



# Azure Security – Securing Data and Applications

Aligned with Microsoft Certification Exam AZ-500

[ine.com](https://ine.com)



# Tracy Wallace

Azure Solutions Architect Expert



twallace@ine.com



@TracyWallaceINE



linkedin.com/in/tracy-wallace-746482a



# Course Topics

**Data Security Policy**  
**Data Infrastructure Security**  
**Data Encryption**  
**Application Security**

# AZ-500 Objective Domains

- + Manage identity and access (30 - 35%)
- + Implement platform protection (15 - 20%)
- + Manage security operations (25 - 30%)
- + **Secure data and applications (20 - 25%)**



# Exam AZ-500: Microsoft Azure Security Technologies

## + Configure security for storage

- + configure access control for storage accounts
- + configure key management for storage accounts
- + configure Azure AD authentication for Azure Storage
- + configure Azure AD Domain Services authentication for Azure Files
- + create and manage Shared Access Signatures (SAS)
- + create a shared access policy for a blob or blob container
- + configure Storage Service Encryption

## + Configure security for databases

- + enable database authentication
- + enable database auditing
- + configure Azure SQL Database Advanced Threat Protection
- + configure security for Azure SQL
- + implement database encryption
- + implement Azure SQL Database Always Encrypted

## + Configure and manage Key Vault

- + manage access to Key Vault
- + manage permissions to secrets, certificates, and keys
- + configure RBAC usage in Azure Key Vault
- + manage certificates
- + manage secrets
- + configure key rotation
- + backup and restore of Key Vault items

Pre-requisites

**Azure Fundamentals**  
**Azure Administrations**



# Data Security in Azure

# Data Security in Azure

- Data Classification
- Demo: Data Classification
- Data Retention
- Demo: Data Retention
- Data Sovereignty

# Data Classification

- + Classify resources based on data risk
  - + What is the impact of a data breach
- + Consider type of data, business criticality, and financial responsibility
- + Microsoft internal classifications
  - + Non-business
  - + Public
  - + General
  - + Confidential
  - + Highly confidential
- + Enforce tagging to add data classification metadata
- + Utilize governance guides from the Microsoft cloud adoption framework
- + SQL Server advanced data security

# ▣ Demo: Data Classification

# Data Retention



Long-term data retention



Backed up every 4 hours, 2 backups retained



Retained up to 35 days



Backup policy



Up to 2 years



Blob storage archive tier

# Demo: Data Retention



# Data Sovereignty

- + Sovereign clouds
- + Azure "geo"s represent regions within geo-political boundaries
  - + Data may be replicated between regions in a geo
  - + Brazil is an exception
- + Exceptions to geo rules for regional resources
  - + Cloud services (obsolete)
  - + LUIS
  - + Machine learning
  - + Azure sentinel
  - + Pre-release (preview)
- + Global services
  - + Azure AD
  - + CDN
  - + MFA
  - + Security center
- + Azure security policy – control region
- + No limit to access location



# Database Security

# Database Security

- Database Authentication
- PaaS Database Security Services
- Azure PaaS Database Advanced Threat Protection
- Demo: Azure SQL Database Security

# Database Authentication

- + Infrastructure
- + PaaS

- SQL Server – Windows and SQL Server
- MySQL – Plugins: PAM, Windows and LDAP
- PostgreSQL – over 10 authentication methods
- MariaDB – pluggable authentication

# Database Authentication

- + Infrastructure
- + PaaS

# PaaS Database Security Services

- + Encryption
  - + At rest
  - + In transit
- + Audit logging
- + Firewall rules and service endpoints
- + Threat protection

# Azure PaaS Database Advanced Threat Protection

- + Integrated with Azure security center
- + Alerts
  - + SQL injection vulnerability\*
  - + Potential SQL injection\*
  - + Access from unusual location/Azure data center
  - + Access from unfamiliar principal
  - + Access from potentially harmful application
  - + Brute force attack

\*Azure SQL database only as of June 2020.



