SC-100Q&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

QUESTION 1

HOTSPOT

You have a hybrid cloud infrastructure.

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

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

What should you use to meet the requirement of each app? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

Answer Area

App1:

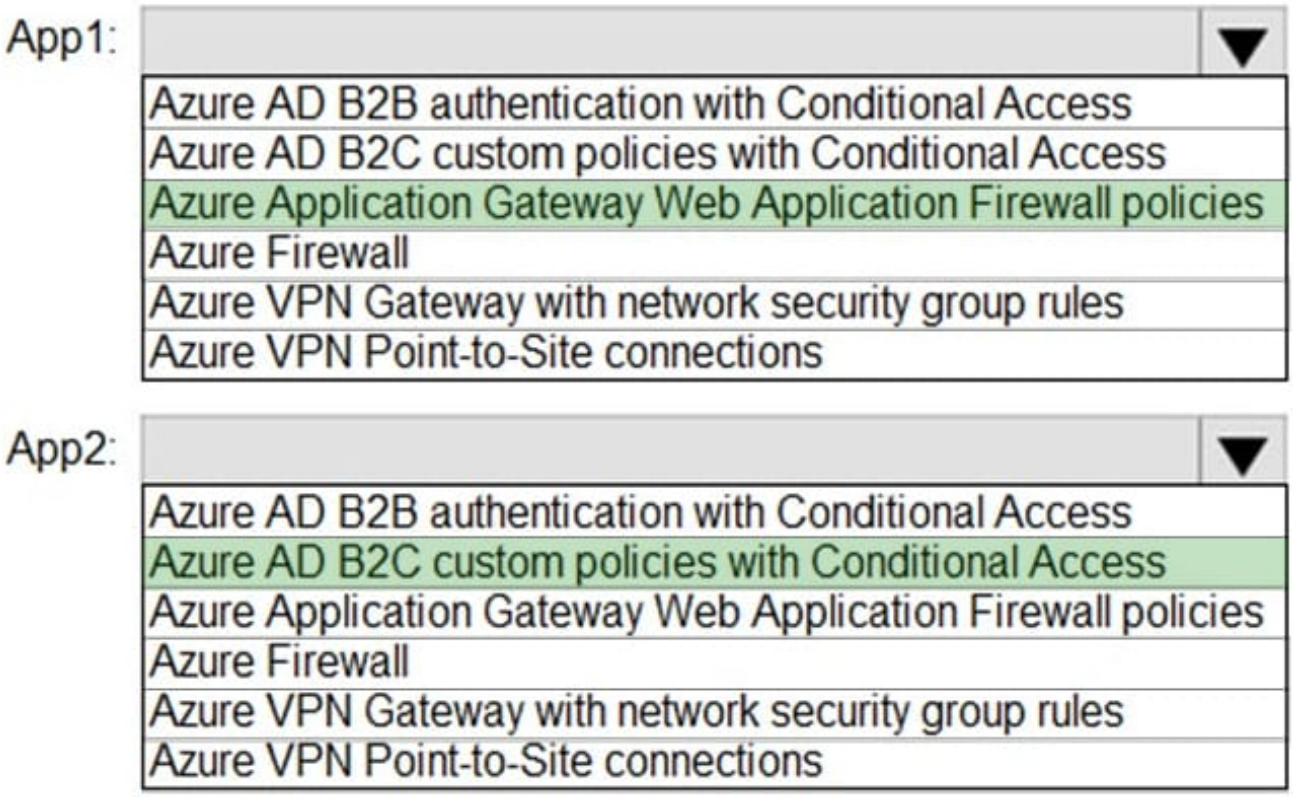
- Azure AD B2B authentication with Conditional Access
- Azure AD B2C custom policies with Conditional Access
- Azure Application Gateway Web Application Firewall policies
- Azure Firewall
- Azure VPN Gateway with network security group rules
- Azure VPN Point-to-Site connections

App2:

- Azure AD B2B authentication with Conditional Access
- Azure AD B2C custom policies with Conditional Access
- Azure Application Gateway Web Application Firewall policies
- Azure Firewall
- Azure VPN Gateway with network security group rules
- Azure VPN Point-to-Site connections

Correct Answer:

Answer Area



Box 1: Azure Application Gateway Web Application Firewall policies

Azure Application Gateway is a web traffic load balancer that enables you to manage traffic to your web applications.

Azure Web Application Firewall is a cloud-native service that protects web apps from common web-hacking techniques such as SQL injection and security vulnerabilities such as cross-site scripting.

