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.certbus.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

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

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

What should you include in the recommendation?

A. business resilience

B. modem access control

C. network isolation

D. security baselines in the Microsoft Cloud Security Benchmark

Correct Answer: D

Explanation:

The Microsoft cloud security benchmark (MCSB) provides prescriptive best practices and recommendations to help improve the security of workloads, data, and services on Azure and your multi-cloud environment. This benchmark focuses

on cloud-centric control areas with input from a set of holistic Microsoft and industry security guidance.

Controls include:

*

Endpoint Security (ES)

Endpoint Security covers controls in endpoint detection and response, including use of endpoint detection and response (EDR) and anti-malware service for endpoints in cloud environments.

*

Data Protection (DP)

Data Protection covers control of data protection at rest, in transit, and via authorized access mechanisms, including discover, classify, protect, and monitor sensitive data assets using access control, encryption, key management and

certificate management.

*

Etc.

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

QUESTION 2

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

You have an on-premises datacenter that contains 100 servers. The servers run Windows Server and are backed up by using Microsoft Azure Backup Server (MABS).

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

You need to ensure that a compromised administrator account cannot be used to delete the backups.

What should you do?

A. From Azure Backup, configure multi-user authorization by using Resource Guard.

B. From Microsoft Azure Backup Setup, register MABS with a Recovery Services vault.

C. From a Recovery Services vault, generate a security PIN for critical operations.

D. From Azure AD Privileged Identity Management (PIM), create a role assignment for the Backup Contributor role.

Correct Answer: C

Security features to help protect hybrid backups that use Azure Backup

Prevent attacks

Checks have been added to make sure only valid users can perform various operations. These include adding an extra layer of authentication, and maintaining a minimum retention range for recovery purposes.

Authentication to perform critical operations

As part of adding an extra layer of authentication for critical operations, you\\'re prompted to enter a security PIN when you perform Stop Protection with Delete data and Change Passphrase operations.

To receive this PIN:

1.

Sign in to the Azure portal.

2.

Browse to Recovery Services vault > Settings > Properties.

3.

Under Security PIN, select Generate. This opens a pane that contains the PIN to be entered in the Azure Recovery Services agent user interface. This PIN is valid for only five minutes, and it gets generated automatically after that period. Reference: https://learn.microsoft.com/en-us/azure/backup/backup-azure-security-feature

QUESTION 3

You need to recommend a strategy for routing internet-bound traffic from the landing zones. The solution must meet the landing zone requirements.

What should you recommend as part of the landing zone deployment?

A. service chaining

B. local network gateways

C. forced tunneling

D. a VNet-to-VNet connection

Correct Answer: A

Service chaining.

Service chaining enables you to direct traffic from one virtual network to a virtual appliance or gateway in a peered network through user-defined routes.

You can deploy hub-and-spoke networks, where the hub virtual network hosts infrastructure components such as a network virtual appliance or VPN gateway. All the spoke virtual networks can then peer with the hub virtual network. Traffic

flows through network virtual appliances or VPN gateways in the hub virtual network.

Virtual network peering enables the next hop in a user-defined route to be the IP address of a virtual machine in the peered virtual network, or a VPN gateway. You can\\'t route between virtual networks with a user-defined route that specifies

an Azure ExpressRoute gateway as the next hop type.

Incorrect:

Not B: Forced tunneling lets you redirect or "force" all Internet-bound traffic back to your on-premises location via a Site-to-Site VPN tunnel for inspection and auditing. This is a critical security requirement for most enterprise IT policies. If you

don\\'t configure forced tunneling, Internet-bound traffic from your VMs in Azure always traverses from the Azure network infrastructure directly out to the Internet, without the option to allow you to inspect or audit the traffic. Unauthorized

Internet access can potentially lead to information disclosure or other types of security breaches.

ExpressRoute forced tunneling is not configured via this mechanism, but instead, is enabled by advertising a default route via the ExpressRoute BGP peering sessions.

Note:

Requirements. Planned Changes

Litware plans to implement the following changes:

Design a landing zone strategy to refactor the existing Azure environment of Litware and deploy all future Azure workloads.

Requirements. Azure Landing Zone Requirements

Litware identifies the following landing zone requirements:

1.

Route all internet-bound traffic from landing zones through Azure Firewall in a dedicated Azure subscription.

2.

Provide a secure score scoped to the landing zone.

3.

Ensure that the Azure virtual machines in each landing zone communicate with Azure App Service web apps in the same zone over the Microsoft backbone network, rather than over public endpoints.

4.

Minimize the possibility of data exfiltration.

5.

Maximize network bandwidth.

The landing zone architecture will include the dedicated subscription, which will serve as the hub for internet and hybrid connectivity. Each landing zone will have the following characteristics:

1.

Be created in a dedicated subscription.

2.

Use a DNS namespace of litware.com.

Reference: https://docs.microsoft.com/en-us/azure/virtual-network/virtual-network-peering-overview#service-chaining https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-forced-tunneling-rm

---

QUESTION 4

HOTSPOT

You use Azure Policy with Azure Repos to implement continuous integration and continuous deployment (CI/CD) workflows.

