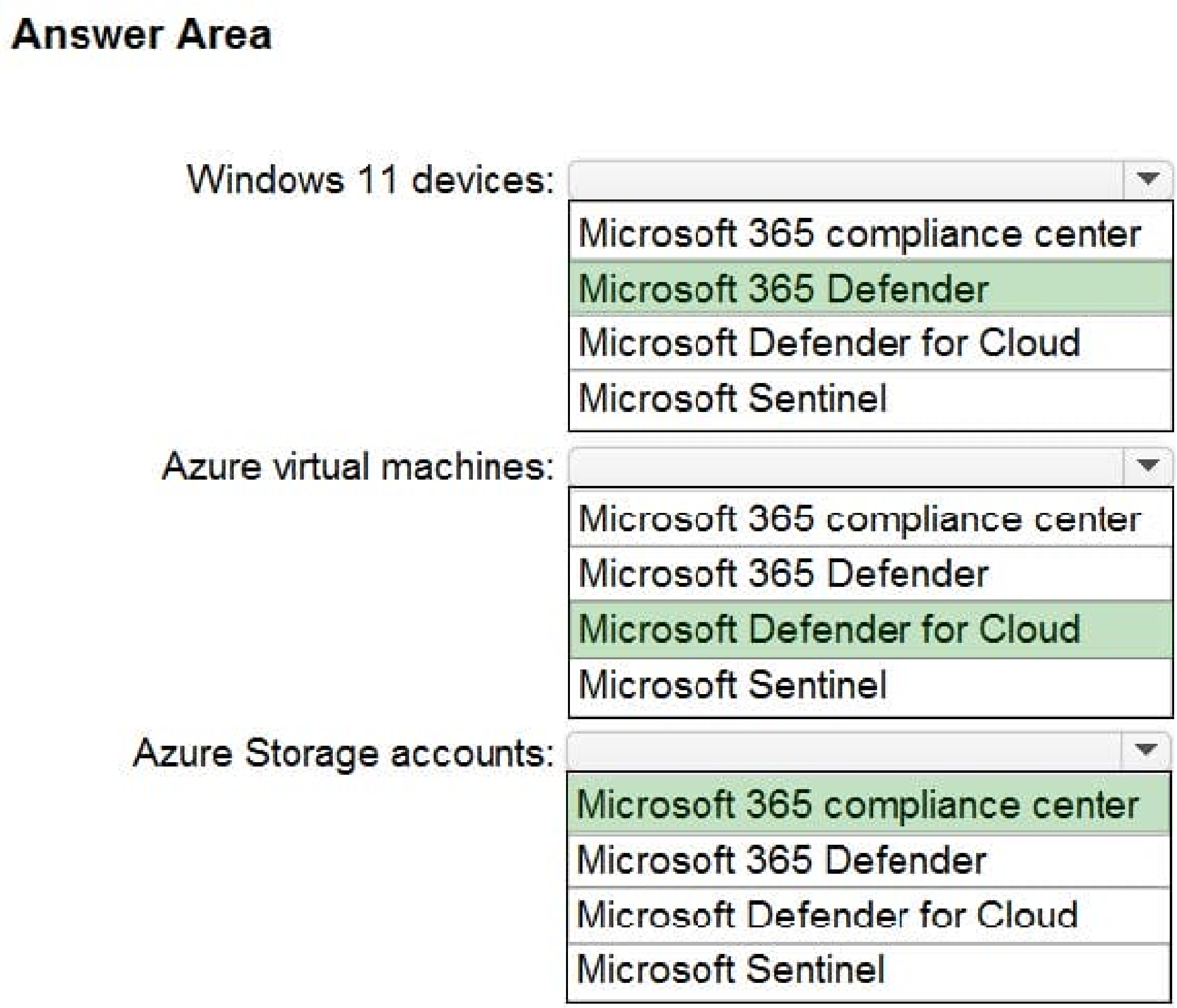
Answer Area

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

Correct Answer:



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

Box 1: Microsoft 365 Defender

The Microsoft 365 Defender portal emphasizes quick access to information, simpler layouts, and bringing related information together for easier use. It includes Microsoft Defender for Endpoint.

