VIDEO PRACTICE EXAM

AZ-500 EXAM CRAM

Are you ready?

Microsoft CERTIFIED

AZURE SECURITY ENGINEER

ASSOCIATE

★★

COVERS ALL 4 EXAM DOMAINS!

WHO AM I?

Cybersecurity Strategist

vCISO for a regional bank

Speaker and Author

16-time Microsoft MVP

LinkedIn Learning Instructor

Content Developer (YouTube)

Pete Zerger

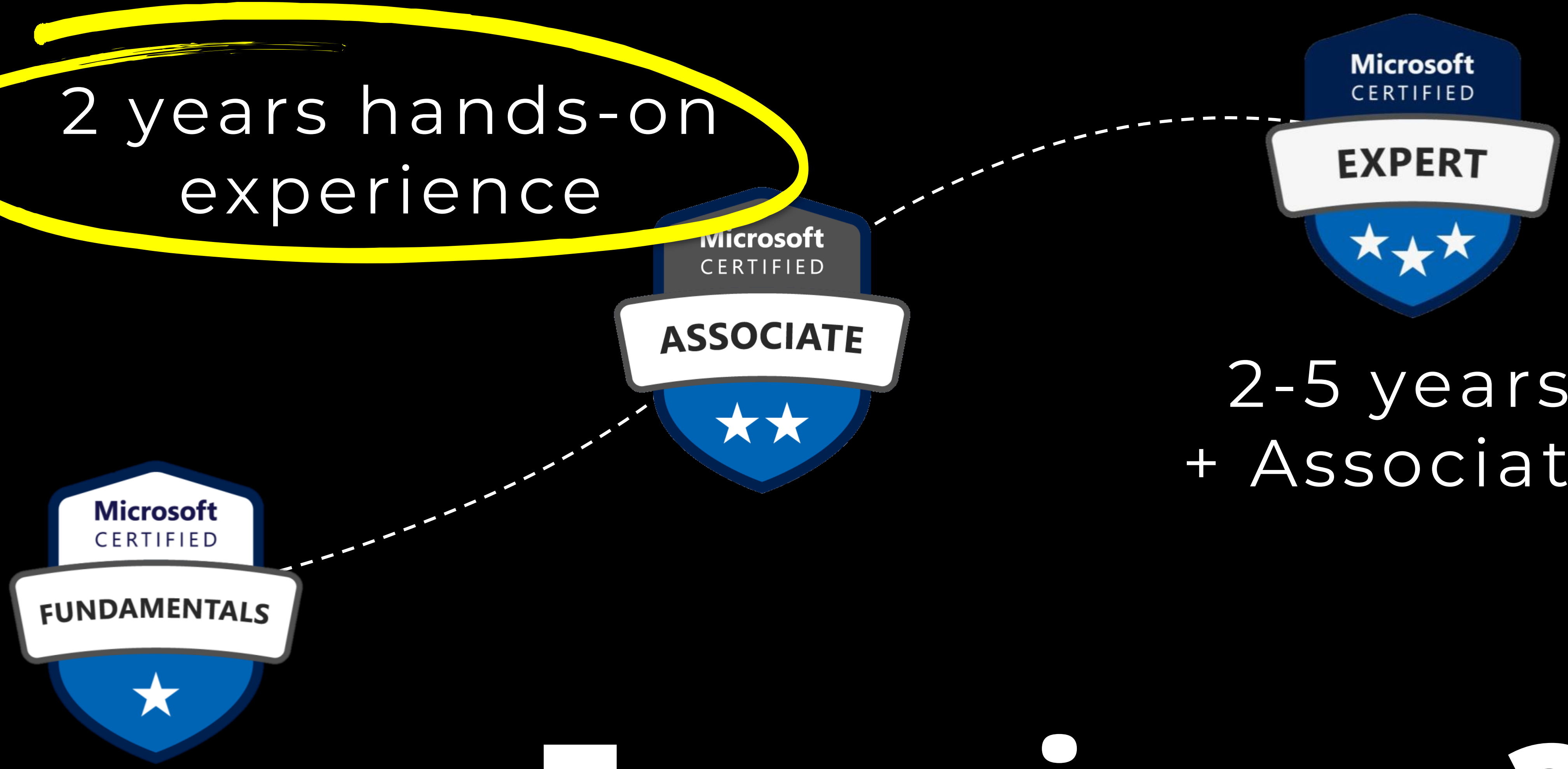
CISSP, vCISO, MVP

MVP Microsoft Most Valuable Professional

in LEARNING

What can you expect on the MICROSOFT AZ-500 EXAM?

Experience?


Microsoft CERTIFIED FUNDAMENTALS
Microsoft CERTIFIED ASSOCIATE
Microsoft CERTIFIED EXPERT

2 years hands-on experience

2-5 years
+ Associate

just getting started

Free access to my AZ-500 Exam Prep resources!

(study guide, video exam prep)

in LEARNING

A pdf copy of the presentation is available in the video description!

SUBSCRIBE

HOW IT WORKS

Microsoft
CERTIFIED
AZURE SECURITY
ENGINEER
ASSOCIATE

HOW IT WORKS

120 practice questions with explanations

Narrated so you can listen anywhere!

Questions for all 4
AZ-500 exam domains

HOW IT WORKS

Not intended to reproduce actual exam questions!

Designed to make sure you really know the material!

Allow you to assess your knowledge as you progress

To ensure you're ready for the exam!

DOMAIN 1: MANAGE IDENTITY AND ACCESS

Microsoft CERTIFIED
AZURE SECURITY ENGINEER
ASSOCIATE

domain

00

In the OAuth Code Grant flow, the user confirms consent by:

1. providing a code back to the app
2. entering their password when prompted
3. by either providing a code or entering their password
4. none of the above

0:15

DOMAIN 1: MANAGE IDENTITY AND ACCESS

Microsoft
CERTIFIED
AZURE SECURITY
ENGINEER
ASSOCIATE

00

In the OAuth Code Grant flow, the user confirms consent by:

question

possible answers

1. providing a code back to the app
2. entering their password when prompted
3. by either providing a code or entering their password
4. none of the above

0:15

00 ANSWER

answer

1. providing a code back to the app

explanation

In the OAuth Code Grant flow, the user confirms consent by entering a code into a textbox provided.

DOMAIN 1: MANAGE IDENTITY AND ACCESS

Microsoft CERTIFIED
AZURE SECURITY ENGINEER
ASSOCIATE

01 Azure AD Privileged Identity Management (PIM) supports which of the following features when users request to activate a privileged identity profile?

1. a ticket number in a helpdesk system
2. an explanation of why they need to activate
3. approval by an admin
4. all of the above

0:15

DOMAIN 1: MANAGE IDENTITY AND ACCESS

01 ANSWER

4. all of the above

Azure AD Privileged Identity Management supports all three of these options, alone or in any combination.

DOMAIN 1: MANAGE IDENTITY AND ACCESS

Microsoft CERTIFIED
AZURE SECURITY ENGINEER
ASSOCIATE

02

Azure APIs can be protected by configuration of permission scopes to limit access to a 3rd party web app, even when users consent.

TRUE or FALSE?

0:15

DOMAIN 1: MANAGE IDENTITY AND ACCESS

02 ANSWER

TRUE

Admins can configure permission scopes ahead of any user consent.

DOMAIN 1: MANAGE IDENTITY AND ACCESS

Microsoft CERTIFIED AZURE SECURITY ENGINEER ASSOCIATE

03

In the OAuth Code Grant flow, the user confirms consent by:

1. providing a code back to the app
2. entering their password when prompted
3. by either providing a code or entering their password
4. none of the above

0:15

DOMAIN 1: MANAGE IDENTITY AND ACCESS

Microsoft
CERTIFIED
AZURE SECURITY
ENGINEER
ASSOCIATE

03 ANSWER

1. providing a code back to the app

In the OAuth Code Grant flow, the user confirms consent by entering a code into a textbox provided.

DOMAIN 1: MANAGE IDENTITY AND ACCESS

Microsoft CERTIFIED
AZURE SECURITY ENGINEER
ASSOCIATE

04

Azure AD Passthrough authentication (PTA) is associated with which of the following identity models?

1. Cloud only
2. Synchronized
3. Federated
4. All of the above

0:15

DOMAIN 1: MANAGE IDENTITY AND ACCESS

04 ANSWER

2. Synchronized

On-premises passwords are never stored in the cloud

Supports controls not present in Azure AD, like "logon hours"

Because it passes the authentication request to on-premises Active Directory, Passthrough Authentication (PTA) is associated with the **Synchronized identity model**

DOMAIN 1: MANAGE IDENTITY AND ACCESS

Microsoft CERTIFIED
AZURE SECURITY ENGINEER
ASSOCIATE

05

Which of the following identities eliminate the need for credentials in code?

1. Managed Identities
2. Service Principals
3. Managed Identities and Service Principals
4. None of the above

0:15

DOMAIN 1: MANAGE IDENTITY AND ACCESS

05 ANSWER

1. Managed Identities

Managed Identities eliminate the need to manage credentials. Managed identities are service principals of a special type, which are locked to only be used with Azure resources.

DOMAIN 1: MANAGE IDENTITY AND ACCESS

Microsoft CERTIFIED AZURE SECURITY ENGINEER ASSOCIATE

06

With Azure AD MFA, you can automatically block authentication for users who report fraud via email to a support address.

TRUE or FALSE?

0:15

DOMAIN 1: MANAGE IDENTITY AND ACCESS

06 ANSWER

FALSE

Users can report fraud using a code via phone (0 by default).

DOMAIN 1: MANAGE IDENTITY AND ACCESS

Microsoft CERTIFIED AZURE SECURITY ENGINEER ASSOCIATE

07

You can activate an eligible privileged identity profile

1. via the Microsoft Authenticator App
2. via the Azure Privileged Identity app in the Azure portal.
3. in the properties of your Office 365 user profile
4. All the above

0:15

DOMAIN 1: MANAGE IDENTITY AND ACCESS

07 ANSWER

2. via the Azure Privileged Identity app in the Azure portal.

