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.geekcert.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

QUESTION 1

A customer has a hybrid cloud infrastructure that contains a Microsoft 365 E5 subscription and an Azure subscription.

All 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 solutions to meet the following requirements:

1.

Ensure that the security operations team can access the security logs and the operation logs.

2.

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 solutions should you include in the recommendation? Each correct answer presents a complete solution. NOTE: Each correct selection is worth one point.

A. a custom collector that uses the Log Analytics agent

B. the Azure Monitor agent

C. resource-based role-based access control (RBAC)

D. Azure Active Directory (Azure AD) Conditional Access policies

Correct Answer: BC

A: You can collect data in custom log formats to Microsoft Sentinel with the Log Analytics agent.

Note: You can use the Log Analytics agent to collect data in text files of nonstandard formats from both Windows and Linux computers. Once collected, you can either parse the data into individual fields in your queries or extract the data

during collection to individual fields.

You can connect your data sources to Microsoft Sentinel using custom log formats.

C: Microsoft Sentinel uses Azure role-based access control (Azure RBAC) to provide built-in roles that can be assigned to users, groups, and services in Azure.

Use Azure RBAC to create and assign roles within your security operations team to grant appropriate access to Microsoft Sentinel. The different roles give you fine-grained control over what Microsoft Sentinel users can see and do. Azure

roles can be assigned in the Microsoft Sentinel workspace directly (see note below), or in a subscription or resource group that the workspace belongs to, which Microsoft Sentinel inherits.

Incorrect:

A: You can collect data in custom log formats to Microsoft Sentinel with the Log Analytics agent.

Note: You can use the Log Analytics agent to collect data in text files of nonstandard formats from both Windows and Linux computers. Once collected, you can either parse the data into individual fields in your queries or extract the data during collection to individual fields.

You can connect your data sources to Microsoft Sentinel using custom log formats.

Reference: https://docs.microsoft.com/en-us/azure/azure-monitor/agents/agents-overview https://docs.microsoft.com/en-us/azure/sentinel/connect-custom-logs?tabs=DCG https://docs.microsoft.com/en-us/azure/sentinel/roles