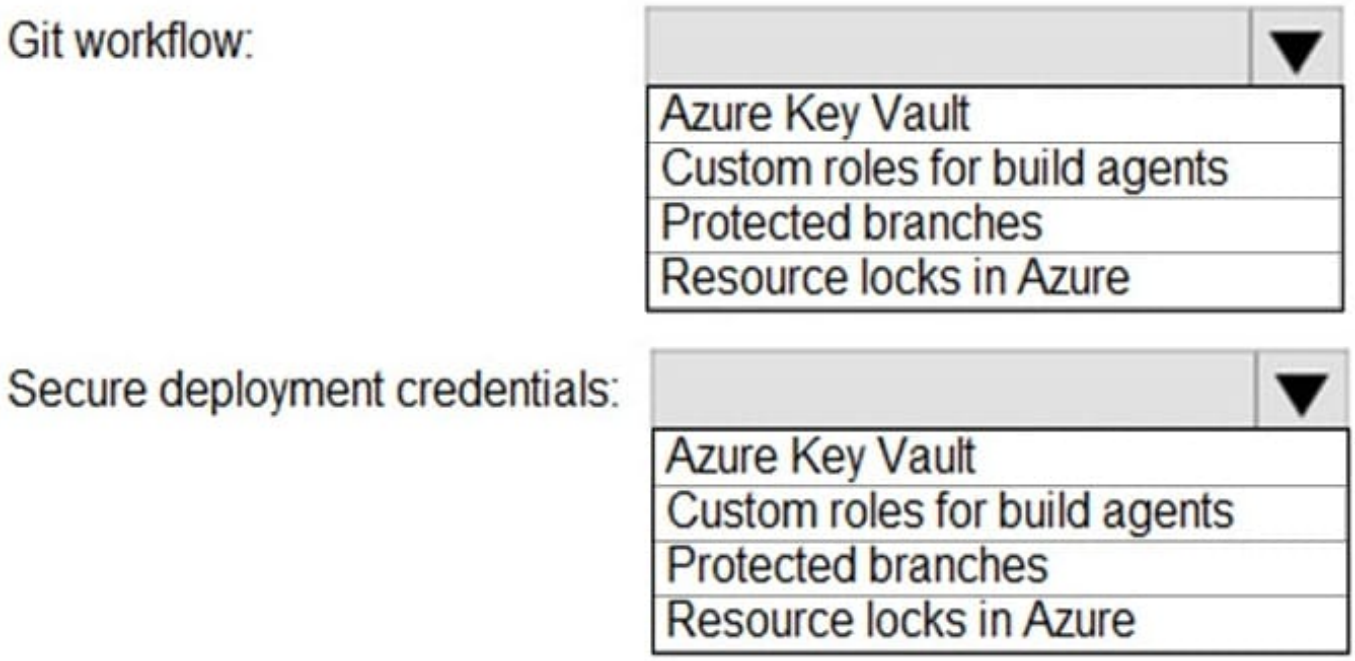
You need to recommend best practices to secure the stages of the CI/CD workflows based on the Microsoft Cloud Adoption Framework for Azure.

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.

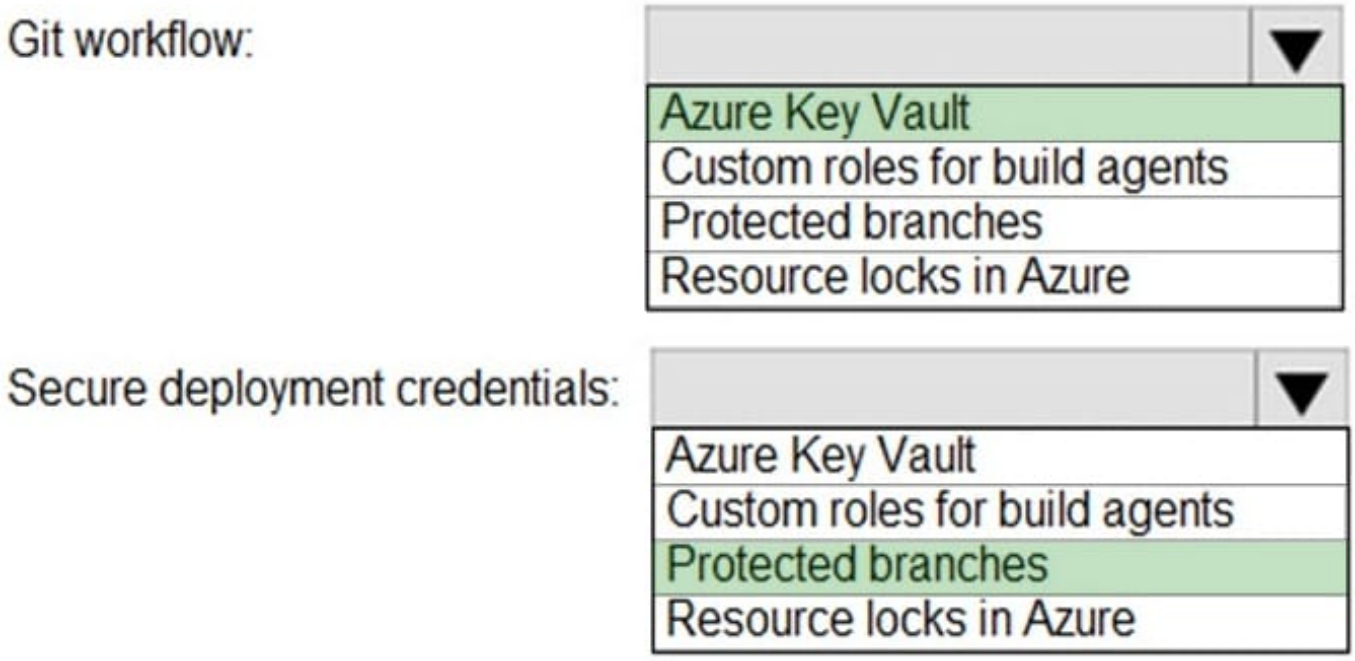
Hot Area:

Answer Area



Correct Answer:

Answer Area



Box 1: Protected branches

Git workflow

The pull request workflow is designed to introduce healthy friction, which is why it should only be applied to secure specific Git branches. Especially the branches that will trigger automated workflows that can deploy, configure, or in any other

way affect your cloud resources. These branches are called protected branches.

Restrict access to protected branches

The pull request workflow is used together with restricted access controls. The pull request workflow can\\'t be enforced however, unless the server is configured to reject direct changes to protected branches.

A developer can\\'t push directly to the production branch, but instead must create a pull request that targets the protected branch. Each SCM vendor has a different flavor for achieving restricted access to protected branches. For example, with

GitHub this feature is only available for organizations using GitHub team or GitHub Enterprise cloud.

Box 2: Azure Key Vault

Secure your deployment credentials

Pipelines and code repositories should not include hard-coded credentials and secrets. Credentials and secrets should be stored elsewhere and use CI vendor features for security. Because pipelines run as headless agents, they should

never use an individual\\'s password.

Azure Key Vault

If your CI platform supports it, consider storing credentials in a dedicated secret store, for example Azure Key Vault. Credentials are fetched at runtime by the build agent and your attack surface is reduced.

Reference:

https://learn.microsoft.com/en-us/azure/cloud-adoption-framework/secure/best-practices/secure-devops

QUESTION 5

Your company has a hybrid cloud infrastructure.

The company plans to hire several temporary employees within a brief period. The temporary employees will need to access applications and data on the company\\' premises network.

The company\\'s security policy prevents the use of personal devices for accessing company data and applications.

You need to recommend a solution to provide the temporary employee with access to company resources. The solution must be able to scale on demand.

What should you include in the recommendation?

A. Deploy Azure Virtual Desktop, Azure AD Conditional Access, and Microsoft Defender for Cloud Apps.

B. Redesign the VPN infrastructure by adopting a split tunnel configuration.

C. Deploy Microsoft Endpoint Manager and Azure AD Conditional Access.

D. Migrate the on-premises applications to cloud-based applications.

Correct Answer: A

You can connect an Azure Virtual Desktop to an on-premises network using a virtual private network (VPN), or use Azure ExpressRoute to extend the on-premises network into the Azure cloud over a private connection.

*

Azure AD: Azure Virtual Desktop uses Azure AD for identity and access management. Azure AD integration applies Azure AD security features like conditional access, multi-factor authentication, and the Intelligent Security Graph, and helps

maintain app compatibility in domain-joined VMs.

*

Azure Virtual Desktop, enable Microsoft Defender for Cloud.

We recommend enabling Microsoft Defender for Cloud\\'s enhanced security features to:

Manage vulnerabilities.

Assess compliance with common frameworks like PCI.

* Microsoft Defender for Cloud Apps, formerly known as Microsoft Cloud App Security, is a comprehensive solution for security and compliance teams enabling users in the organization, local and remote, to safely adopt business applications without compromising productivity.

Reference: https://docs.microsoft.com/en-us/azure/architecture/example-scenario/wvd/windows-virtual-desktop https://docs.microsoft.com/en-us/azure/virtual-desktop/security-guide https://techcommunity.microsoft.com/t5/security-compliance-and-identity/announcing-microsoft-defender-for-cloud-apps/ba-p/2835842