Activating a profile is performed within the Azure AD PIM app in the Azure portal.

DOMAIN 1: MANAGE IDENTITY AND ACCESS

Microsoft
CERTIFIED
AZURE SECURITY
ENGINEER
ASSOCIATE

08

You can create new users in Azure AD with the Create-AzureADUser cmdlet.

TRUE or FALSE?

0:15

DOMAIN 1: MANAGE IDENTITY AND ACCESS

Microsoft CERTIFIED AZURE SECURITY ENGINEER ASSOCIATE

08 ANSWER

FALSE

This is false. The **New-AzureADUser** cmdlet is used to create new users in Azure AD.

DOMAIN 2: IMPLEMENT PLATFORM PROTECTION

Microsoft CERTIFIED AZURE SECURITY ENGINEER ASSOCIATE

09

Azure Container Registry (ACR) supports Kubernetes and Docker running on third-party cloud platforms.

TRUE or FALSE?

0:15

DOMAIN 1: MANAGE IDENTITY AND ACCESS

Microsoft CERTIFIED
AZURE SECURITY ENGINEER
ASSOCIATE

09 ANSWER

TRUE

When Microsoft Defender for container registries is enabled, any image you push to your registry will be scanned immediately.

ACR is a Docker container registry and does not disallow access from clouds other than Azure, with proper authentication.

DOMAIN 1: MANAGE IDENTITY AND ACCESS

10

You are planning on rolling out a new Azure AD Conditional Access policy to restrict access to only specific device platforms. Which of the following device platforms is <u>not</u> supported?

1. Android
2. iOS
3. Chrome OS
4. None of the above

0:15

DOMAIN 1: MANAGE IDENTITY AND ACCESS

10 ANSWER

3. Chrome OS

Chrome OS is not natively supported for device compliance in Conditional Access policies. Android, iOS, Windows, and MacOS are.

DOMAIN 1: MANAGE IDENTITY AND ACCESS

Microsoft CERTIFIED
AZURE SECURITY ENGINEER
ASSOCIATE

11 You can configure an Azure AD Conditional Access policies for specific client applications, such as Microsoft Word.

TRUE or FALSE?

0:15

DOMAIN 1: MANAGE IDENTITY AND ACCESS

11 ANSWER

TRUE

Conditional access can be scoped for specific apps, limited to compliant devices, sign-in risk, and more.

DOMAIN 1: MANAGE IDENTITY AND ACCESS

12

Microsoft Azure AD Identity Protection evaluates risk associated with:

1. users and sign-in attempts
2. users
3. users and devices
4. users, sign-in attempts, and devices

0:15

DOMAIN 1: MANAGE IDENTITY AND ACCESS

12 ANSWER

1. users and sign-in attempts

Azure AD Identity Protection evaluates risk associated to users and sign-in attempts.

Know the difference between "user risk" and sign-in risk

DOMAIN 1: MANAGE IDENTITY AND ACCESS

Microsoft CERTIFIED

AZURE SECURITY ENGINEER

ASSOCIATE ★★

13

Admin consent in Azure Active Directory (Azure AD) grants consent on behalf of

1. a specific user
2. all users
3. a specific user or device
4. none of the above

0:15

DOMAIN 1: MANAGE IDENTITY AND ACCESS

Microsoft
CERTIFIED
AZURE SECURITY ENGINEER
ASSOCIATE

13 ANSWER

2. all users

Admin consent grants consent on behalf of all users (tenant-wide). Admins can control the scope of a user’s ability to consent, including limiting permissions they may consent to, or disabling user consent.

DOMAIN 1: MANAGE IDENTITY AND ACCESS

14

Azure AD Connect or Azure AD Connect Cloud Sync can be used to configure which of the following identity models?

1. Cloud only
2. Synchronized and Federated
3. Synchronized
4. All of the above

0:15

DOMAIN 1: MANAGE IDENTITY AND ACCESS

14 ANSWER

2. Synchronized and Federated

Both the **Synchronized** and **Federated** models leverage Azure AD Connect or Azure AD Connect Cloud Sync.

DOMAIN 1: MANAGE IDENTITY AND ACCESS

Microsoft CERTIFIED AZURE SECURITY ENGINEER ASSOCIATE

15

Security Groups and Microsoft 365 groups can both be used to secure Azure resources.

TRUE or FALSE?

0:15

DOMAIN 1: MANAGE IDENTITY AND ACCESS

15 ANSWER

TRUE

Microsoft 365 groups (formerly called Office 365 groups) can be used to secure resources, just like Security groups. Microsoft 365 groups also include additional functionality for enabling collaboration.

DOMAIN 1: MANAGE IDENTITY AND ACCESS

Microsoft CERTIFIED
AZURE SECURITY ENGINEER
ASSOCIATE

16 You can configure access reviews in Privileged Identity Management (PIM) to be self-completed by the eligible members of the privileged roles.

TRUE or FALSE?

0:15

DOMAIN 1: MANAGE IDENTITY AND ACCESS

16 ANSWER

TRUE

Yes, you can assign designated reviewers, owners, or eligible role members. You can also configure affect to role eligibility when a self-reviewer fails to respond.

DOMAIN 1: MANAGE IDENTITY AND ACCESS

17

You need to continually evaluate the security posture of all identities in Azure Active Directory. You need to provide risk level, risk events, and current status. What should you configure?

1. Azure AD Conditional Access
2. Azure AD Identity Protection
3. Microsoft Cloud App Security
4. Privileged Identity Management

0:15

DOMAIN 1: MANAGE IDENTITY AND ACCESS

17 ANSWER

2. Azure AD Identity Protection

Identity Protection is a tool that allows organizations to automate the detection and remediation of identity-based risks and investigate risks using data in the portal.

DOMAIN 1: MANAGE IDENTITY AND ACCESS

Microsoft CERTIFIED AZURE SECURITY ENGINEER ASSOCIATE

18

You can configure Azure AD Conditional Access policies to target only users in untrusted locations.

TRUE or FALSE?

0:15

DOMAIN 1: MANAGE IDENTITY AND ACCESS

Microsoft CERTIFIED
AZURE SECURITY ENGINEER
ASSOCIATE

18 ANSWER

TRUE

TIP: select "All trusted locations" on the Exclude tab under Conditions > Locations

Conditional access can be scoped for specific users, apps, limited to compliant devices, sign-in risk, and more.

DOMAIN 1: MANAGE IDENTITY AND ACCESS

Microsoft
CERTIFIED
AZURE SECURITY
ENGINEER
ASSOCIATE

19 When configuring Single Sign On (SSO) for hybrid users, you need to ensure that all user passwords are evaluated by the on-premises Active Directory domain controller. What action will you take?

1. Configure Group Writeback in Azure AD Connect
2. Add users to a Privileged Identity Management profile
3. Create an Azure AD Conditional Access policy
4. Configure Passthrough Authentication (PTA)

0:15

DOMAIN 1: MANAGE IDENTITY AND ACCESS

19 ANSWER

4. Configure Passthrough Authentication

Azure AD Pass-through Authentication allows single sign-on for on-premises and cloud-based apps by validating user passwords directly against on-premises Active Directory.

DOMAIN 1: MANAGE IDENTITY AND ACCESS

Microsoft CERTIFIED AZURE SECURITY ENGINEER ASSOCIATE

20

You need to secure all guest user identities by only allowing logging into Microsoft Teams via Windows endpoints, always enforcing MFA. What should you implement to accomplish this goal?

1. Privileged Identity Management (PIM)
2. Azure AD Identity Protection
3. Passthrough Authentication (PTA)
4. Azure AD Conditional Access

0:15

DOMAIN 1: MANAGE IDENTITY AND ACCESS

20 ANSWER

4. Azure AD Conditional Access

Conditional Access supports rule configuration based on platform, app, risk, location, and more.

DOMAIN 1: MANAGE IDENTITY AND ACCESS

21

What is the minimum Azure RBAC role required to view Azure Monitor logs?

1. Security Administrator
2. Monitoring Contributor
3. Monitoring Administrator
4. Monitoring Reader

0:15

DOMAIN 1: MANAGE IDENTITY AND ACCESS

21 ANSWER

4. Monitoring Reader

Always choose your answers with "least privilege access" in mind

The Monitoring Reader role has read-only access to monitoring data.

DOMAIN 1: MANAGE IDENTITY AND ACCESS

22

Transferring a subscription to a new Azure AD tenant will cause Azure VMs to stop running.

TRUE or FALSE?

0:15

DOMAIN 1: MANAGE IDENTITY AND ACCESS

Microsoft
CERTIFIED
AZURE SECURITY
ENGINEER
ASSOCIATE

22 ANSWER

FALSE

This transfer will result in Azure role assignments being permanently deleted. It will impact managed identities. VMs will not stop running, but you will have to re-enable or recreate any managed identities after the transfer.

DOMAIN 1: MANAGE IDENTITY AND ACCESS

Microsoft
CERTIFIED
AZURE SECURITY
ENGINEER
ASSOCIATE

23

An app registration in Azure Active Directory creates an application object, as well as a service principal that can access resources.

TRUE or FALSE?

0:15

DOMAIN 1: MANAGE IDENTITY AND ACCESS

Microsoft CERTIFIED
AZURE SECURITY ENGINEER
ASSOCIATE

23 ANSWER

TRUE

See "Azure AD App Registration in Plain English (exam FAQs)" on YouTube

Yes, the **app object** is the GLOBAL representation of the app in the tenant where the app is registered, and the **service principal** the LOCAL, concrete instance, present in each tenant where the app is used.