# Demo: Azure SQL Database Security





# Data Auditing in Azure

# Data Auditing in Azure

- + Azure SQL Auditing
- + **Demonstration:** Auditing an Azure SQL Database

# Azure SQL Auditing



# **Storage Account Security Architecture**

# Storage Account Security Architecture

- Storage Security
- Traditional Storage Account Authentication Options
- Azure AD Authentication for Storage Accounts
- Demo: Azure AD Authentication for Storage Accounts

# Storage Security

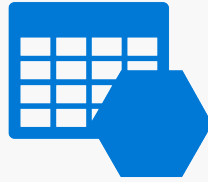
- + Storage encryption
- + Access control
- + Availability and durability
- + Network access control
- + CORS

# Traditional Storage Account Security Options

# Azure AD Authentication for Storage Accounts



# **Demo: Azure AD Authentication for Storage Accounts**



# Storage Account Keys

---



# Storage Account Keys

---

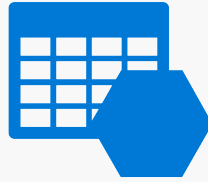
- ▶ Using storage account keys
- ▶ Securing storage account keys
- ▶ Demonstration: Access a storage account with a key

# Storage Account Keys

- Using storage account keys
  - Always need a context. Based on name/key, SAS, or connection string
  - Web apps – App Settings
  - File shares – required for SMB shares
  - Other applications
- Protecting keys
  - Web app settings are in clear text
  - Azure key vault

# Storage Account Keys Take-aways

- When to use keys – Web apps, services, SMB shares
- Protecting keys – Azure key vault
- Generating keys
  - CLI: `az storage account keys renew`
  - PowerShell: `New-AzStorageAccountKey`
  - REST API: POST  
`https://management.azure.com/subscriptions/{subscriptionId}/resourceGroups/{resourceGroupName}/providers/Microsoft.Storage/storageAccounts/{accountName}/regenerateKey?api-version=2018-11-01`



# Shared Access Signatures

---



# Shared Access Signatures

---

- ▶ Shared access signatures
- ▶ Access policy
- ▶ Demonstration: Generate and use a shared access signature

# Shared Access Signatures

- Level
  - Storage account (service)
  - Collection (container, share, table, queue)
  - Item (blob, file, entity, message)
- Permissions – Read, Create, Update, Delete, List
- Timeframe – Start, Expiration
- IP Address filtering
- Policy



# Shared Access Signatures

## ▶ Example

sp= Example st= se= spr= sv=  
+ r sig= sr= 2019-05-08T20:51:55Z 2019-05-  
09T04:51:55Z https 2018-03-  
28 94KTCbiu2U93yOKkWDmOc6g53fOiSDIMexGLw6O5VcU%3D b

# Shared Access Signature Take-aways

- + SAS elements
- + Creating a SAS token
  - + Ad-hoc
  - + Policy-based
- + Using a SAS token
  - + Command line
  - + SDK
  - + REST API



# **Azure AD Domain Services Authentication for Azure Files**

# Azure AD Domain Services Authentication for Azure Files

- File Service Access and Authorization
- Azure AD DS for File Service

# File Service Access and Authorization

# Azure AD DS for File Service

- + Integrates with Azure AD DS and on-premises active directory
  - + On-premises in preview as of April 2020
- + Permissions apply to SMB
- + Storage account key gives super user access
- + Set permissions through Windows explorer, icaccls, Set-ACL
- + Permissions preserved on copy
  - + File sync
  - + Common file movement tools (robocopy)



# Data Encryption At Rest and In Transit

---



# Data Encryption At Rest and In Transit

---

- ▶ Encrypting Data At Rest With Azure
- ▶ Encrypting Data In Transit With Azure
- ▶ Demonstration: Data Encryption At Rest and In Transit





# Encrypt Data With Always Encrypted

---



# Encrypt Data With Always Encrypted

---

- ▶ What is Always Encrypted?
- ▶ Demonstration: Using Always Encrypted



# Azure Disk Encryption

---



# Azure Disk Encryption

---

- ▶ Disk encryption overview
- ▶ Demonstration: Encrypt a VHD

# Azure Disk Encryption Scenarios

- ▶ Encrypt new or existing Azure VMs
- ▶ Create new VMs based on pre-encrypted VHDs and encryption keys
- ▶ Encrypt Windows virtual machine scale sets.
- ▶ Encrypt Linux virtual machine scale set data drives.
- ▶ Disable encryption on Windows VMs.
- ▶ Disable encryption on data drives for Linux VMs.
- ▶ Disable encryption on Windows virtual machine scale sets.
- ▶ Disable encryption on data drives for Linux virtual machine scale sets.
- ▶ Update encryption settings of an existing encrypted VMs.
- ▶ Back up and restore encrypted VMs.