Microsoft Defender for Endpoint is an enterprise endpoint security platform designed to help enterprise networks prevent, detect, investigate, and respond to advanced threats.

You can integrate Microsoft Defender for Endpoint with Microsoft Intune as a Mobile Threat Defense solution. Integration can help you prevent security breaches and limit the impact of breaches within an organization.

Microsoft Defender for Endpoint works with devices that run:

Android

iOS/iPadOS

Windows 10

Windows 11

Box 2: Microsoft Defender for Cloud

Microsoft Defender for Cloud currently protects Azure Blobs, Azure Files and Azure Data Lake Storage Gen2 resources. Microsoft Defender for SQL on Azure price applies to SQL servers on Azure SQL Database, Azure SQL Managed

Instance and Azure Virtual Machines.

Box 3: Microsoft 365 Compliance Center

Azure Storage Security Assessment: Microsoft 365 Compliance Center monitors and recommends encryption for Azure Storage, and within a few clicks customers can enable built-in encryption for their Azure Storage Accounts.

Note: Microsoft 365 compliance is now called Microsoft Purview and the solutions within the compliance area have been rebranded.

Microsoft Purview can be setup to manage policies for one or more Azure Storage accounts.

Reference: https://docs.microsoft.com/en-us/azure/purview/tutorial-data-owner-policies-storage

https://docs.microsoft.com/en-us/microsoft-365/security/defender/microsoft-365-defender?

https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/microsoft-defender-endpoint

https://azure.microsoft.com/en-gb/pricing/details/defender-for-cloud/

QUESTION 8

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 automatical 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

https://azure.microsoft.com/en-us/blog/simplifying-your-environment-setup-while-meeting-compliance-needs-with-built-in-azure-blueprints/

QUESTION 9

You have a Microsoft 365 subscription.

You need to design a solution to block file downloads from Microsoft SharePoint Online by authenticated users on unmanaged devices.

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

NOTE: Each correct selection is worth one point.

A. Azure AD Conditional Access

B. Azure Data Catalog

C. Microsoft Purview Information Protection

D. Azure AD Application Proxy

E. Microsoft Defender for Cloud Apps

Correct Answer: AE

Explanation:

Blocking or limiting access on unmanaged devices relies on Azure AD conditional access policies.

Create a block download policy for unmanaged devices

Defender for Cloud Apps session policies allow you to restrict a session based on device state. To accomplish control of a session using its device as a condition, create both a conditional access policy AND a session policy.

Incorrect:

Not B: Azure Data Catalog is an enterprise-wide metadata catalog that makes data asset discovery straightforward. It\\'s a fully-managed service that lets you — from analyst to data scientist to data developer — register, enrich, discover,

understand, and consume data sources.

Not C: Implement capabilities from Microsoft Purview Information Protection (formerly Microsoft Information Protection) to help you discover, classify, and protect sensitive information wherever it lives or travels.

Reference:

https://learn.microsoft.com/en-us/sharepoint/control-access-from-unmanaged-devices

https://learn.microsoft.com/en-us/defender-cloud-apps/use-case-proxy-block-session-aad