DOMAIN 1: MANAGE IDENTITY AND ACCESS

Microsoft CERTIFIED
AZURE SECURITY ENGINEER
ASSOCIATE

24

For app registration, what are the permission types supported by the Microsoft identity platform? (Select two)

1. Delegated permissions
2. Explicit permissions
3. Inherited permissions
4. Application permissions

0:15

DOMAIN 1: MANAGE IDENTITY AND ACCESS

24 ANSWER

1. Delegated permissions,
4. Application permissions

Delegated permissions are used by apps that have a signed-in user present. **Application permissions** are used by apps that run without a signed-in user present.

DOMAIN 1: MANAGE IDENTITY AND ACCESS

Microsoft CERTIFIED
AZURE SECURITY ENGINEER
ASSOCIATE

25

What is the format of an OpenID Connect token?

1. YAML
2. XML
3. JWT
4. SAML

0:15

25 ANSWER

3. JWT

OpenID tokens are JSON Web Token (JWT) format. They are sent to the client application as part of an OpenID Connect (OIDC) flow and are used by the client to authenticate the user.

DOMAIN 1: MANAGE IDENTITY AND ACCESS

Microsoft CERTIFIED
AZURE SECURITY ENGINEER
ASSOCIATE

26

What is the minimum required license to enable Azure AD Conditional Access for a user?

1. Azure AD Premium Plan 2 (P2)
2. Microsoft 365 Business
3. Microsoft 365 E3
4. Azure AD Premium Plan 1 (P1)

0:15

DOMAIN 1: MANAGE IDENTITY AND ACCESS

26 ANSWER

4. Azure AD Premium Plan 1 (P1)

Azure AD Premium P1 is the minimum licensing required to enable Azure AD Conditional Access policies.

DOMAIN 1: MANAGE IDENTITY AND ACCESS

27

In Privileged Identity Management, what are the available settings when an assigned reviewer does not complete the review before the configured review ends?

1. No change
2. Remove access
3. Approve access
4. Disable account

0:15

DOMAIN 1: MANAGE IDENTITY AND ACCESS

27 ANSWER

1. No change, 2. Remove access,
3. Approve access

You have a variety of options with PIM reviews, enabling you to remove access from users who do not respond to reviews if necessary. Another option, "Take recommendations" is also available.

DOMAIN 1: MANAGE IDENTITY AND ACCESS

Microsoft CERTIFIED AZURE SECURITY ENGINEER ASSOCIATE

28

When multiple Azure Active Directory Conditional Access policies apply to a user, which of the following are true?

1. Policies are not applied in a particular order
2. Block access takes priority over all settings
3. Policies are applied in order by created date
4. Policies with device settings take precedence

0:15

DOMAIN 1: MANAGE IDENTITY AND ACCESS

28 ANSWER

Options 1 and 2

For every sign-in, Azure Active Directory evaluates all policies and ensures that all requirements in all applicable policies are met before granting access to the user. **Block access takes priority** over all other configuration settings.

DOMAIN 1: MANAGE IDENTITY AND ACCESS

Microsoft CERTIFIED AZURE SECURITY ENGINEER ASSOCIATE

29 When configuring an app registration in Azure AD, in which area of the registration do you configure the services the application can access?

1. in the Manifest
2. Authentication blade
3. API Permissions blade
4. Roles and Administrators blade

0:15

DOMAIN 1: MANAGE IDENTITY AND ACCESS

29 ANSWER

3. API Permissions

You use the 'Add a permission' button in the API Permissions blade.

DOMAIN 1: MANAGE IDENTITY AND ACCESS

30

_____ and _____ are required for access for an application that has been registered with Azure AD for modern user authentication.

1. Tenant ID, Client ID
2. Client ID, Client Secret
3. Client ID, Redirect URL
4. Tenant ID, Client Secret

0:15

DOMAIN 1: MANAGE IDENTITY AND ACCESS

30 ANSWER

2. Client ID, Client Secret

Think of **client ID** and **client secret** as the user and password. A **redirect URI** is the location that the authorization server will send the user to once the app has been successfully authorized and granted an authorization code or access token.

DOMAIN 1: MANAGE IDENTITY AND ACCESS

Microsoft
CERTIFIED
AZURE SECURITY
ENGINEER
ASSOCIATE

31

You need to delegate access to an admin for a VM named “VM1” in the “ContosoVM” resource group. They should have full control over the VM but should not be able to grant access to other users.

What permissions will you assign?

1. Scope = “ContosoVM”, Role = “Owner”
2. Scope = “ContosoVM”, Role = “Contributor”
3. Scope = “VM1”, Role = “Owner”
4. Scope = “VM1”, Role = “Contributor”

0:15

DOMAIN 1: MANAGE IDENTITY AND ACCESS

31 ANSWER

4. Scope = “VM1”, Role = “Contributor”

Contributor role access grants all rights except the ability to grant rights to others. Scoping to the VM object only ensures permissions are not granted to other VMs in the resource group.

DOMAIN 1: MANAGE IDENTITY AND ACCESS

32

Which of the following roles can manage assignments for other administrators in Privileged Identity Management (PIM) for Azure AD roles?

1. Global Administrator
2. Security Administrator
3. Security Reader
4. Privileged Role Administrator

0:15

DOMAIN 1: MANAGE IDENTITY AND ACCESS

32 ANSWER

1. Global Administrator,
4. Privileged Role Administrator

The **Global Administrator** who enables Privileged Identity Management (PIM) for an organization automatically get role assignments and access to PIM. The first user can assign others to the Privileged Role Administrator role.

DOMAIN 1: MANAGE IDENTITY AND ACCESS

Microsoft CERTIFIED
AZURE SECURITY ENGINEER
ASSOCIATE

33

Which of the following roles are required to manage assignments for other administrators in PIM for Azure resource roles?

1. Subscription Administrator
2. Resource Administrator
3. Privileged Role Administrator
4. Security Administrator

0:15

DOMAIN 1: MANAGE IDENTITY AND ACCESS

33 ANSWER

2. Resource Administrator

A user cannot manage Privileged Identity Management for resources without Resource Administrator permissions.

DOMAIN 2: IMPLEMENT PLATFORM PROTECTION

Microsoft CERTIFIED AZURE SECURITY ENGINEER ASSOCIATE

01

Azure Update Management can patch both Windows and Linux VMs.

TRUE or FALSE?

0:15

DOMAIN 2: IMPLEMENT PLATFORM PROTECTION

01 ANSWER

TRUE

Azure Update Management supports patching both supported Windows and several Linux distributions.

DOMAIN 2: IMPLEMENT PLATFORM PROTECTION

Microsoft
CERTIFIED
AZURE SECURITY
ENGINEER
ASSOCIATE

02

Network Security Groups include a rule to allow RDP access on which port by default?

1. TCP 22
2. TCP 443
3. TCP 3389
4. None of the above

0:15

DOMAIN 2: IMPLEMENT PLATFORM PROTECTION

Microsoft CERTIFIED AZURE SECURITY ENGINEER ASSOCIATE

02 ANSWER

4. None of the above

No rule is configured to enable remote access by default.

DOMAIN 2: IMPLEMENT PLATFORM PROTECTION

03

Physical isolation in AKS provides the highest pod density for running workloads.

TRUE or FALSE?

0:15

DOMAIN 2: IMPLEMENT PLATFORM PROTECTION

03 ANSWER

FALSE

Separate physical nodes result in lower pod density and greater management overhead.

DOMAIN 2: IMPLEMENT PLATFORM PROTECTION

Microsoft
CERTIFIED
AZURE SECURITY ENGINEER
ASSOCIATE

04

The **Azure Virtual Network Container Network Interface (CNI)** enables advanced networking for the following container solutions. (choose the best answer)

1. Azure Kubernetes Service (AKS)
2. AKS Engine
3. Docker containers
4. All the above

0:15

DOMAIN 2: IMPLEMENT PLATFORM PROTECTION

Microsoft CERTIFIED AZURE SECURITY ENGINEER ASSOCIATE ★★

04 ANSWER

4. All of the above

Also works with Kubernetes resources such as services, ingress controllers, and Kube DNS.

Azure Virtual Network CNI supports AKS, AKS Engine, as well as Docker.

DOMAIN 2: IMPLEMENT PLATFORM PROTECTION

05

The following are the available types of Azure resource locks. (choose the best answer)

1. CanNotDelete,ReadOnly
2. CanNotDelete,ReadOnly,NoAccess
3. CanNotDelete,NoAccess
4. CanNotDelete

0:15

DOMAIN 2: IMPLEMENT PLATFORM PROTECTION

05 ANSWER

1. CanNotDelete,ReadOnly

The two resource lock types are CanNotDelete and ReadOnly

DOMAIN 2: IMPLEMENT PLATFORM PROTECTION

06

The following resources support Azure resource firewall. (choose the best answer)

1. Azure SQL and Storage Accounts
2. Azure SQL and Azure VMs
3. Azure VMs and Storage Accounts
4. Storage Accounts

0:15

DOMAIN 2: IMPLEMENT PLATFORM PROTECTION

Microsoft CERTIFIED AZURE SECURITY ENGINEER ASSOCIATE

06 ANSWER

1. Azure SQL Servers and Databases, as well as Azure Storage Accounts support resource firewall.

Azure SQL Servers and Databases, as well as Azure Storage Accounts support resource firewall. Several other Azure PaaS services also support resource firewall.

DOMAIN 2: IMPLEMENT PLATFORM PROTECTION

Microsoft
CERTIFIED
AZURE SECURITY
ENGINEER
ASSOCIATE

07

The Standard tier of Microsoft Defender for Cloud is required to capture data on resource security hygiene.

TRUE or FALSE?

0:15

DOMAIN 2: IMPLEMENT PLATFORM PROTECTION

07 ANSWER

FALSE

The free tier of Microsoft Defender for Cloud will also provide information on resource security hygiene.