QUESTION 2

HOTSPOT

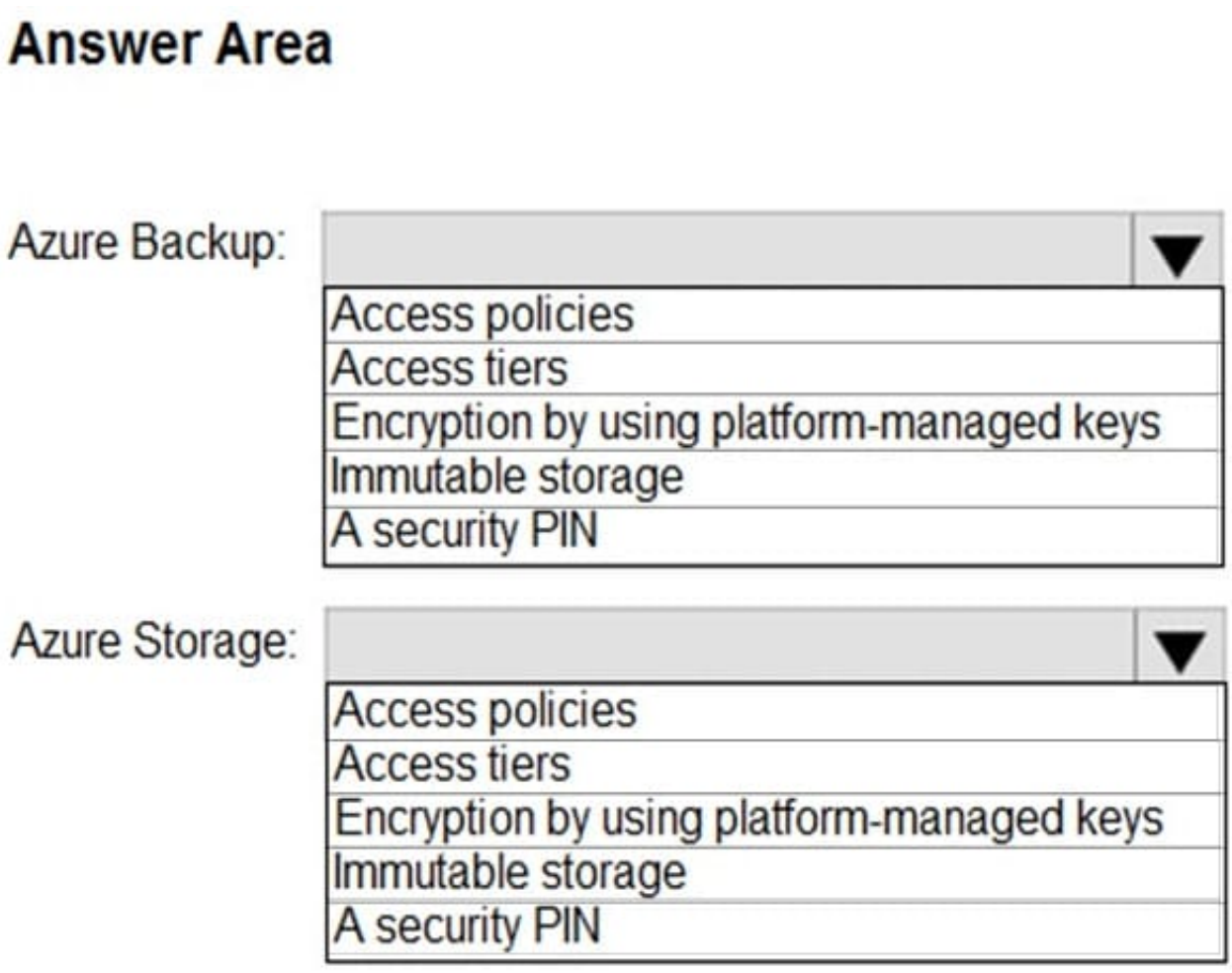
Your company wants to optimize using Azure to protect its resources from ransomware.

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.