QUESTION 6

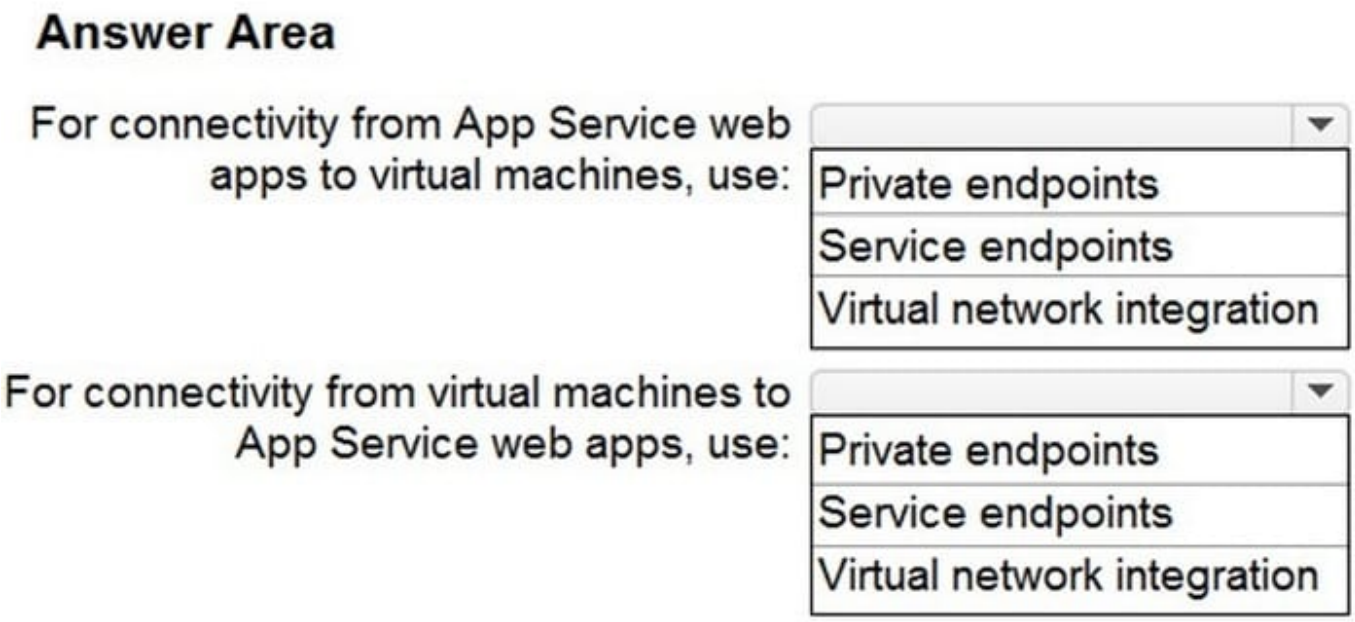
HOTSPOT

You need to recommend a strategy for App Service web app connectivity. The solution must meet the landing zone requirements.

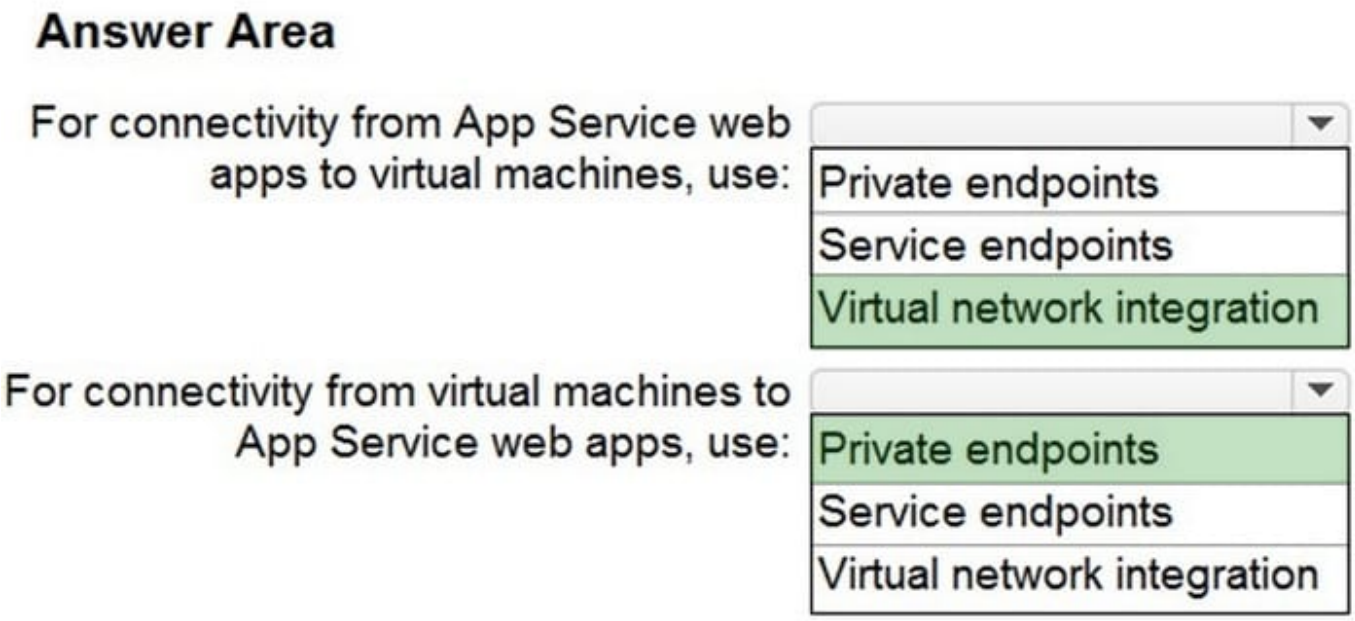
What should you recommend? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Correct Answer:



Box 1: Virtual network integration

Integrate your app with an Azure virtual network.

With Azure virtual networks, you can place many of your Azure resources in a non-internet-routable network. The App Service virtual network integration feature enables your apps to access resources in or through a virtual network.

Box 2: Private endpoints

Ensure that the Azure virtual machines in each landing zone communicate with Azure App Service web apps in the same zone over the Microsoft backbone network, rather than over public endpoints.

A virtual machine can connect to the web app across the private endpoint.