DOMAIN 2: IMPLEMENT PLATFORM PROTECTION

08

To provide full access to the resources in an Azure resource group, you should grant only the Contributor role for the subscription.

TRUE or FALSE?

0:15

DOMAIN 2: IMPLEMENT PLATFORM PROTECTION

Microsoft
CERTIFIED
AZURE SECURITY
ENGINEER
ASSOCIATE

08 ANSWER

FALSE

The Contributor role provides all permissions except the ability to grant access to others

There is no need to grant permissions at the subscription level. Always apply rule of least privilege when configuring RBAC in Azure.

DOMAIN 2: IMPLEMENT PLATFORM PROTECTION

Microsoft
CERTIFIED
AZURE SECURITY
ENGINEER
ASSOCIATE

09

You will configure a separate Front Door instance to route requests by URL path to different backend pools.

TRUE or FALSE?

0:15

DOMAIN 2: IMPLEMENT PLATFORM PROTECTION

09 ANSWER

FALSE

URL Path Based Routing allows you to route traffic to backend pools based on URL paths of the request. This can be accommodated from a single Front Door instance.

DOMAIN 2: IMPLEMENT PLATFORM PROTECTION

Microsoft CERTIFIED AZURE SECURITY ENGINEER ASSOCIATE

10 You need to block outbound Internet traffic from Azure VMs, while allowing global access to Azure Storage, with minimum administrative effort. Which technology will you use?

1. Microsoft Defender for Cloud Apps
2. Network Security Group (NSG)
3. Application Security Groups (ASG)
4. Azure Application Gateway

0:15

DOMAIN 2: IMPLEMENT PLATFORM PROTECTION

Microsoft
CERTIFIED
AZURE SECURITY
ENGINEER
ASSOCIATE

10 ANSWER

2. Network Security Group (NSG)

NSG **Service Tags** allow you to block outbound access to the Internet, but still allow access to Azure storage in the same region for diagnostics & metrics.

DOMAIN 2: IMPLEMENT PLATFORM PROTECTION

11 Azure Firewall requires you to specify the number of network virtual appliances according to your expected scale needs.

TRUE or FALSE?

0:15

DOMAIN 1: MANAGE IDENTITY AND ACCESS

Microsoft CERTIFIED
AZURE SECURITY ENGINEER
ASSOCIATE

11 ANSWER

FALSE

For the exam, ensure you are familiar with Azure Firewall Manager for central policy management of multiple firewalls

High availability and auto-scale are built into the service. There is no network virtual appliance (NVA) count necessary.

DOMAIN 2: IMPLEMENT PLATFORM PROTECTION

12

Azure VMs can communicate across VNETs by default

TRUE or FALSE?

0:15

DOMAIN 2: IMPLEMENT PLATFORM PROTECTION

12 ANSWER

FALSE

VMs on subnets within the same VNET have connectivity. Communication across VNETs requires VNET peering or VPN connectivity.

DOMAIN 2: IMPLEMENT PLATFORM PROTECTION

Microsoft CERTIFIED
AZURE SECURITY ENGINEER
ASSOCIATE

13

You plan to secure remote access from your on-premises network to your AKS cluster with minimum network latency and maximum security. Which solution will you choose?

1. Site-to-Site VPN
2. Point-to-Site VPN
3. Azure VNET Peering
4. Azure ExpressRoute

0:15

DOMAIN 2: IMPLEMENT PLATFORM PROTECTION

13 ANSWER

4. Azure ExpressRoute

Azure ExpressRoute does not use the public Internet, increasing security and control over network performance.

DOMAIN 2: IMPLEMENT PLATFORM PROTECTION

14

VMs included in an Application Security Group cannot be located in different Azure regions.

TRUE or FALSE?

0:15

DOMAIN 2: IMPLEMENT PLATFORM PROTECTION

Microsoft CERTIFIED
AZURE SECURITY ENGINEER
ASSOCIATE

14 ANSWER

TRUE

Members of an Application Security Group must be located in the same Azure region.

DOMAIN 2: IMPLEMENT PLATFORM PROTECTION

15

Microsoft best practices recommend adding an additional layer of access control security to Azure SQL databases. Which feature will you implement?

1. Azure Active Directory Conditional Access
2. Azure App Gateway
3. Network Security Group
4. Azure SQL Server-level firewall rule

0:15

DOMAIN 2: IMPLEMENT PLATFORM PROTECTION

Microsoft CERTIFIED
AZURE SECURITY ENGINEER
ASSOCIATE

15 ANSWER

4. Azure SQL Server-level firewall rule

You can create server-level firewall rules for single and pooled databases.

DOMAIN 2: IMPLEMENT PLATFORM PROTECTION

Microsoft
CERTIFIED
AZURE SECURITY
ENGINEER
ASSOCIATE

16

To achieve high availability for VMs in an Azure region, the following options are available

1. Availability Sets and Azure Site Recovery
2. Availability Sets, Availability Zones, Azure Site Recovery
3. Availability Sets and Availability Zones
4. Azure Site Recovery and Availability Zones

0:15

DOMAIN 2: IMPLEMENT PLATFORM PROTECTION

16 ANSWER

3. Availability Sets and Availability Zones

Both Availability Sets and Availability Zones enable VM high availability (HA) in an Azure region. Azure Site Recovery delivers disaster recovery (DR), not HA.

DOMAIN 2: IMPLEMENT PLATFORM PROTECTION

17

The service principal required by Azure Kubernetes Service (AKS) can be created by the following methods:

1. Automatically during AKS deployment via the Azure CLI
2. Manually using the Azure CLI before AKS deployment
3. No service principal is required for AKS
4. Option 1 or 2

0:15

DOMAIN 2: IMPLEMENT PLATFORM PROTECTION

17 ANSWER

4. Manually before deployment or automatically during deployment via Azure CLI

Both manual and automatic service principal creation is possible. Ideally, you would instead use a **managed identity**, which can by enabled only during cluster creation.

DOMAIN 2: IMPLEMENT PLATFORM PROTECTION

18

SSH is disabled on AKS nodes by default.

TRUE or FALSE?

0:15

DOMAIN 2: IMPLEMENT PLATFORM PROTECTION

18 ANSWER

FALSE

AKS allows SSH from private IPs by default. On the topic of access, know that Azure Kubernetes Service (AKS) can be configured to use Azure AD for user authentication.

DOMAIN 2: IMPLEMENT PLATFORM PROTECTION

Microsoft CERTIFIED
AZURE SECURITY ENGINEER
ASSOCIATE

19

You need to enforce that all new resources are created in specific Azure regions. You create an Azure policy. Does this meet your objective?

YES or NO?

0:15

DOMAIN 2: IMPLEMENT PLATFORM PROTECTION

19 ANSWER

YES

Initiative = a group of policies

Blueprints for governed environments

You can assign a **policy** to enforce a condition for resources you create in the future. For the exam, know what **initiatives** and **blueprints** are as well.

DOMAIN 2: IMPLEMENT PLATFORM PROTECTION

20

You can configure the following scanning options for your container images for Azure Kubernetes Service

1. In the Azure Container Registry
2. At design time in Visual Studio Code
3. In the AKS container runtime
4. Options 1 and 3

0:15

DOMAIN 2: IMPLEMENT PLATFORM PROTECTION

20 ANSWER

1. In the ACR, 3. In AKS container runtime

Scanning of both the ACR and AKS runtime are possible to identify vulnerabilities related to your containerized services.

DOMAIN 2: IMPLEMENT PLATFORM PROTECTION

Microsoft CERTIFIED
AZURE SECURITY ENGINEER
ASSOCIATE

21

What are the two distinct modes of runtime isolation for Windows containers?

1. Process
2. Global
3. Hyper-V
4. Local

0:15

DOMAIN 2: IMPLEMENT PLATFORM PROTECTION

21 ANSWER

1. Process, 3. Hyper-V

With process isolation mode, containers share the same kernel with the host as well as each other. With Hyper-V isolation, each container effectively gets its own kernel.

DOMAIN 2: IMPLEMENT PLATFORM PROTECTION

Microsoft CERTIFIED AZURE SECURITY ENGINEER ASSOCIATE

22

Which of the following can be associated to a Network Security Group (NSG)? Select all that apply.

1. Virtual Network (VNET)
2. Subnet
3. Resource Group
4. Network Interface Card (NIC)

0:15

DOMAIN 2: IMPLEMENT PLATFORM PROTECTION

22 ANSWER

2. Subnet and 4. NIC

You can configure NSGs on subnet and Network Interface Card (NIC) and may be used together if desired.

DOMAIN 2: IMPLEMENT PLATFORM PROTECTION

Microsoft
CERTIFIED
AZURE SECURITY
ENGINEER
ASSOCIATE

23

Which of the following options can be used to create custom RBAC roles? Select all that apply.

1. Azure PowerShell
2. Azure CLI
3. REST API
4. ARM Template

0:15

DOMAIN 2: IMPLEMENT PLATFORM PROTECTION

23 ANSWER

1. Azure PowerShell, 2. Azure CLI, 3. REST API

All are valid options for creating custom RBAC roles except ARM template. You can configure an existing custom RBAC role with an ARM template.

DOMAIN 2: IMPLEMENT PLATFORM PROTECTION

Microsoft
CERTIFIED
AZURE SECURITY ENGINEER
ASSOCIATE

24

You need to configure a reverse proxy for TLS termination for inbound access to an Azure Kubernetes cluster. What option do you deploy?

1. Azure Firewall
2. Ingress Controller
3. Container Network Interface (CNI) plug-in
4. Azure Application Gateway

0:15

24 ANSWER

2. Ingress Controller

An **ingress controller** is a piece of software that provides reverse proxy, configurable traffic routing, and TLS termination for Kubernetes services.