QUESTION 10

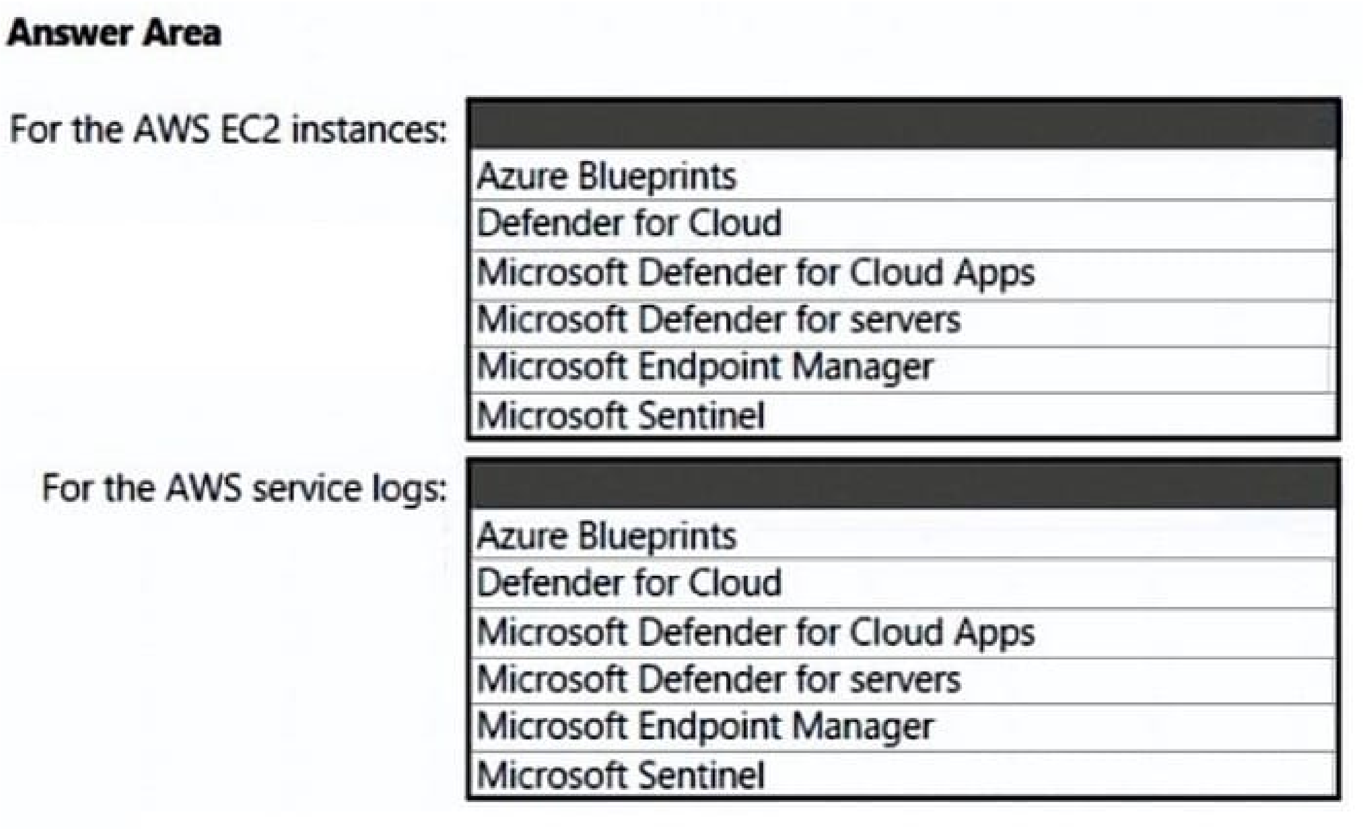
HOTSPOT

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

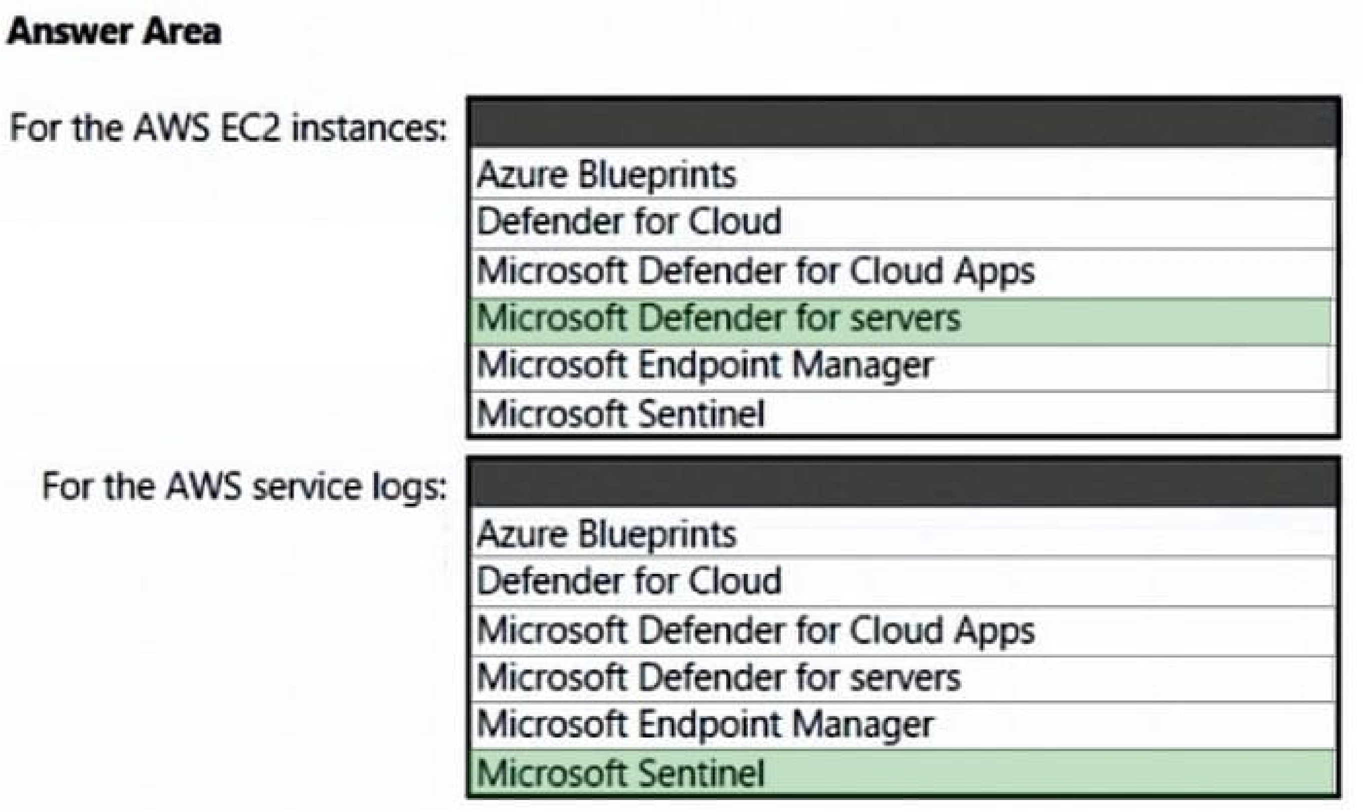
For the AWS EC2 instances:

- 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

Correct Answer:



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]

Box 1: Microsoft Defender for servers

Scenario: Notify security administrators at Fabrikam if any AWS EC2 instances are noncompliant with secure score recommendations.