Reference: https://docs.microsoft.com/en-us/azure/app-service/overview-vnet-integration

https://docs.microsoft.com/en-us/azure/private-link/tutorial-private-endpoint-webapp-portal

QUESTION 7

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 workbooks to monitor risk detections

B. Azure AD Conditional Access integration with user flows and custom policies

C. smart account lockout in Azure AD B2C

D. access packages in Identity Governance

E. custom resource owner password credentials (ROPC) flows in Azure AD B2C

Correct Answer: BC

B. Azure AD Conditional Access integration with user flows and custom policies

C. Smart account lockout in Azure AD B2C.

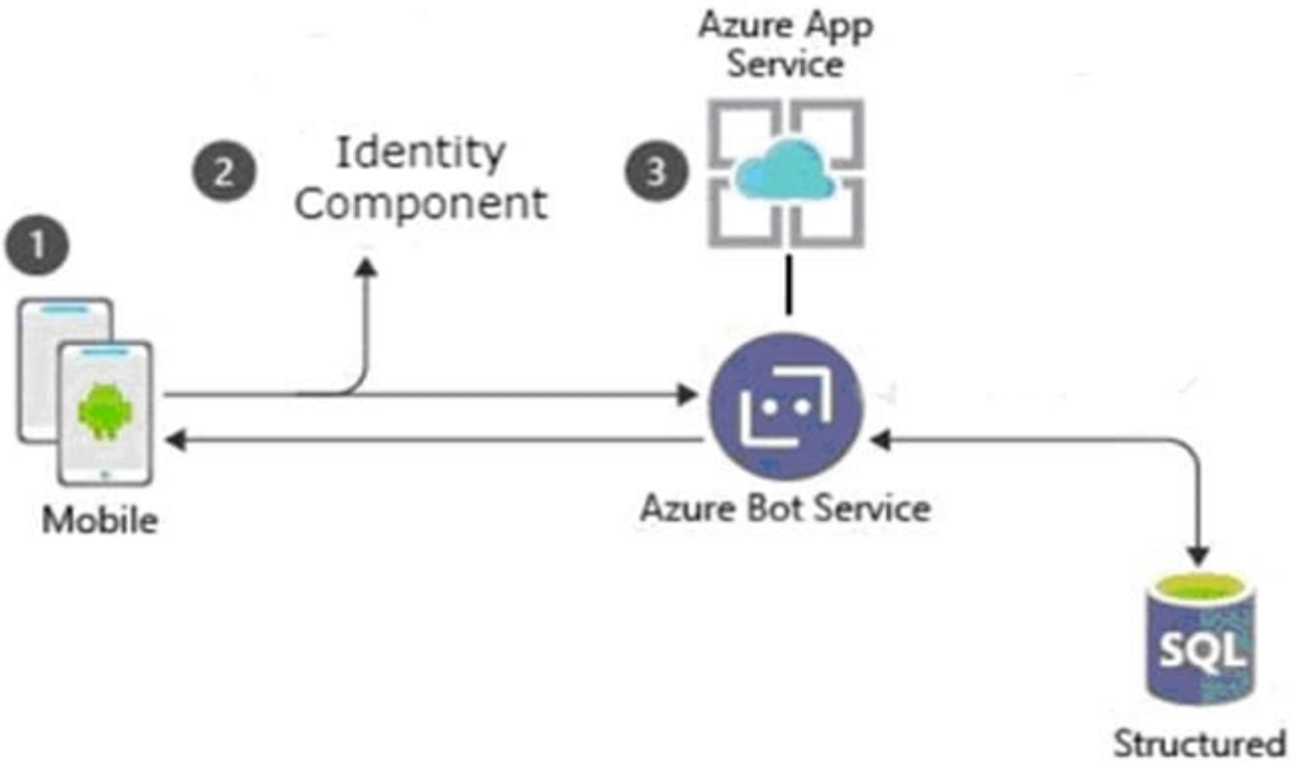
Conditional Access in Azure Active Directory (Azure AD) is a feature that enables you to enforce security policies and control access to applications based on specific conditions

https://docs.microsoft.com/en-us/azure/active-directory-b2c/threat-management

https://docs.microsoft.com/en-us/azure/active-directory-b2c/conditional-access-user-flow?pivots=b2c-user-flow

QUESTION 8

A customer uses Azure to develop a mobile app that will be consumed by external users as shown in the following exhibit.



You need to design an identity strategy for the app. The solution must meet the following requirements:

1.

Enable the usage of external IDs such as Google, Facebook, and Microsoft accounts.

2.

Be managed separately from the identity store of the customer.

3.

Support fully customizable branding for each app. Which service should you recommend to complete the design?

A. Azure Active Directory (Azure AD) B2B

B. Azure Active Directory Domain Services (Azure AD DS)

C. Azure Active Directory (Azure AD) B2C

D. Azure AD Connect

Correct Answer: C

Azure Active Directory B2C (Azure AD B2C), an identity store, is an identity management service that enables custom control of how your customers sign up, sign in, and manage their profiles when using your iOS, Android, .NET, single-page

(SPA), and other applications.

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

Branding

Branding and customizing the user interface that Azure Active Directory B2C (Azure AD B2C) displays to your customers helps provide a seamless user experience in your application. These experiences include signing up, signing in, profile

editing, and password resetting. This article introduces the methods of user interface (UI) customization.