DOMAIN 2: IMPLEMENT PLATFORM PROTECTION

Microsoft CERTIFIED
AZURE SECURITY ENGINEER
ASSOCIATE

25 Microsoft Defender for Cloud includes a "quick fix" option to add a vulnerability assessment solution to your Azure virtual machines. Which partner option is integrated with Defender for this feature?

1. Rapid7
2. Nessus
3. Qualys
4. Thales

0:15

DOMAIN 2: IMPLEMENT PLATFORM PROTECTION

25 ANSWER

3. Qualys

This VM scanning capability from **Qualys** was incorporated into the Standard tier of Microsoft Defender for Cloud with simplified deployment for free.

DOMAIN 2: IMPLEMENT PLATFORM PROTECTION

Microsoft CERTIFIED AZURE SECURITY ENGINEER ASSOCIATE

26

The following security principals may be granted rights to a resource group:

1. Service Principal
2. Managed Identity
3. Azure AD User
4. All of the above

0:15

DOMAIN 2: IMPLEMENT PLATFORM PROTECTION

26 ANSWER

4. All of the above

Options 1, 2, and 3 are all security principals to which resource group access may be granted.

DOMAIN 2: IMPLEMENT PLATFORM PROTECTION

Microsoft CERTIFIED AZURE SECURITY ENGINEER ASSOCIATE

27

What are the options for configuring a custom RBAC role in Azure AD? (choose the best answer)

1. PowerShell
2. Azure Portal
3. REST API
4. All of the above

0:15

DOMAIN 2: IMPLEMENT PLATFORM PROTECTION

Microsoft CERTIFIED AZURE SECURITY ENGINEER ASSOCIATE

27 ANSWER

4. All of the above

Custom RBAC roles can be configured both in the Azure portal and programmatically.

DOMAIN 2: IMPLEMENT PLATFORM PROTECTION

28

You need to ensure that all your Azure VMs have a consistent operating system configuration at deploy time. Which of the following options would you configure?

1. ARM templates
2. Desired State Configuration (DSC)
3. Application Security Groups
4. Device configuration policies

0:15

DOMAIN 2: IMPLEMENT PLATFORM PROTECTION

28 ANSWER

2. Desired State Configuration (DSC)

DSC will enable policy-based configuration of the OS and is used by management features such as Azure Update Management.

DOMAIN 2: IMPLEMENT PLATFORM PROTECTION

Microsoft CERTIFIED
AZURE SECURITY ENGINEER
ASSOCIATE

29

You are configuring an Azure Firewall instance. You want to ensure all traffic from an Azure subnet going to www.kineteco.com is routed through the Azure Firewall. Which option should you implement?

1. Network Rule
2. Route Table
3. Application Rule
4. Network Security Group (NSG)

0:15

DOMAIN 2: IMPLEMENT PLATFORM PROTECTION

Microsoft CERTIFIED AZURE SECURITY ENGINEER ASSOCIATE

29 ANSWER

For the exam, know the difference between NAT rules, Network rules, and Application rules

3. Application Rule

You can configure application rules that define fully qualified domain names (FQDNs) that can be accessed from a subnet, and network rules that define source address, protocol, destination port and address.

DOMAIN 2: IMPLEMENT PLATFORM PROTECTION

30 Contoso hosts Azure resources which they have shared with guest users from Kineteco Corp. Both orgs have their own Azure AD tenant. Which tenant owns the user lifecycle in this external identity scenario?

1. Account tenant
2. Resource tenant
3. Microsoft
4. It depends

0:15

DOMAIN 2: IMPLEMENT PLATFORM PROTECTION

30 ANSWER

See "Managing external identities in Azure AD" in my LinkedIn Learning course

2. Resource tenant

The resource tenant is Contoso, which owns the lifecycle of guest account access. The account tenant is Kineteco, which owns the credentials in the Kineteco Azure AD tenant that was granted guest access.

DOMAIN 2: IMPLEMENT PLATFORM PROTECTION

31 Which modes are available for rules in Azure Web Application Firewall (WAF)? (choose two)

1. Block mode
2. Prevention mode
3. Detection mode
4. Report-only mode

0:15

DOMAIN 2: IMPLEMENT PLATFORM PROTECTION

Microsoft CERTIFIED
AZURE SECURITY ENGINEER
ASSOCIATE

31 ANSWER

WAF is based on is based on
Core Rule Set (CRS) from OWASP

2. Prevention Mode 3. Detection mode

WAF can be configured to run in the following two modes:
Detection mode: Monitors and logs all threat alerts.
Prevention mode: Blocks intrusions and attacks that the rules detect.

See "Create and configure Web App Firewall" in my 'AZ-500 Exam Prep 2' course

DOMAIN 2: IMPLEMENT PLATFORM PROTECTION

Microsoft CERTIFIED AZURE SECURITY ENGINEER ASSOCIATE

32 How do you enable the Basic tier of Azure DDoS for your Azure subscriptions?

1. Configure an Azure DDoS instance
2. Enable Azure DDoS within Microsoft Defender
3. No action is necessary

0:15

DOMAIN 2: IMPLEMENT PLATFORM PROTECTION

32 ANSWER

3. No action is necessary

Azure DDoS Basic is enabled by default in the Azure platform, which constantly monitors traffic and enforces real-time mitigation of the most common network attacks. No configuration is required for the Basic tier.

DOMAIN 2: IMPLEMENT PLATFORM PROTECTION

Microsoft
CERTIFIED
AZURE SECURITY
ENGINEER
ASSOCIATE

33 You want to ensure access for all Azure SQL instances from a specific VNET does not traverse the public Internet. Which solution will you implement?

1. Private Link
2. Service Endpoint
3. Private Endpoint
4. Site-to-Site VPN

0:15

DOMAIN 2: IMPLEMENT PLATFORM PROTECTION

Microsoft CERTIFIED
AZURE SECURITY ENGINEER
ASSOCIATE

33 ANSWER

Know the differences between Private Link, Private Endpoint, and Service Endpoint

2. Service Endpoint

Service endpoint is configured at the VNET level for all instances of a PaaS service, optimizing traffic routing over the Azure backbone network. The destination IP is still a public IP (but accessed via the Azure backbone).

See the videos for these three services in my 'AZ-500 Exam Prep 2' course

DOMAIN 3: MANAGE SECURITY OPERATIONS

Microsoft CERTIFIED AZURE SECURITY ENGINEER ASSOCIATE

01

Azure Monitor can be used to alert on events of interest to Security Operations (SecOps).

TRUE or FALSE?

0:15

DOMAIN 3: MANAGE SECURITY OPERATIONS

Microsoft
CERTIFIED
AZURE SECURITY ENGINEER
ASSOCIATE

01 ANSWER

TRUE

Events from the Administrative and Security categories of the Activity Log are definitely of interest to SecOps.

DOMAIN 3: MANAGE SECURITY OPERATIONS

Microsoft CERTIFIED
AZURE SECURITY ENGINEER
ASSOCIATE

02

Which Microsoft tool is designed to help identify and mitigate potential application security issues early in the software development lifecycle (SDLC)?

1. Microsoft Defender for Cloud
2. Microsoft Threat Modeling Tool
3. Microsoft Compliance Manager
4. Microsoft Defender for Cloud Apps

0:15

DOMAIN 3: MANAGE SECURITY OPERATIONS

02 ANSWER

2. Microsoft Threat Modeling Tool

The Microsoft Threat Modeling Tool enables software architects to evaluate designs using the **STRIDE** threat modeling methodology.

DOMAIN 3: MANAGE SECURITY OPERATIONS

Microsoft CERTIFIED AZURE SECURITY ENGINEER ASSOCIATE

03

The VM vulnerability scanning feature in Microsoft Defender can also scan for vulnerabilities in open-source databases on Azure VMs.

TRUE or FALSE?

0:15

DOMAIN 3: MANAGE SECURITY OPERATIONS

03 ANSWER

FALSE

Only Microsoft SQL on VMs is available.

3. MANAGE SECURITY OPERATIONS

04

The free tier of Microsoft Defender for Cloud can identify deficiencies in baseline Azure network configuration, such as a subnet without a network security group (NSG).

TRUE or FALSE?

0:15

3. MANAGE SECURITY OPERATIONS

04 ANSWER

TRUE

Intelligence, hybrid, threat protection (formerly ATP), and regulatory compliance require the Standard tier

The free tier of Microsoft Defender for Cloud does identify configurations that deviate from best practices for network resources, as well as storage, compute, and other services.

3. MANAGE SECURITY OPERATIONS

Microsoft CERTIFIED
AZURE SECURITY ENGINEER
ASSOCIATE

05

The Free tier of Microsoft Defender for Cloud allows you to change the default policy to disable checks that you wish to ignore.

TRUE or FALSE?

0:15

3. MANAGE SECURITY OPERATIONS

05 ANSWER

TRUE

Yes, you can change the default Microsoft Defender policy settings, even in the Free tier.

3. MANAGE SECURITY OPERATIONS

06

Just-in-Time VM access allows the requester to specify duration of access up to the configured maximum.

TRUE or FALSE?

0:15

3. MANAGE SECURITY OPERATIONS

06 ANSWER

TRUE

The requester is able to specify how much time is needed, up to the maximum the service has been configured to allow for the specific VM.

DOMAIN 3: MANAGE SECURITY OPERATIONS

07

Microsoft Defender for Cloud recommendations are listed in descending order of the severity of the security vulnerabilities they address.

TRUE or FALSE?

0:15

DOMAIN 3: MANAGE SECURITY OPERATIONS

07 ANSWER

FALSE

Recommendations are listed in descending order of the point value (impact) to the Security Score.

DOMAIN 3: MANAGE SECURITY OPERATIONS

08

Which of the following solutions features automated security investigations?

1. Microsoft Defender for Endpoint
2. Microsoft Defender for Cloud
3. Azure Monitor
4. Microsoft Sentinel

0:15

DOMAIN 3: MANAGE SECURITY OPERATIONS

08 ANSWER

1. Microsoft Defender for Endpoint

Only Microsoft Defender for Endpoint includes an automated investigation feature (as of Jan 2022).