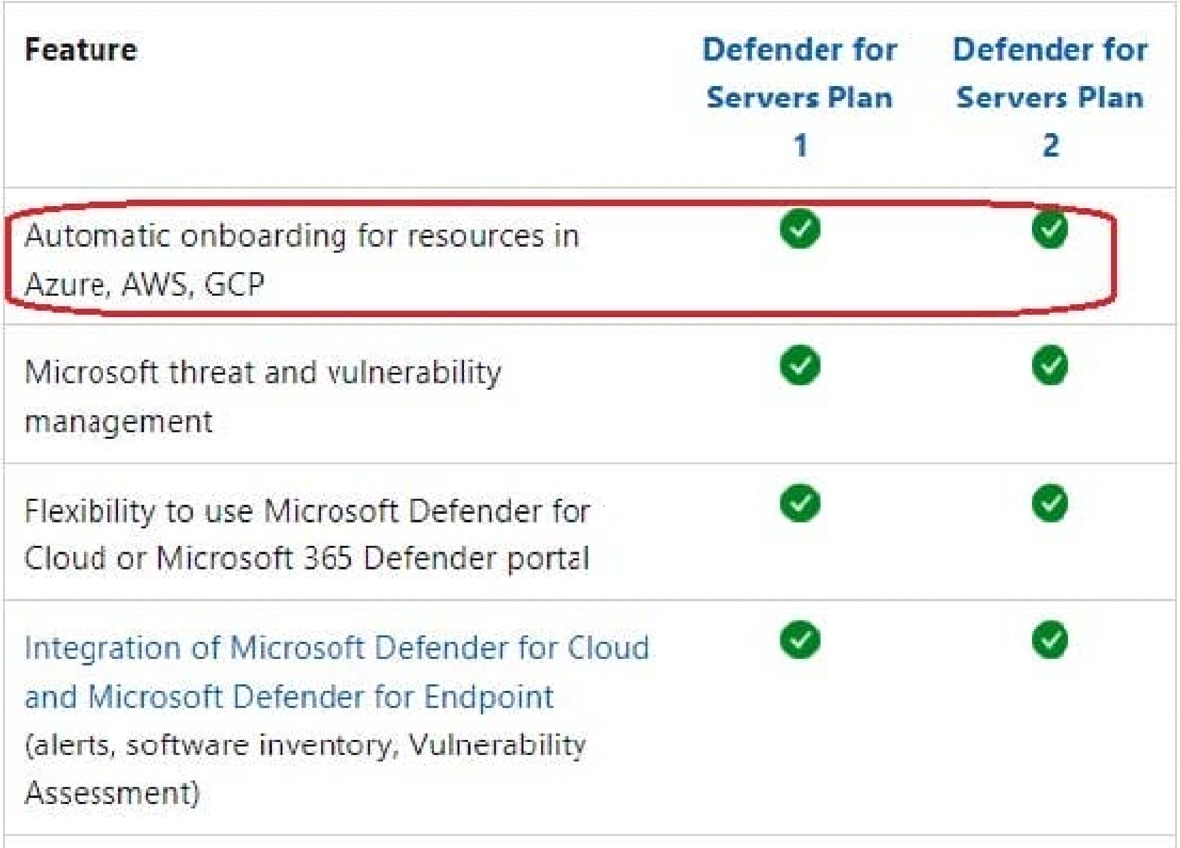
Defender for Servers is one of the enhanced security features available in Microsoft Defender for Cloud. You can use it to add threat detection and advanced defenses to your Windows and Linux machines that exist in hybrid and multicloud

environments.

Available Defender for Server plans

Defender for Servers offers you a choice between two paid plans.

Both include automatic onboarding for resources in Azure, AWS, GCP.



Feature	Defender for Servers Plan 1	Defender for Servers Plan 2
Automatic onboarding for resources in Azure, AWS, GCP	✓	✓
Microsoft threat and vulnerability management	✓	✓
Flexibility to use Microsoft Defender for Cloud or Microsoft 365 Defender portal	✓	✓
Integration of Microsoft Defender for Cloud and Microsoft Defender for Endpoint (alerts, software inventory, Vulnerability Assessment)	✓	✓

Plan 1 includes the following benefits:

Automatic onboarding for resources in Azure, AWS, GCP

Microsoft threat and vulnerability management

Flexibility to use Microsoft Defender for Cloud or Microsoft 365 Defender portal

A Microsoft Defender for Endpoint subscription that includes access to alerts, software inventory, Vulnerability Assessment and an automatic integration with Microsoft Defender for Cloud.

Plan 2 includes everything in Plan 1 plus some additional benefits.

Box 2: Microsoft Sentinel

Scenario: AWS Requirements

Fabrikam identifies the following security requirements for the data hosted in ContosoAWS1:

Ensure that the security administrators can query AWS service logs directly from the Azure environment.

Use the Amazon Web Services (AWS) connectors to pull AWS service logs into Microsoft Sentinel.

Note: These connectors work by granting Microsoft Sentinel access to your AWS resource logs. Setting up the connector establishes a trust relationship between Amazon Web Services and Microsoft Sentinel. This is accomplished on AWS

by creating a role that gives permission to Microsoft Sentinel to access your AWS logs.