Incorrect:

Not D: Azure AD Connect is a tool for connecting on-premises identity infrastructure to Microsoft Azure AD.

Reference: https://docs.microsoft.com/en-us/azure/active-directory-b2c/

https://docs.microsoft.com/en-us/azure/active-directory-b2c/identity-provider-facebook?pivots=b2c-user-flow

https://docs.microsoft.com/en-us/azure/active-directory-b2c/customize-ui-with-html?pivots=b2c-user-flow

QUESTION 9

Your company finalizes the adoption of Azure and is implementing Microsoft Defender for Cloud. You receive the following recommendations in Defender for Cloud

1.

Access to storage accounts with firewall and virtual network configurations should be restricted.

2.

Storage accounts should restrict network access using virtual network rules.

3.

Storage account should use a private link connection.

4.

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 Policy

B. Azure Network Watcher

C. Azure Storage Analytics

D. Microsoft Sentinel

Correct Answer: A

An Azure Policy definition, created in Azure Policy, is a rule about specific security conditions that you want controlled. Built in definitions include things like controlling what type of resources can be deployed or enforcing the use of tags on all resources. You can also create your own custom policy definitions.

Note: Azure security baseline for Azure Storage This security baseline applies guidance from the Azure Security Benchmark version 1.0 to Azure Storage. The Azure Security Benchmark provides recommendations on how you can secure your cloud solutions on Azure. The content is grouped by the security controls defined by the Azure Security Benchmark and the related guidance applicable to Azure Storage.

You can monitor this security baseline and its recommendations using Microsoft Defender for Cloud. Azure Policy definitions will be listed in the Regulatory Compliance section of the Microsoft Defender for Cloud dashboard.

For example:

*

1.1: Protect Azure resources within virtual networks Guidance: Configure your storage account\\'s firewall by restricting access to clients from specific public IP address ranges, select virtual networks, or specific Azure resources. You can also configure Private Endpoints so traffic to the storage service from your enterprise travels exclusively over private networks.

*

1.8: Minimize complexity and administrative overhead of network security rules Guidance: For resource in Virtual Networks that need access to your Storage account, use Virtual Network Service tags for the configured Virtual Network to define network access controls on network security groups or Azure Firewall. You can use service tags in place of specific IP addresses when creating security rules.

Reference: 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 10

For an Azure deployment, you are designing a security architecture based on the Microsoft Cloud Security Benchmark.

You need to recommend a best practice for implementing service accounts for Azure API management.

What should you include in the recommendation?

A. application registrations in Azure AD

B. managed identities in Azure

C. Azure service principals with usernames and passwords

D. device registrations in Azure AD

E. Azure service principals with certificate credentials

Correct Answer: B

IM-3: Manage application identities securely and automatically Features Managed Identities Description: Data plane actions support authentication using managed identities.

Configuration Guidance: Use a Managed Service Identity generated by Azure Active Directory (Azure AD) to allow your

API Management instance to easily and securely access other Azure AD-protected resources, such as Azure Key Vault instead of using service principals. Managed identity credentials are fully managed, rotated, and protected by the platform, avoiding hard-coded credentials in source code or configuration files.

Reference: https://learn.microsoft.com/en-us/security/benchmark/azure/baselines/api-management-security-baseline

QUESTION 11

You are designing a ransomware response plan that follows Microsoft Security Best Practices.

You need to recommend a solution to minimize the risk of a ransomware attack encrypting local user files.

What should you include in the recommendation?

A. Windows Defender Device Guard

B. Microsoft Defender for Endpoint

C. Azure Files

D. BitLocker Drive Encryption (BitLocker)

E. protected folders

Correct Answer: B

QUESTION 12

You have an Azure subscription that contains virtual machines, storage accounts, and Azure SQL databases.

All resources are backed up multiple times a day by using Azure Backup.

You are developing a strategy to protect against ransomware attacks.

You need to recommend which controls must be enabled to ensure that Azure Backup can be used to restore the resources in the event of a successful ransomware attack.

Which two controls should you include in the recommendation? Each correct answer presents a complete solution.

NOTE: Each correct selection is worth one point.

A. Enable soft delete for backups.

B. Require PINs for critical operations.

C. Encrypt backups by using customer-managed keys (CMKs).

D. Perform offline backups to Azure Data Box.

E. Use Azure Monitor notifications when backup configurations change.

Correct Answer: BE

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.

Your backups need to be protected from sophisticated bot and malware attacks. Permanent loss of data can have significant cost and time implications to your business. To help protect against this, Azure Backup guards against malicious attacks through deeper security, faster notifications, and extended recoverability.

For deeper security, only users with valid Azure credentials will receive a security PIN generated by the Azure portal to allow them to backup data. If a critical backup operation is authorized, such as “delete backup data,” a notification is immediately sent so you can engage and minimize the impact to your business. If a hacker does delete backup data, Azure Backup will store the deleted backup data for up to 14 days after deletion.

E: Key benefits of Azure Monitor alerts include:

Monitor alerts at-scale via Backup center: In addition to enabling you to manage the alerts from Azure Monitor dashboard, Azure Backup also provides an alert management experience tailored to backups via Backup center. This allows you

to filter alerts by backup specific properties, such as workload type, vault location, and so on, and a way to get quick visibility into the active backup security alerts that need attention.