Response automation is possible in Sentinel with playbooks, but is not full-scale automated investigation

DOMAIN 3: MANAGE SECURITY OPERATIONS

Microsoft
CERTIFIED
AZURE SECURITY
ENGINEER
ASSOCIATE

09

Which of the following logs capture control plane operations in your Azure subscription?

1. Metrics
2. Diagnostic Log
3. Activity Log
4. Subscription Log

0:15

DOMAIN 3: MANAGE SECURITY OPERATIONS

09 ANSWER

4. Activity Log

Activity logs provide information about Azure Resource Manager control plan operations like CREATE, UPDATE, and DELETE operations.

DOMAIN 3: MANAGE SECURITY OPERATIONS

Microsoft
CERTIFIED
AZURE SECURITY ENGINEER
ASSOCIATE

10 When you don't know how long you need to retain data in a blob, you can configure a legal hold.

TRUE or FALSE?

0:15

DOMAIN 3: MANAGE SECURITY OPERATIONS

10 ANSWER

TRUE

A legal hold remains in place until you release it, preventing the blob from being deleted.

DOMAIN 3: MANAGE SECURITY OPERATIONS

Microsoft CERTIFIED

AZURE SECURITY ENGINEER

ASSOCIATE

11

You are configuring Azure Policy. Which of the following policy effects require you to assign a managed identity? (Choose two)

1. Append
2. AuditIfNotExists
3. Modify
4. DeployIfNotExists

0:15

DOMAIN 3: MANAGE SECURITY OPERATIONS

11 ANSWER

3. Modify, 4. DeployIfNotExists

Because they are write actions, **Modify** and **DeployIfNotExists** require a managed identity to succeed.

DOMAIN 3: MANAGE SECURITY OPERATIONS

12

You are deploying VMs using ARM templates. You want to include enrollment into Azure Log Analytics as part of the deployment. Which two parameters must you include in the ARM template?

1. WorkspaceID
2. AccessKey
3. WorkspaceKey
4. WorkspaceName

0:15

DOMAIN 3: MANAGE SECURITY OPERATIONS

12 ANSWER

1. WorkspaceID, 3. WorkspaceKey

You will need to provide the Log Analytics **WorkspaceID** and **WorkspaceKey** for the VM extension that deploys the agent.

DOMAIN 3: MANAGE SECURITY OPERATIONS

13

Which Azure platform log captures data plane events?

1. Resource Log
2. Activity Log
3. Azure AD Log
4. Audit Log

0:15

DOMAIN 3: MANAGE SECURITY OPERATIONS

13 ANSWER

1. Resource Log

Resource logs provide insight into operations that were performed within an Azure resource (the data plane)

DOMAIN 3: MANAGE SECURITY OPERATIONS

Microsoft CERTIFIED
AZURE SECURITY ENGINEER
ASSOCIATE

14

Playbooks in Microsoft Sentinel are based on which of the following technologies?

1. Azure Automation Runbooks
2. Jupyter Notebooks
3. Azure Logic Apps
4. Azure Functions

0:15

DOMAIN 3: MANAGE SECURITY OPERATIONS

14 ANSWER

3. Azure Logic Apps

Security playbooks are based on Logic Apps and include specific triggers and actions to automate response to alerts in Microsoft Sentinel.

DOMAIN 3: MANAGE SECURITY OPERATIONS

Microsoft CERTIFIED
AZURE SECURITY ENGINEER
ASSOCIATE

15 Which Microsoft Sentinel RBAC role is required to allow an analyst to manage incidents (assign, dismiss, etc.)? (choose the best answer)

1. Microsoft Sentinel Reader
2. Microsoft Sentinel Responder
3. Microsoft Sentinel Contributor
4. Microsoft Sentinel Automation Contributor

0:15

DOMAIN 3: MANAGE SECURITY OPERATIONS

15 ANSWER

4. Microsoft Sentinel Responder

Microsoft Sentinel Responder can manage incidents (assign, dismiss, etc.). So can the Microsoft Sentinel Contributor, but that role also includes authoring rights.

Remember "least privilege access"

DOMAIN 3: MANAGE SECURITY OPERATIONS

Microsoft
CERTIFIED
AZURE SECURITY
ENGINEER
ASSOCIATE

16

Which of the following statements is true for an Azure Policy initiative? An initiative is:

1. A policy assignment
2. A policy assignment scope
3. A collection of policies
4. A policy definition

0:15

DOMAIN 3: MANAGE SECURITY OPERATIONS

Microsoft CERTIFIED
AZURE SECURITY ENGINEER
ASSOCIATE

16 ANSWER

3. A collection of policies

An Azure initiative is a collection of Azure policy definitions that are grouped together towards a specific goal or purpose in mind.

DOMAIN 3: MANAGE SECURITY OPERATIONS

Microsoft
CERTIFIED
AZURE SECURITY ENGINEER
ASSOCIATE

17

Which of the following are advantages of Azure Bastion over traditional remote desktop access?

1. The session is managed in the browser
2. No public IP addresses are necessary
3. Uses standard RDP ports
4. Supports both Windows and Linux VMs

0:15

17 ANSWER

1) Browser-based and 2) Uses private IPs

Azure Bastion provides remote access directly from the Azure portal over port 443, connecting to private IP addresses of the target Azure VMs.

DOMAIN 3: MANAGE SECURITY OPERATIONS

18 In Microsoft Sentinel, __________ are groups of related __________ that together create an actionable potential threat that you can investigate and resolve.

1. Alerts, Incidents
2. Incidents, Events
3. Events, Alerts
4. Incidents, Alerts

0:15

DOMAIN 3: MANAGE SECURITY OPERATIONS

18 ANSWER

4. Incidents, Alerts

Incidents are groups of related alerts that together create an actionable, potential threats that you can investigate and resolve. Microsoft Sentinel uses analytics and machine learning rules to correlate low fidelity alerts into high fidelity incidents.

DOMAIN 3: MANAGE SECURITY OPERATIONS

Microsoft CERTIFIED
AZURE SECURITY ENGINEER
ASSOCIATE

19

Azure Policy allows the assignment of a policy to a management group. What level of scope is affected by a policy targeted to a management group?

1. All Azure subscriptions
2. All resource groups in a subscription
3. All subscriptions in the management group
4. Resource groups in the management groups

0:15

DOMAIN 3: MANAGE SECURITY OPERATIONS

19 ANSWER

3. All subscriptions in the management group

A management group facilitates targeting policy to multiple subscriptions of your choosing, or all subscriptions in the tenant if you target the root group.

DOMAIN 3: MANAGE SECURITY OPERATIONS

Microsoft CERTIFIED AZURE SECURITY ENGINEER ASSOCIATE

20

When creating alert rules in Azure Monitor for events in the Azure Activity log, what must you configure to notify users when an alert is triggered?

1. Resource
2. Action group
3. Target criteria
4. Alert logic

0:15

Microsoft CERTIFIED AZURE SECURITY ENGINEER ASSOCIATE

20 ANSWER

2. Action group

An **action group** is a collection of notification preferences defined by the owner of an Azure subscription. Azure Monitor and Service Health alerts use action groups to notify users that an alert has been triggered.

DOMAIN 3: MANAGE SECURITY OPERATIONS

Microsoft CERTIFIED

AZURE SECURITY ENGINEER

ASSOCIATE

21

An Azure Bastion host provides ______ and ______ connectivity to workloads sitting behind the bastion host.

1. SSH, HTTPS
2. HTTPS, RDP
3. SSH, RDP
4. RDP, HTTP

0:15

DOMAIN 3: MANAGE SECURITY OPERATIONS

21 ANSWER

3. SSH, RDP

While you connect to the bastion host on 443 from the Azure portal, the bastion provides RDP (Windows) and SSH (Linux) connectivity to Azure VMs.

DOMAIN 3: MANAGE SECURITY OPERATIONS

Microsoft CERTIFIED AZURE SECURITY ENGINEER ASSOCIATE

22

Just-in Time VM Access and Azure Bastion are designed to work together.

TRUE or FALSE?

0:15

DOMAIN 3: MANAGE SECURITY OPERATIONS

22 ANSWER

FALSE

The JIT VM Access feature provides a gated solution for RDP and SSH to public IPs. Azure Bastion provides remote access via a browser and Azure portal using a VMs private IP.

DOMAIN 3: MANAGE SECURITY OPERATIONS

23

Playbooks in Microsoft Sentinel use a special ______ to instantiate an automated response using an Azure Logic App.

1. Action
2. Trigger
3. Condition
4. Connector

0:15

DOMAIN 3: MANAGE SECURITY OPERATIONS

23 ANSWER

2. Trigger

Security playbooks are Azure Logic Apps that use a special trigger designed for Microsoft Sentinel.

DOMAIN 3: MANAGE SECURITY OPERATIONS

24

You notice that when you attempt to investigate an incident created from your custom rule in Microsoft Sentinel that the investigation graph is empty. What is the most likely cause?

1. Rule is disabled
2. Permissions (RBAC)
3. Query syntax
4. Entity mapping

0:15

DOMAIN 3: MANAGE SECURITY OPERATIONS

24 ANSWER

4. Entity mapping

You'll only be able to investigate the incident if you used the **entity mapping** fields when you set up your analytics rule. The investigation graph requires that your original incident includes entities.

DOMAIN 4. SECURE DATA AND APPLICATIONS

Microsoft
CERTIFIED
AZURE SECURITY
ENGINEER
ASSOCIATE

01

You can configure Azure AD authentication for which of the following?

1. Queues, Blobs
2. Queues, Blobs, Files
3. Queues, Blobs, Tables
4. Queues, Files

0:15

DOMAIN 4. SECURE DATA AND APPLICATIONS

01 ANSWER

1. Queues, Blobs

Only Azure Storages queues and blobs support Azure AD authentication.