# Azure Disk Encryption

- Pre-requisites:
  - Supported OS
  - Networking – connect to Azure AD, connect to key vault, extension storage access
  - Windows requirements – Bitlocker policy (GPO)
  - Linux requirements – 7GB RAM, vfat, /etc/fstab
- Key vault:
  - Same region as VM
  - Advanced access policy
  - Add a key encryption key (KEK) – optional
- Encrypt – PowerShell, CLI, template

# Azure Disk Encryption Take-aways

- Disk encryption options:
  - Storage – managed vs unmanaged
  - OS disk – BitLocker, DM-Crypt
- Managed disk encryption:
  - Pre-requisites
  - Process



# Security for Azure PaaS Resources



## Security for Azure PaaS Resources

- Security for HDInsight
- Security for Cosmos DB
- Security for Azure Data Lake

# Security for HDInsight

- + HDInsight is "sort of" PaaS
- + Traditionally a single-user cluster
- + Enterprise security package for HDInsight
  - + Leverages Azure AD DS
- + Encryption at rest
- + Customer responsibility
  - + Network security
  - + OS security and patching
  - + App level security
    - + Apache Ranger
    - + Log analytics
  - + Storage security

# Security for Cosmos DB

- + Encryption at rest
- + Network security
  - + IP address ACL firewall
  - + Service endpoint
- + Authentication
  - + Key-based - master and read-only
  - + Granular – tokens for resource access
    - + Users
    - + Permissions – Containers and below
- + Azure ARM – down to containers

# Security for Cosmos DB

## Resource Access Token



# Security for Azure Data Lake

- + Generation 1
  - + Authentication - Azure AD
  - + Authorization - POSIX ACLs
  - + IP-based firewall
  - + Encryption at rest and in transit
- + Generation 2
  - + Integrated with blob storage
  - + Integrates with Azure AD
  - + ACL-based – read, write, execute



# **Configure Azure Services to Protect Web Apps**

# Configure Azure Services to Protect Web Apps

- Web App Protection Options
- Service Endpoints
- Web Application Firewall
- Security Center
- Demo: Protect a Web App

# Web App Protection Options



# Web App Protection Options

- + Authentication
- + Service endpoints
- + Application gateway, front door, web application firewall
- + Encryption settings
- + Managed identity
- + Deep diagnostics
- + Key vault integration

# Protect Web Apps

Service Endpoints

Web Application Firewall

Security Center

Service Endpoints  
Web Application Firewall  
Security Center

## Protect Web Apps

- + Component of application gateway and front door
  - Application gateway – regional
  - Front door - global
- + Protects against
  - SQL-injection
  - Cross-site scripting
  - Other common web attacks
  - HTTP protocol violations and anomalies
  - Crawlers and scanners
  - Other vulnerabilities
  - Custom rules

# Protect Web Apps

Service Endpoints

Web Application Firewall

Security Center

Service Endpoints  
Web Application Firewall  
Security Center

## Protect Web Apps

- + Requires security center standard tier
- + Protects
  - Web apps
  - Function apps
  - App service environments

# Demo: Protect a Web App



# Configure SSL/TLS Certs

## Configure SSL/TLS Certs

- TLS Certificates in App Services
- SSL/TLS Termination
- Custom Storage Account Domains
- Azure AD Certificates
- Demo: Web App Certificates



# TLS Certificates in App Services

- + Require HTTPS
- + Choose TLS 1.2 (or later)
- + Bind certificates for custom domains

# SSL/TLS Termination

# Custom Storage Account Domains

- + Storage accounts can have custom domains
- + Storage accounts cannot use custom certificates
- + Consider a CDN if you need a custom domain for storage
- + Determine whether you actually need a custom domain

# Azure AD Certificates

- + Certificate-based authentication for service principals
- + Certificates for application identity
- + Certificates for ADFS

# Demo: Web App Certificates



# Using the KeyVault API

---



# Using the KeyVault API

---

- ▶ Azure Key Vault
- ▶ Using the Azure Key Vault API to Manage Sensitive Data
- ▶ Demonstration: Using the Azure Key Vault API to Manage Sensitive Data