Reference: https://docs.microsoft.com/en-us/azure/security/fundamentals/backup-plan-to-protect-against-ransomware https://www.microsoft.com/security/blog/2017/01/05/azure-backup-protects-against-ransomware/ https://docs.microsoft.com/en-us/azure/backup/move-to-azure-monitor-alerts

---

QUESTION 13

A customer follows the Zero Trust model and explicitly verifies each attempt to access its corporate applications.

The customer discovers that several endpoints are infected with malware.

The customer suspends access attempts from the infected endpoints.

The malware is removed from the end point.

Which two conditions must be met before endpoint users can access the corporate applications again? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. The client access tokens are refreshed.

B. Microsoft Intune reports the endpoints as compliant.

C. A new Azure Active Directory (Azure AD) Conditional Access policy is enforced.

D. Microsoft Defender for Endpoint reports the endpoints as compliant.

Correct Answer: AC

A: When a client acquires an access token to access a protected resource, the client also receives a refresh token. The refresh token is used to obtain new access/refresh token pairs when the current access token expires. Refresh tokens

are also used to acquire extra access tokens for other resources.

Refresh token expiration

Refresh tokens can be revoked at any time, because of timeouts and revocations.

C: Microsoft Defender for Endpoint is an enterprise endpoint security platform designed to help enterprise networks prevent, detect, investigate, and respond to advanced threats. It uses a combination of endpoint behavioral sensors, cloud

security analytics, and threat intelligence.

The interviewees said that “by implementing Zero Trust architecture, their organizations improved employee experience (EX) and increased productivity.” They also noted, “increased device performance and stability by managing all of their endpoints with Microsoft Endpoint Manager.” This had a bonus effect of reducing the number of agents installed on a user\\'s device, thereby increasing device stability and performance. “For some organizations, this can reduce boot times from 30 minutes to less than a minute,” the study states. Moreover, shifting to Zero Trust moved the burden of security away from users. Implementing single sign-on (SSO), multifactor authentication (MFA), leveraging passwordless authentication, and eliminating VPN clients all further reduced friction and improved user productivity.

Note: Azure AD at the heart of your Zero Trust strategy Azure AD provides critical functionality for your Zero Trust strategy. It enables strong authentication, a point of integration for device security, and the core of your user-centric policies to guarantee least-privileged access. Azure AD\\'s Conditional Access capabilities are the policy decision point for access to resource

Reference: https://www.microsoft.com/security/blog/2022/02/17/4-best-practices-to-implement-a-comprehensive-zero-trust-security-approach/ https://docs.microsoft.com/en-us/azure/active-directory/develop/refresh-tokens

---

QUESTION 14

HOTSPOT

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

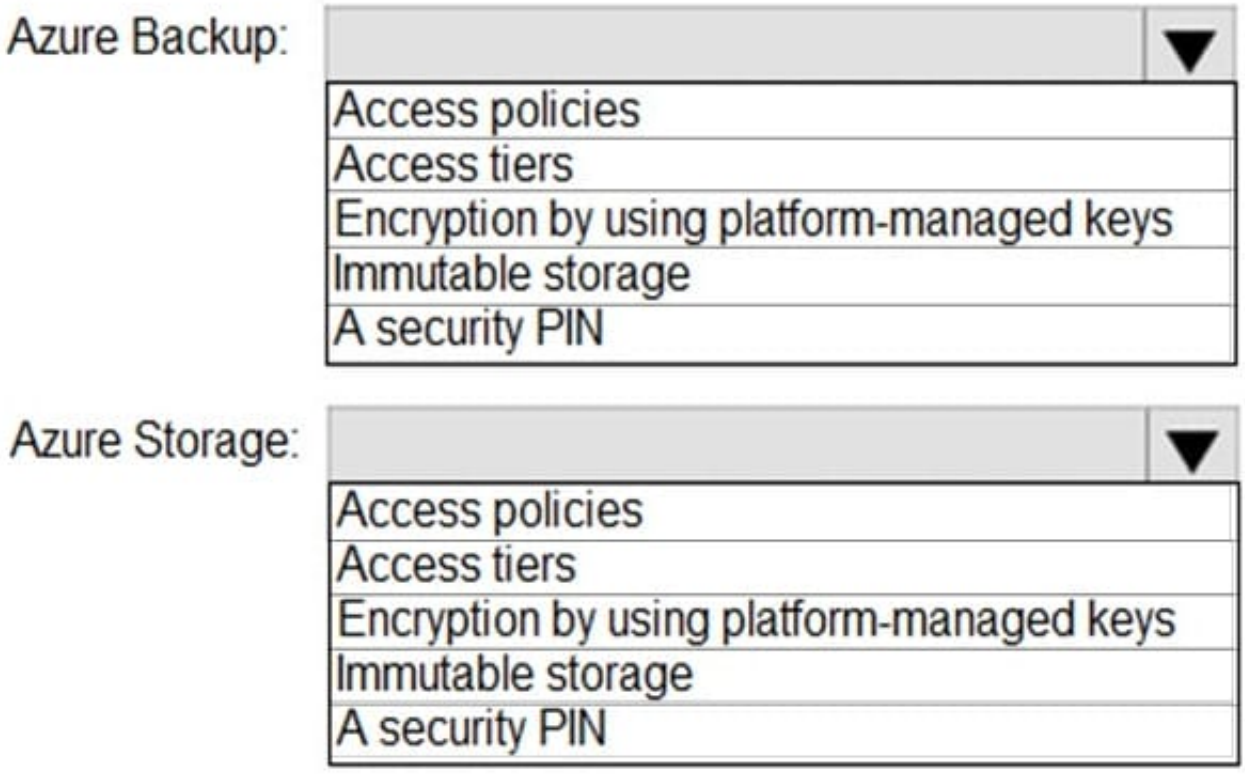
You need to recommend which capabilities of Azure Backup and Azure Storage provide the strongest protection against ransomware attacks. The solution must follow Microsoft Security Best Practices.