DOMAIN 4. SECURE DATA AND APPLICATIONS

Microsoft CERTIFIED
AZURE SECURITY ENGINEER
ASSOCIATE

02

Microsoft Defender for App Service can be enabled for an App Service plan only if the plan is associated with dedicated machines.

TRUE or FALSE?

0:15

DOMAIN 4. SECURE DATA AND APPLICATIONS

Microsoft CERTIFIED
AZURE SECURITY ENGINEER
ASSOCIATE

02 ANSWER

FALSE

Microsoft Defender for App Service supports all App Service plans except Azure Functions on the consumption plan.

DOMAIN 4. SECURE DATA AND APPLICATIONS

03

With Azure SQL, you can configure Azure AD Domain Services authentication.

TRUE or FALSE?

0:15

DOMAIN 4. SECURE DATA AND APPLICATIONS

Microsoft CERTIFIED
AZURE SECURITY ENGINEER
ASSOCIATE

03 ANSWER

FALSE

Azure SQL supports Azure AD authentication, but not Azure AD Domain Services authentication.

DOMAIN 4. SECURE DATA AND APPLICATIONS

04

Azure Disk Encryption uses Bitlocker to encrypt OS and data volumes.

TRUE or FALSE?

0:15

DOMAIN 4. SECURE DATA AND APPLICATIONS

04 ANSWER

TRUE

DM-CRYPT is used for Linux VMs

Azure Disk Encryption does utilize Bitlocker, but only for Windows machines.

DOMAIN 4. SECURE DATA AND APPLICATIONS

Microsoft
CERTIFIED
AZURE SECURITY ENGINEER
ASSOCIATE

05

You need to obfuscate data in Azure SQL at the record level. Which feature will you use?

1. Transparent data encryption
2. Microsoft Defender for SQL
3. Azure AD authentication
4. Dynamic data masking

0:15

05 ANSWER

4. Dynamic data masking

Dynamic data masking (sometimes simply called “dynamic masking” enables partially obscuring sensitive data, like a credit card number or email address.

Examples ****-****-****-4656 or pete.****@****.com

DOMAIN 4. SECURE DATA AND APPLICATIONS

Microsoft CERTIFIED AZURE SECURITY ENGINEER ASSOCIATE

06 Shared access signature (SAS) tokens can be configured to restrict access by IP address.

TRUE or FALSE?

0:15

DOMAIN 4. SECURE DATA AND APPLICATIONS

Microsoft CERTIFIED
AZURE SECURITY ENGINEER
ASSOCIATE

06 ANSWER

TRUE

Yes, SAS tokens can restrict access to specific IPs or IP ranges, for specific resources, and if desired, for a limited period of time.

DOMAIN 4. SECURE DATA AND APPLICATIONS

Microsoft
CERTIFIED
AZURE SECURITY ENGINEER
ASSOCIATE

07

SAS tokens provide root access to an Azure Storage account until the key is revoked or rolled.

TRUE or FALSE?

0:15

DOMAIN 4. SECURE DATA AND APPLICATIONS

07 ANSWER

FALSE

This describes Shared Keys. SAS tokens are restricted to specified permissions for a limited period of time (specified at creation time).

DOMAIN 4. SECURE DATA AND APPLICATIONS

Microsoft CERTIFIED

AZURE SECURITY ENGINEER

ASSOCIATE

08

Microsoft Defender for SQL can scan your Azure SQL databases weekly to identify vulnerabilities.

TRUE or FALSE?

0:15

DOMAIN 4. SECURE DATA AND APPLICATIONS

08 ANSWER

TRUE

You can also set custom baselines for permissions and feature configurations, and database settings.

The service can also scan SQL Managed Instance Database and Azure Synapse.

DOMAIN 4. SECURE DATA AND APPLICATIONS

Microsoft CERTIFIED AZURE SECURITY ENGINEER ASSOCIATE

09

You can enforce data residency and sovereignty using which of the following?

1. Microsoft Defender for Cloud
2. Azure Policy
3. Azure Storage Encryption
4. Azure Automation

0:15

DOMAIN 4. SECURE DATA AND APPLICATIONS

Microsoft CERTIFIED AZURE SECURITY ENGINEER ASSOCIATE

09 ANSWER

2. Azure Policy

Azure Policy enables you to configure an "allowed locations" policy to limit deployments to your approved Azure regions only.

DOMAIN 4. SECURE DATA AND APPLICATIONS

10

You can use Azure AD authentication to secure Key Vault at the management plane.

TRUE or FALSE?

0:15

DOMAIN 4. SECURE DATA AND APPLICATIONS

10 ANSWER

TRUE

You can secure a Key Vault instance using Azure AD authentication.

DOMAIN 4. SECURE DATA AND APPLICATIONS

Microsoft CERTIFIED

AZURE SECURITY ENGINEER

ASSOCIATE

11

Microsoft Defender for Cloud uses Azure policy to configure default monitoring and remediation behaviors.

TRUE or FALSE?

0:15

DOMAIN 4. SECURE DATA AND APPLICATIONS

Microsoft
CERTIFIED
AZURE SECURITY ENGINEER
ASSOCIATE

11 ANSWER

TRUE

and can be customized even on the Free tier

Yes, Microsoft Defender for Cloud includes a default Azure policy containing a number of default settings that control monitoring and remediation behavior.

DOMAIN 4. SECURE DATA AND APPLICATIONS

Microsoft CERTIFIED AZURE SECURITY ENGINEER ASSOCIATE

12

You can limit operations on a key in Azure Key Vault by configuring the settings under Permitted operations.

TRUE or FALSE?

0:15

DOMAIN 4. SECURE DATA AND APPLICATIONS

12 ANSWER

TRUE

You can limit a variety of operations under Permitted operations, like Encrypt, Decrypt, Sign, and Verify.

DOMAIN 4. SECURE DATA AND APPLICATIONS

Microsoft CERTIFIED AZURE SECURITY ENGINEER ASSOCIATE

13

You can bind client certificates to which App Service Plan tiers?

1. Isolated only
2. Premium only
3. Standard or Premium
4. Basic, Standard, Premium, or Isolated

0:15

DOMAIN 4. SECURE DATA AND APPLICATIONS

13 ANSWER

4. Basic, Standard, Premium, or Isolated

App Service supports client certificates on Basic, Standard, Premium, or Isolated tiers.

DOMAIN 4. SECURE DATA AND APPLICATIONS

14

Azure Storage accounts are encrypted by default:

1. Always
2. For Premium storage only
3. Only for zone-redundant storage (ZRS)
4. Only for geo-redundant storage (GRS)

0:15

DOMAIN 4. SECURE DATA AND APPLICATIONS

14 ANSWER

1. Always

All Azure Storage accounts are always encrypted by default. Customers can choose to choose to manage their own keys for encrypting the storage service.

DOMAIN 4. SECURE DATA AND APPLICATIONS

15

A resource forest in Azure AD Domain Services will sync accounts from on-premises as well as Azure.

TRUE or FALSE?

0:15

DOMAIN 4. SECURE DATA AND APPLICATIONS

15 ANSWER

FALSE

Only a user forest synchronizes accounts from on-premises Active Directory (AD).

DOMAIN 4. SECURE DATA AND APPLICATIONS

Microsoft
CERTIFIED
AZURE SECURITY
ENGINEER
ASSOCIATE

16

Microsoft recommends shared keys in Azure Storage should be rolled automatically using which core service?

1. Azure App Service
2. Azure Key Vault
3. Logic Apps
4. Azure Functions

0:15

DOMAIN 4. SECURE DATA AND APPLICATIONS

16 ANSWER

2. Azure Key Vault

Microsoft recommends automating rolling of storage account keys exclusively with Key Vault.

DOMAIN 4. SECURE DATA AND APPLICATIONS

17

What are the types of authentication are supported as an access control measure to Azure SQL Database? (Choose two)

1. Passthrough Authentication
2. Certificate Authentication
3. Azure Active Directory (AD) authentication
4. SQL authentication

0:15

DOMAIN 4. SECURE DATA AND APPLICATIONS

17 ANSWER

3. Azure AD auth and 4. SQL auth

You can use traditional **SQL authentication** (user and password) or enable **Azure AD authentication**. Your apps can use a connection string, but this will generally leverage SQL authentication

DOMAIN 4. SECURE DATA AND APPLICATIONS

Microsoft
CERTIFIED
AZURE SECURITY
ENGINEER
ASSOCIATE

18

You can configure Transparent Data Encryption (TDE) for individual database columns containing your sensitive data.

TRUE or FALSE?

0:15

DOMAIN 4. SECURE DATA AND APPLICATIONS

18 ANSWER

FALSE

TDE encrypts the storage of an entire database by using a symmetric key called the database encryption key (DEK).

DOMAIN 4. SECURE DATA AND APPLICATIONS

Microsoft CERTIFIED
AZURE SECURITY ENGINEER
ASSOCIATE

19

You cannot configure Always Encrypted for individual database columns containing your sensitive data.

TRUE or FALSE?

0:15

DOMAIN 4. SECURE DATA AND APPLICATIONS

19 ANSWER

FALSE

You can encrypt individual database columns. **Always Encrypted** is a data encryption technology that ensures that sensitive data never appears as plaintext inside the database system.

DOMAIN 4. SECURE DATA AND APPLICATIONS

20

You create a new Azure Key Vault and want to ensure that permanent deletions of secrets, keys, and certificates can be recovered for at least 30 days. Which two settings will you enable?

1. Soft delete
2. Delete lock
3. Purge protection
4. Read-only lock

0:15

Microsoft CERTIFIED AZURE SECURITY ENGINEER ASSOCIATE

20 ANSWER

1. Soft delete, 3. Purge protection

When **soft-delete** is enabled, resources marked as deleted resources are retained for a specified period (90 days by default). **Purge protection** ensures objects cannot be purged during the retention period.