Box 2: Azure Active Directory B2C with Conditional Access

You can set up sign-up and sign-in with a LinkedIn account using Azure Active Directory B2C.

You can enhance the security of Azure Active Directory B2C (Azure AD B2C) with Azure AD Identity Protection and Conditional Access. Incorrect:

* Azure VPN Gateway with network security group rules NSGs cannot protect against XSS.

Reference: https://learn.microsoft.com/en-us/azure/application-gateway/overview https://azure.microsoft.com/en-us/products/web-application-firewall/#overview https://learn.microsoft.com/en-us/azure/active-directory-b2c/identity-provider-linkedin

QUESTION 2

You are designing the security standards for a new Azure environment.

You need to design a privileged identity strategy based on the Zero Trust model.

Which framework should you follow to create the design?

A. Enhanced Security Admin Environment (ESAE)

B. Microsoft Security Development Lifecycle (SDL)

C. Rapid Modernization Plan (RaMP)

D. Microsoft Operational Security Assurance (OSA)

Correct Answer: C

RaMP initiatives for Zero Trust.

To rapidly adopt Zero Trust in your organization, RaMP offers technical deployment guidance organized in these initiatives.

In particular, meet these deployment objectives to protect your privileged identities with Zero Trust.

1.

Deploy secured privileged access to protect administrative user accounts.

2.

Deploy Azure AD Privileged Identity Management (PIM) for a time-bound, just-in-time approval process for the use of privileged user accounts.

Note 1: RaMP guidance takes a project management and checklist approach:

* User access and productivity

1. Explicitly validate trust for all access requests Identities Endpoints (devices) Apps Network

* Data, compliance, and governance

2.

Ransomware recovery readiness

3.

Data

* Modernize security operations

4.

Streamline response

5.

Unify visibility

6.

Reduce manual effort

Note 2: As an alternative to deployment guidance that provides detailed configuration steps for each of the technology pillars being protected by Zero Trust principles, Rapid Modernization Plan (RaMP) guidance is based on initiatives and

gives you a set of deployment paths to more quickly implement key layers of protection.

By providing a suggested mapping of key stakeholders, implementers, and their accountabilities, you can more quickly organize an internal project and define the tasks and owners to drive them to conclusion.

By providing a checklist of deployment objectives and implementation steps, you can see the bigger picture of infrastructure requirements and track your progress.

Incorrect:

Not B: Enhanced Security Admin Environment (ESAE)

The Enhanced Security Admin Environment (ESAE) architecture (often referred to as red forest, admin forest, or hardened forest) is an approach to provide a secure environment for Windows Server Active Directory (AD) administrators.

Microsoft\\'s recommendation to use this architectural pattern has been replaced by the modern privileged access strategy and rapid modernization plan (RAMP) guidance as the default recommended approach for securing privileged users.

The ESAE hardened administrative forest pattern (on-prem or cloud-based) is now considered a custom configuration suitable only for exception cases listed below.

What are the valid ESAE use cases?

While not a mainstream recommendation, this architectural pattern is valid in a limited set of scenarios.

In these exception cases, the organization must accept the increased technical complexity and operational costs of the solution. The organization must have a sophisticated security program to measure risk, monitor risk, and apply consistent

operational rigor to the usage and maintenance of the ESAE implementation.

Example scenarios include:

Isolated on-premises environments - where cloud services are unavailable such as offline research laboratories, critical infrastructure or utilities, disconnected operational technology (OT) environments such as Supervisory control and data

acquisition (SCADA) / Industrial Control Systems (ICS), and public sector customers that are fully reliant on on-premises technology.

Highly regulated environments – industry or government regulation may specifically require an administrative forest configuration.

High level security assurance is mandated - organizations with low risk tolerance that are willing to accept the increased complexity and operational cost of the solution.

Reference: https://docs.microsoft.com/en-us/security/zero-trust/zero-trust-ramp-overview

https://docs.microsoft.com/en-us/security/zero-trust/user-access-productivity-validate-trust#identities

https://docs.microsoft.com/en-us/security/compass/esae-retirement

QUESTION 3

You have an Azure subscription.

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

What should you recommend using to enforce the governance requirement?

A. Azure management groups

B. custom Azure roles

C. Azure Policy assignments

D. regulatory compliance standards in Microsoft Defender for Cloud

Correct Answer: C

Explanation:

Azure Policy helps to enforce organizational standards and to assess compliance at-scale.