Reference: https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-servers-introduction

https://docs.microsoft.com/en-us/azure/defender-for-cloud/recommendations-reference-aws

https://docs.microsoft.com/en-us/azure/sentinel/connect-aws

QUESTION 11

To meet the application security requirements, which two authentication methods must the applications support? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. Security Assertion Markup Language (SAML)

B. NTLMv2

C. certificate-based authentication

D. Kerberos

Correct Answer: AD

A: SAML

Litware identifies the following application security requirements:

Identify internal applications that will support single sign-on (SSO) by using Azure AD Application Proxy.

You can provide single sign-on (SSO) to on-premises applications that are secured with SAML authentication and provide remote access to these applications through Application Proxy. With SAML single sign-on, Azure Active Directory (Azure AD) authenticates to the application by using the user\\'s Azure AD account.

D: You can provide single sign-on for on-premises applications published through Application Proxy that are secured with integrated Windows authentication. These applications require a Kerberos ticket for access. Application Proxy uses Kerberos Constrained Delegation (KCD) to support these applications.

Incorrect:

Not C: Certificate. This is not a custom domain scenario!

If you\\'re using a custom domain, you also need to upload the TLS/SSL certificate for your application.

To configure an on-premises app to use a custom domain, you need a verified Azure Active Directory custom domain, a PFX certificate for the custom domain, and an on-premises app to configure.

Reference:

https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-configure-single-sign-on-on-premises-apps

https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-configure-single-sign-on-with-kcd

https://docs.microsoft.com/en-us/azure/active-directory/app-proxy/application-proxy-configure-custom-domain

---

QUESTION 12

You have an Azure subscription.

You have a DNS domain named contoso.com that is hosted by a third-party DNS registrar.

Developers use Azure DevOps to deploy web apps to App Service Environments. When a new app is deployed, a CNAME record for the app is registered in contoso.com.

You need to recommend a solution to secure the DNS record for each web app. The solution must meet the following requirements:

- Ensure that when an app is deleted, the CNAME record for the app is removed also.

- Minimize administrative effort.

What should you include in the recommendation?

A.

Microsoft Defender for Cloud Apps

B.

Microsoft Defender for DevOps

C.

Microsoft Defender for App Service

D.

Microsoft Defender for DNS

Correct Answer: C

QUESTION 13

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:

1.

Minimizes manual intervention by security operation analysts

2.

Supports triaging alerts within Microsoft Teams channels What should you include in the strategy?

A. KQL

B. playbooks

C. data connectors

D. KQLworkbooks

Correct Answer: B

Playbooks in Microsoft Sentinel are based on workflows built in Azure Logic Apps, a cloud service that helps you schedule, automate, and orchestrate tasks and workflows across systems throughout the enterprise.

A playbook is a collection of these remediation actions that can be run from Microsoft Sentinel as a routine. A playbook can help automate and orchestrate your threat response; it can be run manually or set to run automatically in response to

specific alerts or incidents, when triggered by an analytics rule or an automation rule, respectively.

Incorrect:

Not A: Kusto Query Language is a powerful tool to explore your data and discover patterns, identify anomalies and outliers, create statistical modeling, and more. The query uses schema entities that are organized in a hierarchy similar to

SQL\\'s: databases, tables, and columns.

Not D: Workbooks provide a flexible canvas for data analysis and the creation of rich visual reports within the Azure portal. They allow you to tap into multiple data sources from across Azure, and combine them into unified interactive

experiences.

Workbooks allow users to visualize the active alerts related to their resources.

Reference: https://docs.microsoft.com/en-us/azure/sentinel/automate-responses-with-playbooks

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

QUESTION 14

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. a Microsoft Sentinel data connector

B. Azure Event Hubs

C. a Microsoft Sentinel workbook

D. Azure Data Factory

Correct Answer: A

Microsoft Sentinel Add-On for Splunk allows Azure Log Analytics and Microsoft Sentinel users to ingest security logs from Splunk platform using the Azure HTTP Data Collector API. Reference: https://splunkbase.splunk.com/app/5312/

QUESTION 15

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 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

