WEEK 10
IDENTITY & ACCESS MANAGEMENT
Q&A

Taha Yiğit ALKAN

Agenda

- Identity, Access, Security
- Azure Active Directory
- Authentication vs Authorization
- Azure AD Conditional Access
- Multi-Factor Authentication
- Paswordless
- Role-Based Access Control
- Microsoft Defender for Cloud

IDENTITY, ACCESS, SECURITY

Virtual Machines, Scale Sets, Virtual Desktops, Web Apps, Functions

“Identity”

“representation of a person, application or a device”

Scott Duffy

Question

TechCorp needs to ensure that different teams have specific permissions when working with Azure resources. Which Azure service allows them to define and enforce access policies by assigning roles to users or groups?

a. Azure Active Directory (Azure AD)
b. Azure Virtual Network
c. Azure Role-Based Access Control (RBAC)
d. Azure App Service

Question

EduTech wants to ensure that its students and staff can securely access educational resources and applications with a single set of credentials. Which Azure service would allow them to achieve centralized identity management and single sign-on?

a. Azure Key Vault
b. Azure Virtual Network
c. Azure Active Directory (Azure AD)
d. Azure Blob Storage

Question

What is the primary role of Azure Active Directory (Azure AD) in identity and access management?

a. To manage containers and orchestrate applications
b. To provide secure networking configurations
c. To centrally manage user identities and access to applications
d. To store and manage unstructured data

Question

FinanceCo wants to add an extra layer of security to user logins, requiring a second form of verification in addition to passwords. Which Azure service can they implement to achieve this enhanced security?

a. Azure Key Vault
b. Azure SQL Database
c. Azure Multi-Factor Authentication (MFA)
d. Azure Functions

Question

What is the primary purpose of Azure Multi-Factor Authentication (MFA)?

a. To manage and store cryptographic keys securely
b. To provide fully managed relational database services
c. To enhance security by requiring multiple forms of verification
d. To deploy and manage containerized applications

Question

EnterpriseX wants to implement policies that restrict access to sensitive data based on conditions such as user location, device compliance, and time of day. Which Azure service allows them to define these conditional access policies?

a. Azure Role-Based Access Control (RBAC)
b. Azure Conditional Access
c. Azure Active Directory (Azure AD)
d. Azure Key Vault

Question

What is the primary purpose of Azure Role-Based Access Control (RBAC)?

a. To manage and store sensitive information securely
b. To create and run serverless functions in the cloud
c. To control access to Azure resources based on roles and permissions
d. To host and scale web applications

Question

In a healthcare organization, which Azure feature can be used to ensure that different departments have specific permissions when accessing Azure resources?

a. Azure Multi-Factor Authentication (MFA)
b. Azure Role-Based Access Control (RBAC)
c. Azure Conditional Access
d. Azure Managed Identity

Question

To add an extra layer of security for user logins, requiring a second form of verification, which Azure service should be implemented?

a. Azure File Sync
b. Azure Multi-Factor Authentication (MFA)
c. Azure Managed Identity
d. Azure Traffic Manager

Question

Which Azure service allows an organization to securely collaborate with external partners by enabling them to use their own credentials for accessing specified resources?

a. Azure Blob Storage
b. Azure AD B2B
c. Azure Data Box
d. Azure Virtual Network

Question

What sets Zero Trust apart from traditional security models regarding authentication?

a. Single sign-on for all users
b. Periodic password changes
c. Continuous and adaptive authentication
d. Static access controls based on job roles

Question

How does Zero Trust approach data protection?

a. By allowing unrestricted access to sensitive data
b. Relying on network firewalls for data security
c. Encrypting data at rest and in transit, regardless of network location
d. Depending on perimeter security for data confidentiality

Question

What is the primary goal of the Defense in Depth strategy?

a. To focus solely on perimeter security
b. To rely on a single layer of security controls
c. To provide redundancy in case of a security breach
d. To create multiple layers of security to protect against various threats

THANK YOU

Taha Yiğit ALKAN
yigitalkan@akdeniz.edu.tr