Common use cases for Azure Policy include implementing governance for resource consistency, regulatory compliance, security, cost, and management. Policy definitions for these common use cases are already available in your Azure

environment as built-ins to help you get started.

Specifically, some useful governance actions you can enforce with Azure Policy include:

Ensuring your team deploys Azure resources only to allowed regions

Enforcing the consistent application of taxonomic tags

Requiring resources to send diagnostic logs to a Log Analytics workspace

Note: Once your business rules have been formed, the policy definition or initiative is assigned to any scope of resources that Azure supports, such as management groups, subscriptions, resource groups, or individual resources. The

assignment applies to all resources within the Resource Manager scope of that assignment.

Reference:

https://learn.microsoft.com/en-us/azure/governance/policy/overview

QUESTION 4

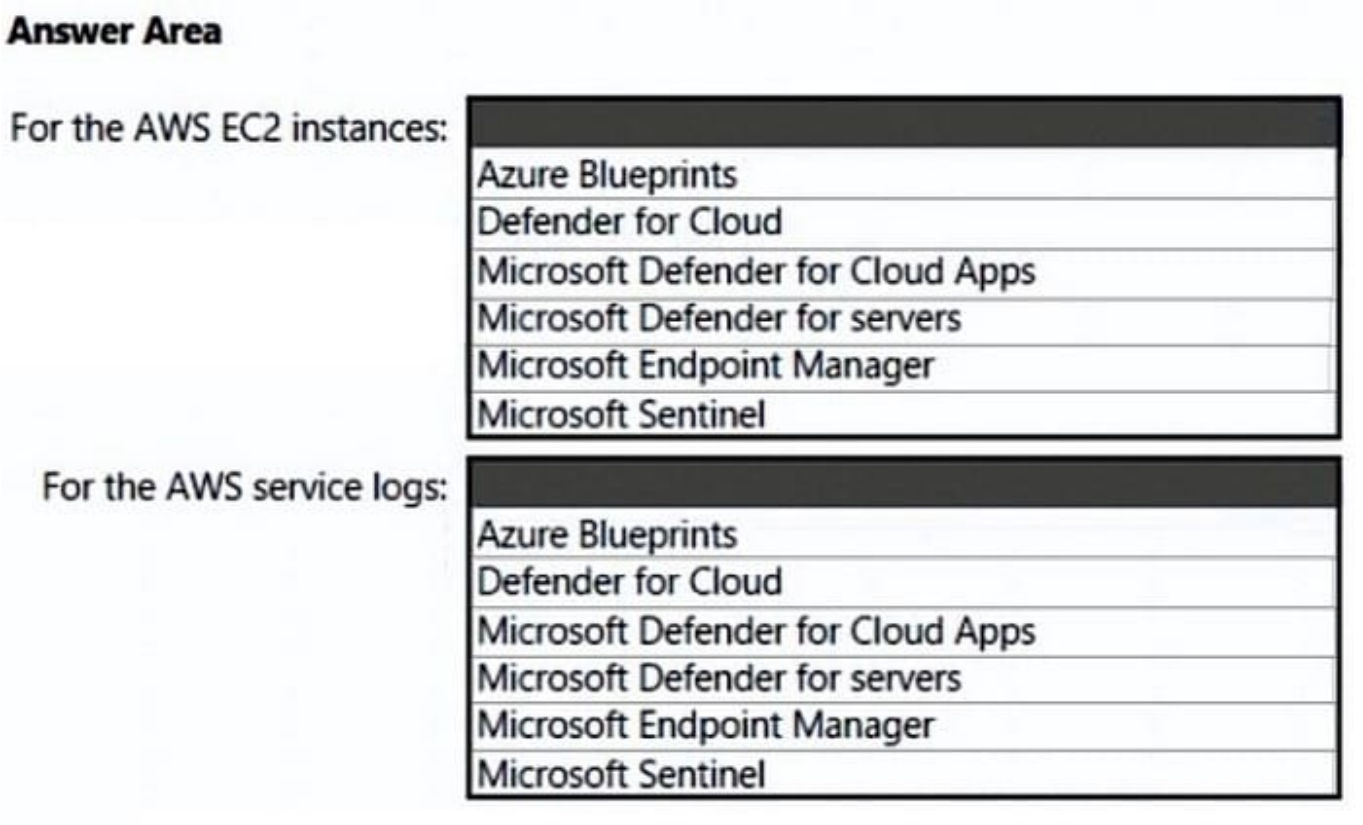
HOTSPOT

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.