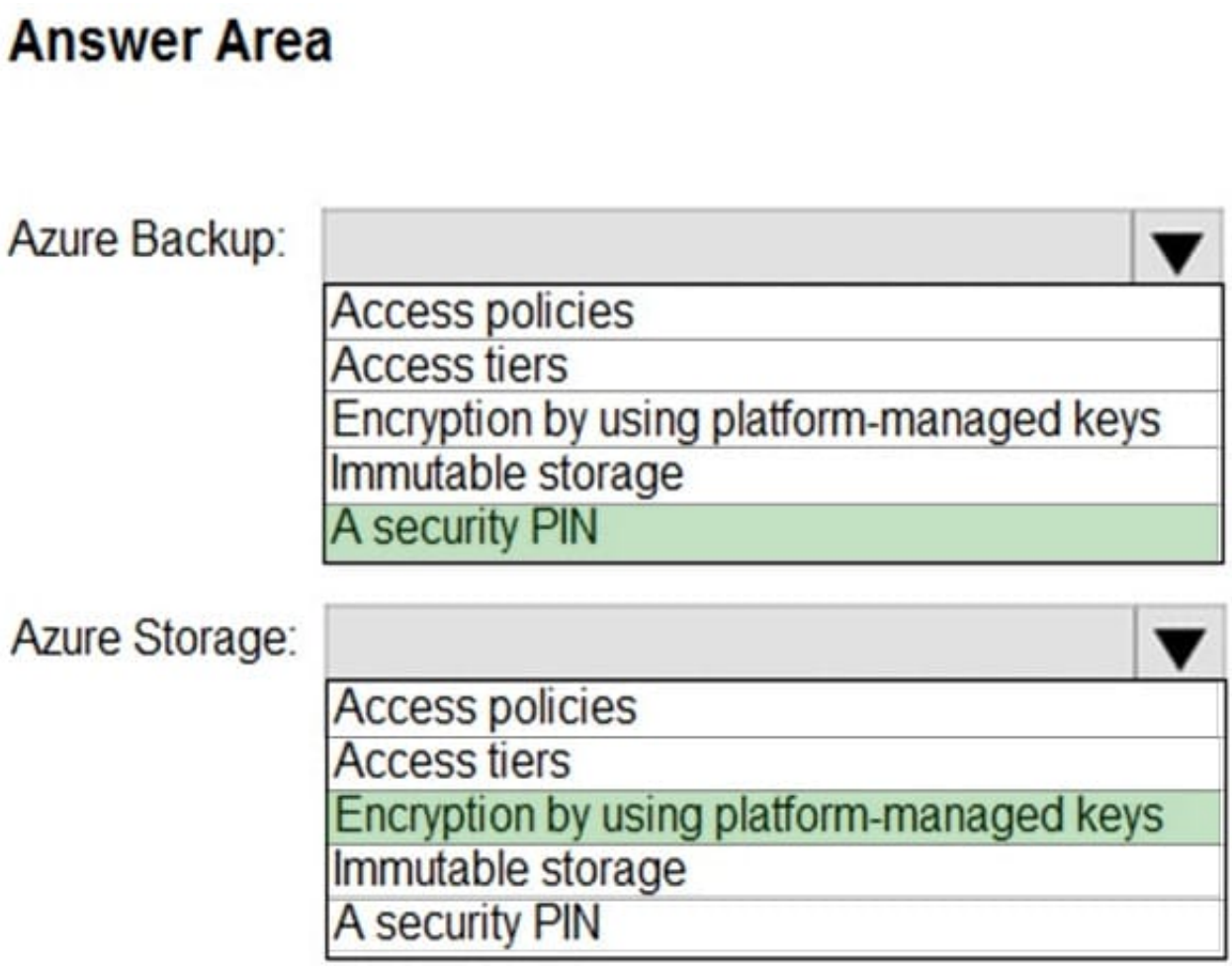
What should you recommend? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



Box 1: A security PIN

Azure Backup

The best way to prevent falling victim to ransomware is to implement preventive measures and have tools that protect your organization from every step that attackers take to infiltrate your systems.

You can reduce your on-premises exposure by moving your organization to a cloud service.

Checks have been added to make sure only valid users can perform various operations. These include adding an extra layer of authentication. As part of adding an extra layer of authentication for critical operations, you\\'re prompted to enter a

security PIN before modifying online backups.

Box 2: Encryption by using platform-managed keys

Ensure backup data is encrypted.

By default, backup data at rest is encrypted using platform-managed keys (PMK). For vaulted backups, you can choose to use customer-managed keys (CMK) to own and manage the encryption keys yourself. Additionally, you can configure

encryption on the storage infrastructure using infrastructure-level encryption, which along with CMK encryption provides double encryption of data at rest.

Reference:

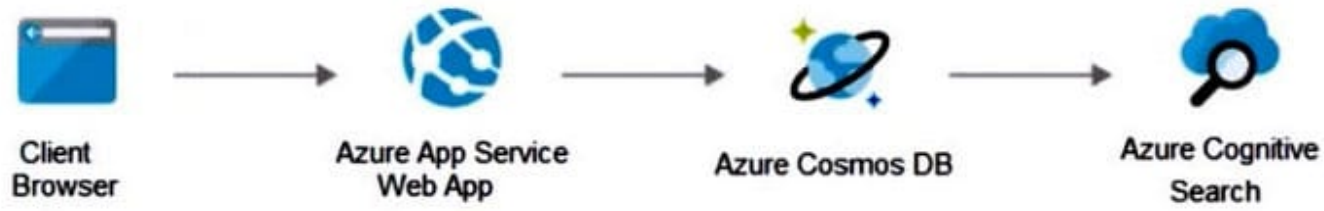
https://learn.microsoft.com/en-us/azure/security/fundamentals/backup-plan-to-protect-against-ransomware

https://learn.microsoft.com/en-us/azure/backup/protect-backups-from-ransomware-faq

QUESTION 3

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.