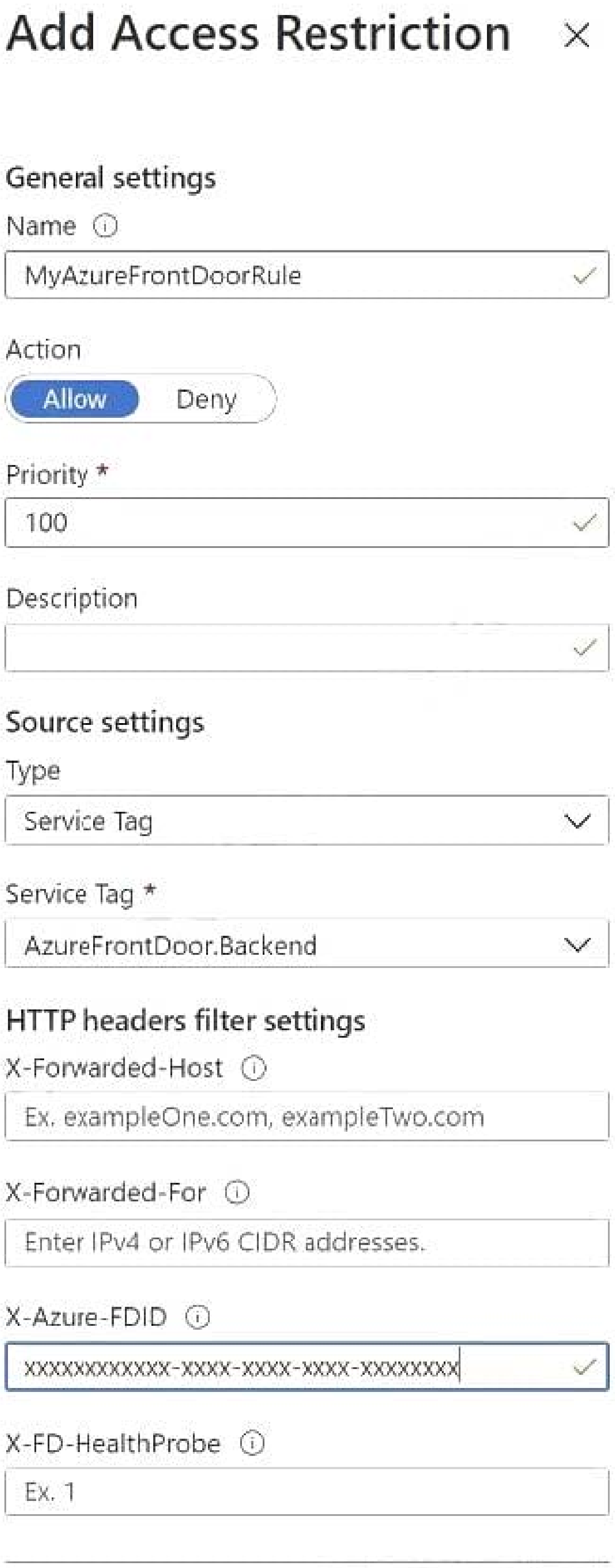
B. No

Correct Answer: A

Restrict access to a specific Azure Front Door instance.

Traffic from Azure Front Door to your application originates from a well-known set of IP ranges defined in the AzureFrontDoor.Backend service tag. Using a service tag restriction rule, you can restrict traffic to only originate from Azure Front

Door. To ensure traffic only originates from your specific instance, you will need to further filter the incoming requests based on the unique http header that Azure Front Door sends.



Add Access Restriction ×

General settings

Name ⓘ

MyAzureFrontDoorRule ✓

Action

● Allow ○ Deny

Priority *

100 ✓

Description

✓

Source settings

Type

Service Tag

Service Tag *

AzureFrontDoor.Backend

HTTP headers filter settings

X-Forwarded-Host ⓘ

Ex. exampleOne.com, exampleTwo.com

X-Forwarded-For ⓘ

Enter IPv4 or IPv6 CIDR addresses.

X-Azure-FDID ⓘ

xxxxxxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxx ✓

X-FD-HealthProbe ⓘ

Ex. 1

Reference: https://docs.microsoft.com/en-us/azure/app-service/app-service-ip-restrictions#managing-access-restriction-rules