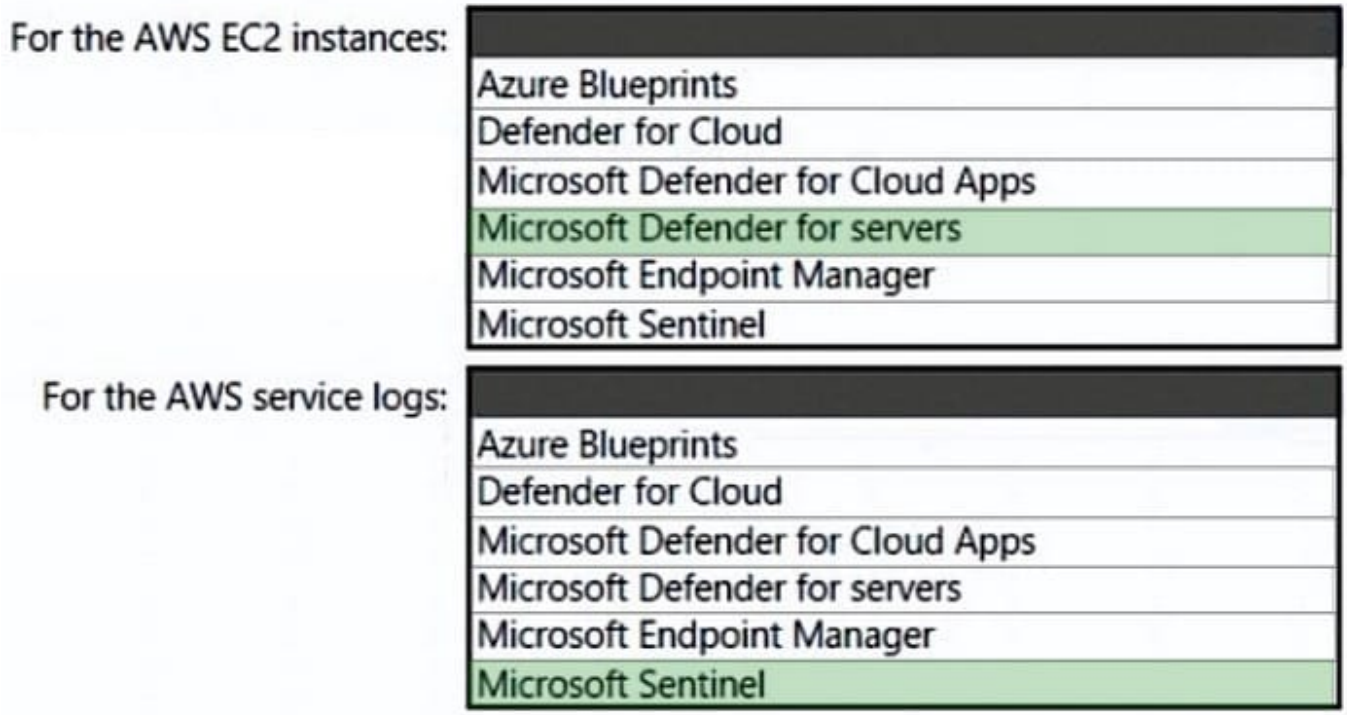
NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:

Answer Area



Box 1: Microsoft Defender for servers

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

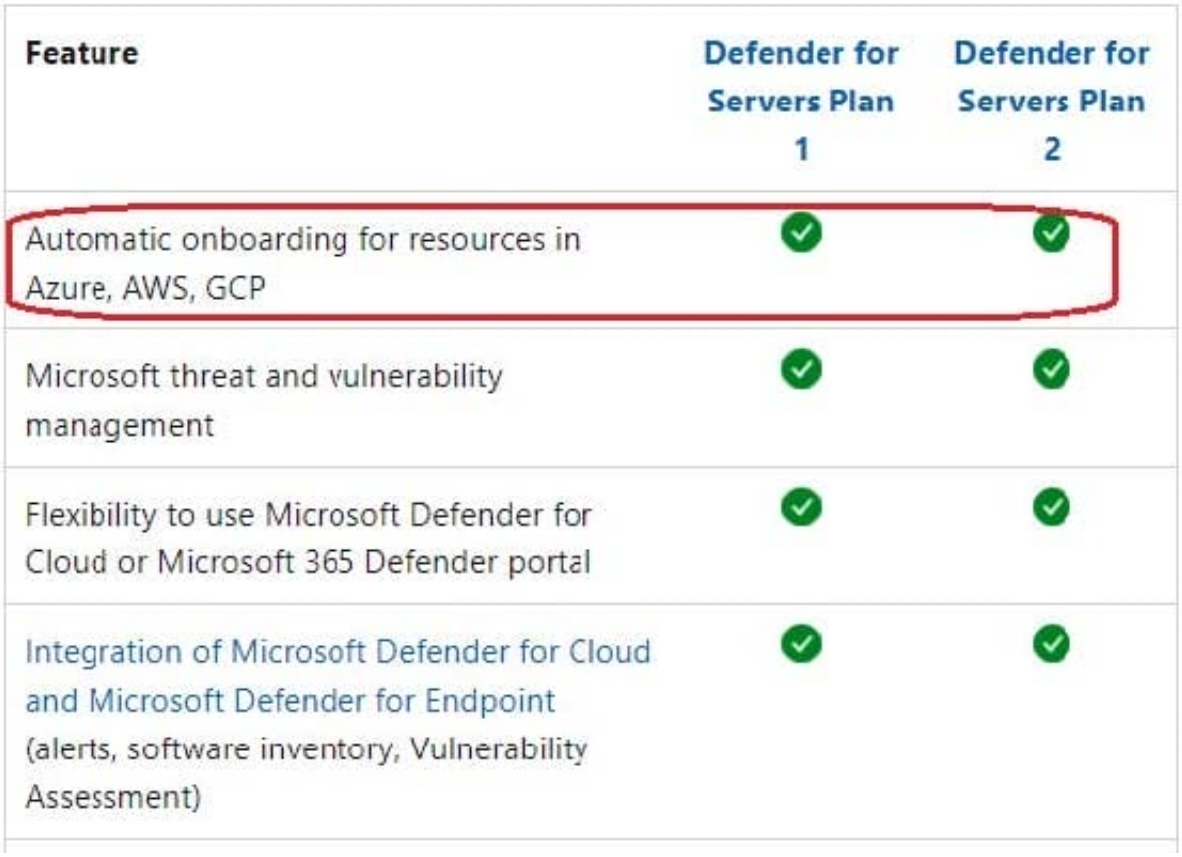
Defender for Servers is one of the enhanced security features available in Microsoft Defender for Cloud. You can use it to add threat detection and advanced defenses to your Windows and Linux machines that exist in hybrid and multicloud

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 5

HOTSPOT

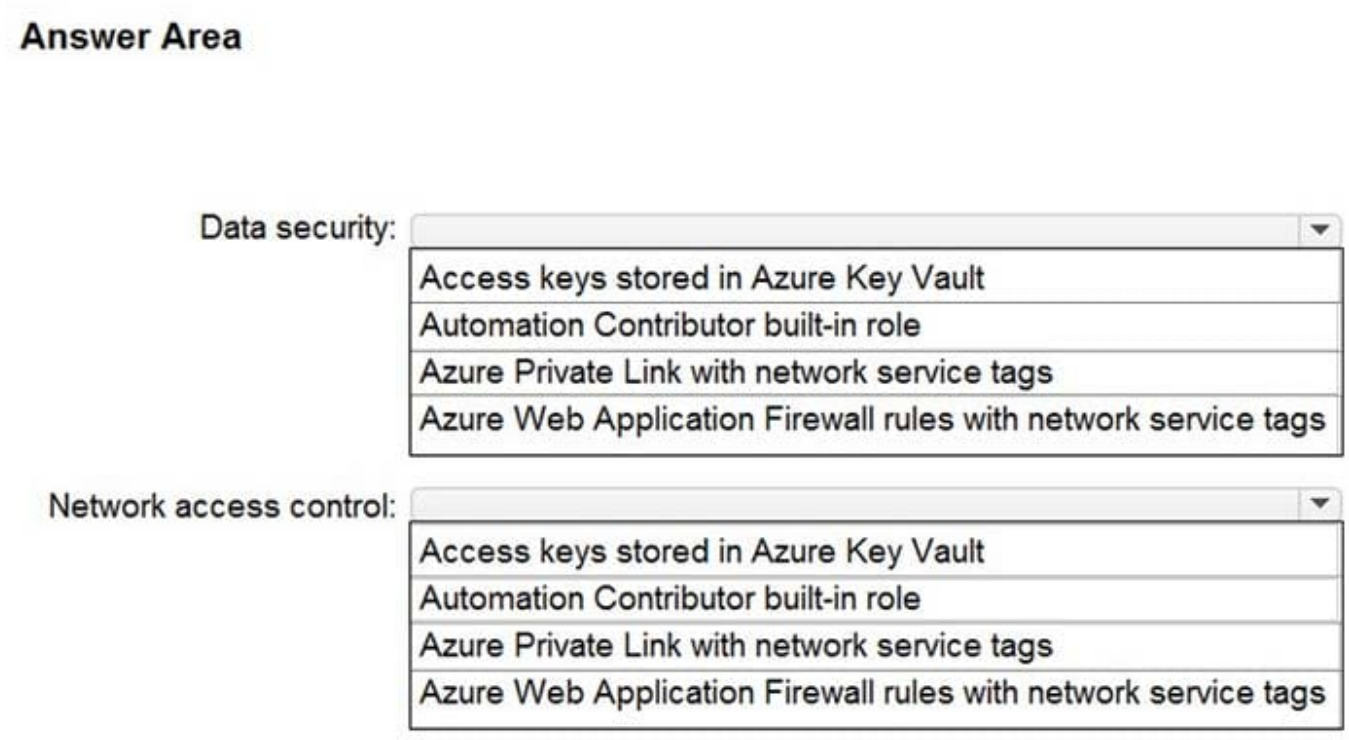
You are designing security for a runbook in an Azure Automation account. The runbook will copy data to Azure Data Lake Storage Gen2.