Your on-premises network contains an e-commerce web app that was developed in Angular and Node,js. The web app uses a MongoDB database. You plan to migrate the web app to Azure. The solution architecture team proposes the following architecture as an Azure landing zone.



You need to provide recommendations to secure the connection between the web app and the database. The solution must follow the Zero Trust model.

Solution: You recommend implementing Azure Key Vault to store credentials.

Does this meet the goal?

A. Yes

B. No

Correct Answer: B

Instead use solution: You recommend creating private endpoints for the web app and the database layer.

Note:

How to Use Azure Private Endpoints to Restrict Public Access to WebApps.

As an Azure administrator or architect, you are sometimes asked the question: “How can we safely deploy internal business applications to Azure App Services?”

These applications characteristically are:

Not accessible from the public internet.

Accessible from within the on-premises corporate network

Accessible via an authorized VPN client from outside the corporate network.

For such scenarios, we can use Azure Private Links, which enables private and secure access to Azure PaaS services over Azure Private Endpoints, along with the Site-to-Site VPN, Point-to-Site VPN, or the Express Route. Azure Private

Endpoint is a read-only network interface service associated with the Azure PAAS Services. It allows you to bring deployed sites into your virtual network, limiting access to them at the network level.

It uses one of the private IP addresses from your Azure VNet and associates it with the Azure App Services. These services are called Private Link resources. They can be Azure Storage, Azure Cosmos DB, SQL, App Services Web App,

your own / partner owned services, Azure Backups, Event Grids, Azure Service Bus, or Azure Automations.

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

QUESTION 4

You have an Azure AD tenant that syncs with an Active Directory Domain Services (AD DS) domain.

You are designing an Azure DevOps solution to deploy applications to an Azure subscription by using continuous integration and continuous deployment (CI/CD) pipelines.

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

What should you recommend?

A. a managed identity in Azure

B. an Azure AD user account that has role assignments in Azure AD Privileged Identity Management (PIM)

C. a group managed service account (gMSA)

D. an Azure AD user account that has a password stored in Azure Key Vault

Correct Answer: D

QUESTION 5

Your company has a hybrid cloud infrastructure that contains an on-premises Active Directory Domain Services (AD DS) forest, a Microsoft 365 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:

1.

Prevent the remote users from accessing any other resources on the network.

2.

Support Azure Active Directory (Azure AD) Conditional Access.

3.

Simplify the end-user experience. What should you include in the recommendation?

A. Azure AD Application Proxy

B. web content filtering in Microsoft Defender for Endpoint

C. Microsoft Tunnel

D. Azure Virtual WAN

Correct Answer: A

Azure Active Directory\\'s Application Proxy provides secure remote access to on-premises web applications. After a single sign-on to Azure AD, users can access both cloud and on-premises applications through an external URL or an internal

application portal.

Azure AD Application Proxy is:

Secure. On-premises applications can use Azure\\'s authorization controls and security analytics. For example, on-premises applications can use Conditional Access and two-step verification. Application Proxy doesn\\'t require you to open

inbound connections through your firewall.

Simple to use. Users can access your on-premises applications the same way they access Microsoft 365 and other SaaS apps integrated with Azure AD. You don\\'t need to change or update your applications to work with Application Proxy.

Incorrect:

Not D: Azure Virtual WAN

Azure Virtual WAN is for end users, not for applications.

Note: Azure Virtual WAN is a networking service that brings many networking, security, and routing functionalities together to provide a single operational interface. Some of the main features include:

Branch connectivity (via connectivity automation from Virtual WAN Partner devices such as SD-WAN or VPN CPE).

Site-to-site VPN connectivity.

Remote user VPN connectivity (point-to-site).

Private connectivity (ExpressRoute).

Intra-cloud connectivity (transitive connectivity for virtual networks).

VPN ExpressRoute inter-connectivity.

Routing, Azure Firewall, and encryption for private connectivity.

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