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

NOTE: Each correct selection is worth one point.

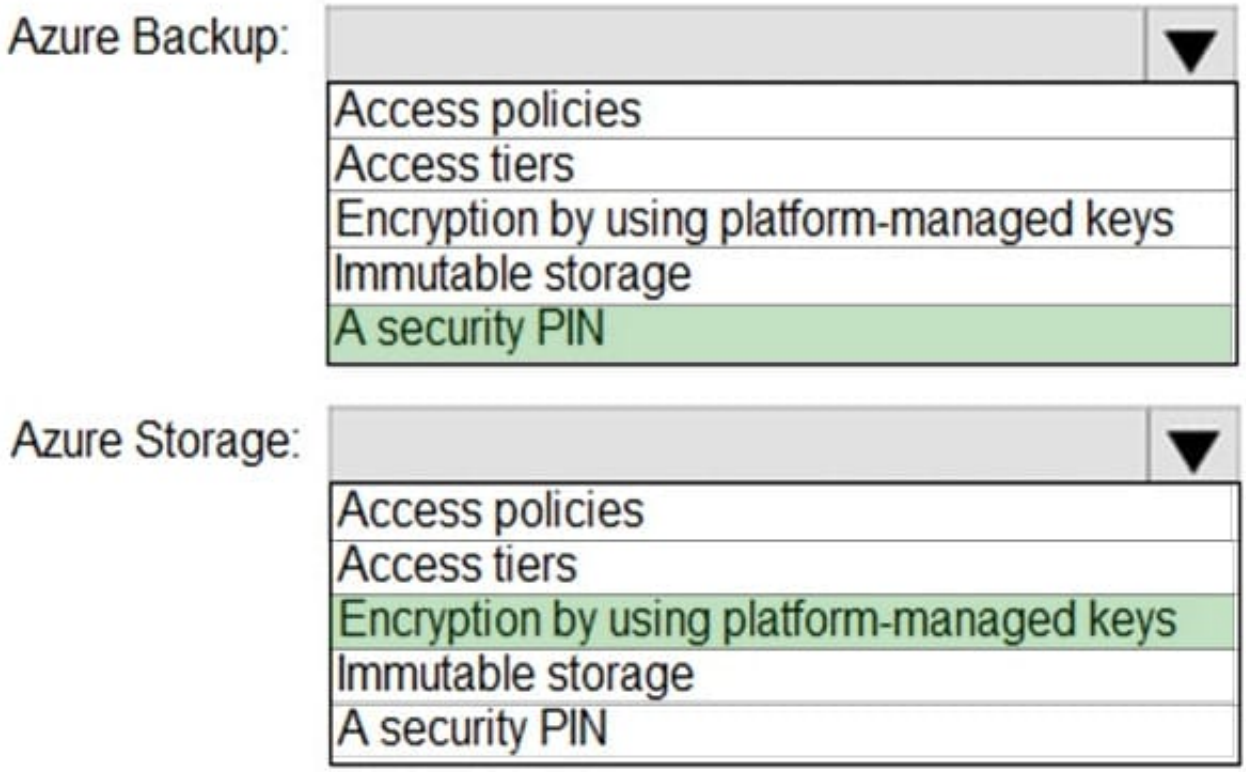
Hot Area:

Answer Area



Correct Answer:

Answer Area



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 15

Your company plans to apply the Zero Trust Rapid Modernization Plan (RaMP) to its IT environment.

You need to recommend the top three modernization areas to prioritize as part of the plan.

Which three areas should you recommend based on RaMP? Each correct answer presents part of the solution.

NOTE: Each correct selection is worth one point.

A. data, compliance, and governance

B. infrastructure and development

C. user access and productivity

D. operational technology (OT) and IoT

E. modern security operations

Correct Answer: ACE

RaMP initiatives for Zero Trust

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

Critical security modernization initiatives:

(C) User access and productivity

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

(A) Data, compliance, and governance

2.

Ransomware recovery readiness

3.

Data

(E) Modernize security operations

4.

Streamline response

5.

Unify visibility

6.

reduce manual effort

Incorrect:

As needed

Additional initiatives based on Operational Technology (OT) or IoT usage, on-premises and cloud adoption, and security for in-house app development:

*

(not D) OT and Industrial IoT Discover Protect Monitor

*

Datacenter and DevOps Security Security Hygiene Reduce Legacy Risk DevOps Integration Microsegmentation

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