You need to recommend a solution to secure the components of the copy process.

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

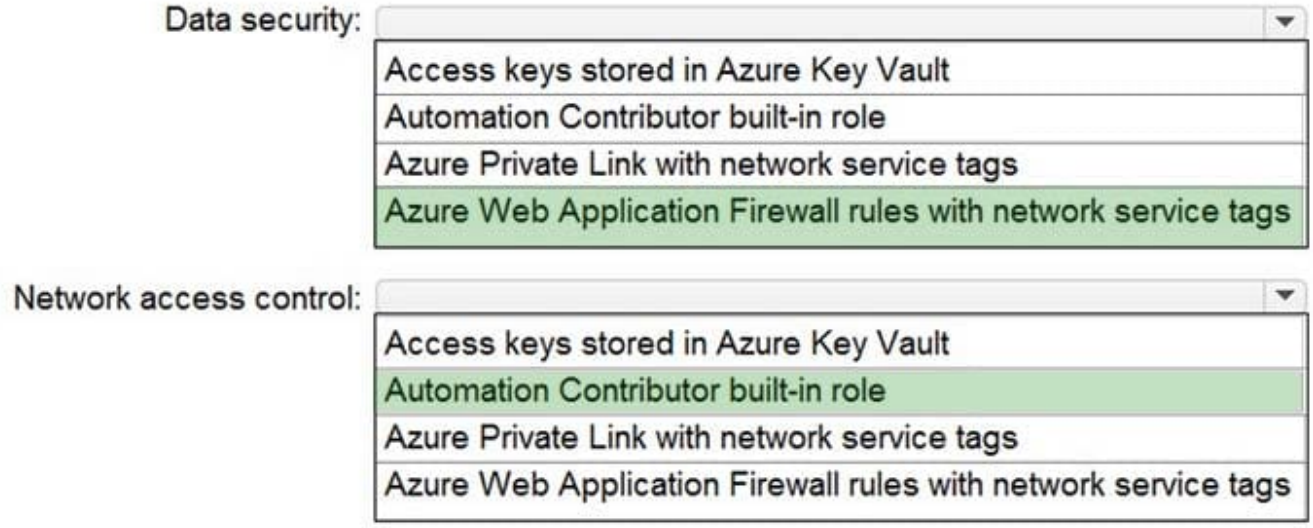
NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:

Answer Area



Box 1: Azure Web Application Firewall with network service tags A service tag represents a group of IP address prefixes from a given Azure service. Microsoft manages the address prefixes encompassed by the service tag and automatically updates the service tag as addresses change, minimizing the complexity of frequent updates to network security rules.

You can use service tags to define network access controls on network security groups, Azure Firewall, and user-defined routes.

Incorrect:

* Not Azure private link with network service tags Network service tags are not used with Private links.

Box 2: Automation Contributor built-in role

The Automation Contributor role allows you to manage all resources in the Automation account, except modifying other user\\'s access permissions to an Automation account.

Reference: https://docs.microsoft.com/en-us/azure/virtual-network/service-tags-overview

https://docs.microsoft.com/en-us/azure/automation/automation-role-based-access-control