Soft delete is ON by default, but purge protection is OPTIONAL

DOMAIN 4. SECURE DATA AND APPLICATIONS

Microsoft
CERTIFIED
AZURE SECURITY
ENGINEER
ASSOCIATE

21

You need to provide a user access to download content from your Storage Account, limited to 24 hours. Which option should you choose?

1. Storage Account Firewall
2. Shared Key (storage account key)
3. Storage Blob Data Reader RBAC role
4. Shared Access Signatures (SAS)

0:15

DOMAIN 4. SECURE DATA AND APPLICATIONS

21 ANSWER

4. Shared Access Signatures (SAS)

SAS tokens offer a variety of controls to limit time and scope of access, where shared keys offer the equivalent of root access forever.

DOMAIN 4. SECURE DATA AND APPLICATIONS

Microsoft
CERTIFIED
AZURE SECURITY ENGINEER
ASSOCIATE

22

In Azure SQL Database Always Encrypted, two types of column encryption are supported. (Choose both types from the list below)

1. Deterministic
2. Symmetric
3. Randomized
4. Asymmetric

0:15

DOMAIN 4. SECURE DATA AND APPLICATIONS

Microsoft CERTIFIED
AZURE SECURITY ENGINEER
ASSOCIATE

22 ANSWER

1. Deterministic, 3. Randomized

All Azure SQL Database Always Encrypted supports **deterministic** and **randomized** encryption

Deterministic encryption supports equality lookups, joins, and group by operations but is slightly less secure than Randomized.

DOMAIN 4. SECURE DATA AND APPLICATIONS

Microsoft
CERTIFIED
AZURE SECURITY ENGINEER
ASSOCIATE

23

Which is the most accurate description of the Transparent Data Encryption (TDE) feature of Azure SQL Database?

1. Table-level encryption at-rest
2. Row-level encryption in-transit
3. Row-level encryption at-rest
4. Database-level encryption at-rest

0:15

DOMAIN 4. SECURE DATA AND APPLICATIONS

23 ANSWER

4. Database-level encryption at-rest

TDE performs real-time encryption and decryption of the database, associated backups, and transaction log files at rest without requiring changes to the application.

DOMAIN 4. SECURE DATA AND APPLICATIONS

Microsoft
CERTIFIED
AZURE SECURITY ENGINEER
ASSOCIATE

24 Azure storage accounts are exposed to the Internet by default. Access is possible through which of the following methods? (Choose all that apply)

1. Storage account key
2. Shared access signature (SAS)
3. Master key
4. Azure AD (RBAC permissions)

0:15

DOMAIN 4. SECURE DATA AND APPLICATIONS

24 ANSWER

1. Storage account key, 2. SAS, and 4. Azure AD

Storage account key, shared access signature (SAS), and Azure AD are all methods for accessing Azure storage.

DOMAIN 4. SECURE DATA AND APPLICATIONS

Microsoft CERTIFIED AZURE SECURITY ENGINEER ASSOCIATE

25

What PowerShell cmdlet is used to initiate Azure Disk Encryption for a Windows or Ubuntu-based VM in Azure?

1. Set-AzVMDiskEncryptionWindows
2. Set-AzVMDiskEncryptionExtension
3. Set-AzVMDiskEncryptionLinux
4. Set-AzVMDiskEncryption

0:15

DOMAIN 4. SECURE DATA AND APPLICATIONS

25 ANSWER

2. Set-AzVMDiskEncryptionExtension

The cmdlet to enable the disk encryption is the same for Windows or Linux. The **-ExtensionType** parameter is where you specify the OS type (Windows or Linux)

DOMAIN 4. SECURE DATA AND APPLICATIONS

Microsoft CERTIFIED
AZURE SECURITY ENGINEER
ASSOCIATE

26 You need to implement security in SQL server to ensure database admins never see sensitive customer info, such as credit card data, in databases they manage. Which option should you choose?

1. Row-level security
2. Always Encrypted
3. Transparent Data Encryption
4. Dynamic Masking

0:15

DOMAIN 4. SECURE DATA AND APPLICATIONS

26 ANSWER

3. Always Encrypted

Always Encrypted allows clients to encrypt sensitive data inside client applications and never reveal the encryption keys to the Database Engine. As a result, Always Encrypted provides separation between data owner and manager.

DOMAIN 4. SECURE DATA AND APPLICATIONS

27

Which options allow configuration of Key Vault secrets? (Choose all that apply)

1. Azure CLI
2. Azure PowerShell
3. REST API
4. ARM Templates

0:15

DOMAIN 4. SECURE DATA AND APPLICATIONS

27 ANSWER

1,2,3,4 (all in the list)

In addition to PowerShell, Azure CLI, and the REST API, ARM templates can also be used to configure Key Vault secrets.

DOMAIN 4. SECURE DATA AND APPLICATIONS

Microsoft
CERTIFIED
AZURE SECURITY
ENGINEER
ASSOCIATE

28

When securing Azure Key Vault (AKV), you need to secure the 1) AKV instance and the 2) secrets hosted in the key vault. Which controls are used for each? (choose the best answer)

1. 1)RBAC, 2)RBAC
2. 1)RBAC, 2)Access policies or RBAC
3. 1)Access policies, 2)RBAC
4. 1) RBAC or Access policies 2) Access policies

0:15

DOMAIN 4. SECURE DATA AND APPLICATIONS

28 ANSWER

2. 1)RBAC, 2)Access policies or RBAC

You control access to a Key Vault instance (management plane) with role-based access control (RBAC). You can secure secrets, certs, and passwords in the vault (data plane) with access policies or RBAC.

DOMAIN 4. SECURE DATA AND APPLICATIONS

Microsoft
CERTIFIED
AZURE SECURITY
ENGINEER
ASSOCIATE

29

Which of the following Azure tools can be used for detecting and remediating deviations from Microsoft's recommended security baseline for common workloads? (Choose the best answer)

1. Azure Monitor
2. Desired State Configuration
3. Azure Automation
4. Microsoft Defender for Cloud

0:15

DOMAIN 4. SECURE DATA AND APPLICATIONS

29 ANSWER

4. Microsoft Defender for Cloud

This functionality is built into Microsoft Defender for Cloud, even in the Free tier (Resource Security Hygiene). Microsoft offers a step-by-step tutorial on how to create a baseline in Microsoft Defender for Cloud.

DOMAIN 4. SECURE DATA AND APPLICATIONS

Microsoft CERTIFIED
AZURE SECURITY ENGINEER
ASSOCIATE

30

Which of the Azure RBAC roles below will allow you to create custom RBAC roles in Azure? (Choose all that apply)

1. Contributor
2. Owner
3. User Access Administrator
4. Security Administrator

0:15

DOMAIN 4. SECURE DATA AND APPLICATIONS

Microsoft CERTIFIED
AZURE SECURITY ENGINEER
ASSOCIATE

30 ANSWER

2. Owner, 3. User Access Administrator

You need explicit permissions to create custom roles, such as Owner or User Access Administrator

DOMAIN 4. SECURE DATA AND APPLICATIONS

Microsoft CERTIFIED
AZURE SECURITY ENGINEER
ASSOCIATE

31

How does Azure SQL Database provide protection for data at rest?

1. Dynamic Masking
2. Azure Storage Service Encryption
3. Always Encrypted
4. Transparent Data Encryption

0:15

DOMAIN 4. SECURE DATA AND APPLICATIONS

31 ANSWER

4. Transparent Data Encryption

Transparent Data Encryption performs real-time encryption and decryption of the database, associated backups, and transaction log files at rest without requiring changes to the application.

DOMAIN 4. SECURE DATA AND APPLICATIONS

Microsoft
CERTIFIED
AZURE SECURITY ENGINEER
ASSOCIATE

32

What is the minimum Azure Active Directory built-in RBAC role required to manage Azure Key Vault?

1. Key Vault Reader
2. Key Vault Contributor
3. Security Administrator
4. Privileged Role Administrator

0:15

DOMAIN 4. SECURE DATA AND APPLICATIONS

32 ANSWER

2. Key Vault Contributor

To grant access to a user to manage key vaults, you assign a predefined **Key Vault Contributor** role to the user at a specific scope.

DOMAIN 4. SECURE DATA AND APPLICATIONS

Microsoft CERTIFIED
AZURE SECURITY ENGINEER
ASSOCIATE

33

What is the advantage of using an App Service certificate in managing TLS/SSL communication on your web app. (Choose all that apply)

1. Certificate is stored in Azure Key Vault
2. Certificate is issued by a trusted 3rd party provider
3. Certificate is self-signed
4. Certificate renewal is managed by Azure

0:15

DOMAIN 4. SECURE DATA AND APPLICATIONS

Microsoft CERTIFIED AZURE SECURITY ENGINEER ASSOCIATE ★★

33 ANSWER

1. Stored in AKV, 2. Issued by 3rd party, and 4. Renewal managed by Azure

Certificates acquired through this App Service feature are stored in Key Vault, are renewed automatically, and come from a trusted provider, such as Digicert.

DOMAIN 4. SECURE DATA AND APPLICATIONS

Microsoft CERTIFIED

AZURE SECURITY ENGINEER

ASSOCIATE

34

You are configuring security using a managed identity for your custom web app. Which option will minimize administrative effort?

1. User managed identity
2. System managed identity
3. Default managed identity
4. Service principal with Contributor rights

0:15

DOMAIN 4. SECURE DATA AND APPLICATIONS

34 ANSWER

2. System Managed Identity

A **system managed identity** is lower effort than a user managed identity because its password is maintained automatically. It is also deprovisioned automatically when the associated resource is deprovisioned.

INSIDE CLOUD

AND SECURITY

THANKS

FOR WATCHING!