



# AZ-500: Microsoft Azure Security Engineer

Review and Preparation

ine.com

<https://t.me/learningnets>





# Tracy Wallace

Azure Solutions Architect  
Expert



twallace@ine.com



@TracyWallaceINE



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



- Getting Ready
- Manage Identity and Access
- Implement Platform Protection
- Manage Security Operations
- Secure Data and Applications

## Topics



# What to Expect

**Exam Domains**  
**Exam Length**  
**Types of Questions**  
**General**

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

**Exam Domains**  
**Exam Length**  
**Types of Questions**  
**General**

- + Around 2 hours
- + Around 40 questions
- + Plenty of time

**Exam Domains**  
**Exam Length**  
**Types of Questions**  
**General**

- + Standard multi-choice
- + Drag and drop
- + Drop down list
- + Scenario
- + Case Study

**Exam Domains**  
**Exam Length**  
**Types of Questions**  
**General**

- + The test is fair
- + The test is very detailed



# How to Prepare

## **Study tips**

### **Exam tips**

- + Track progress to the topic detail level
- + Use INE videos as study material
- + Practice with INE quiz questions
- + Consider MeasureUp practice exam
- + Look for material under docs.microsoft.com  
(site:docs.microsoft.com)
- + Use pricing pages
- + Pay attention to tiers
- + Take notes – include details
- + Practice

**Study tips**  
**Exam tips**

- + Manage your time
- + Read questions and answers carefully
- + Eliminate wrong answers
- + Choose the answer that makes Microsoft look the best
- + Don't freak out



# **Manage Identity and Access (30-35%)**

# Manage Identity and Access (30-35%)

- + Manage Azure Active Directory Identities
- + Configure Secure access by Using Azure AD
- + Manage Application Access
- + Manage Access Control

# Manage Azure Active Directory Identities

- manage Azure AD directory groups
- manage Azure AD users
- configure password writeback
- configure authentication methods including password hash and Pass Through Authentication (PTA), OAuth, and passwordless (not ADFS)

# Configure Secure access by Using Azure AD

- monitor privileged access for Azure AD Privileged Identity Management (PIM)
- configure Access Reviews
- activate and configure PIM
- implement Conditional Access policies including Multi-Factor Authentication (MFA)
- configure Azure AD identity protection

# Manage Application Access

- create App Registration
- configure App Registration permission scopes
- manage App Registration permission consent
- manage API access to Azure subscriptions and resources

# Manage Access Control

- configure subscription and resource permissions
- configure resource group permissions
- configure custom RBAC roles
- identify the appropriate role
- apply principle of least privilege
- interpret permissions
- check access



# **Implement Platform Protection (15-20%)**

# Implement Platform Protection (15-20%)

- + Implement Advanced Network Security
- + Configure Advanced Security for Compute

# Implement Advanced Network Security

- Secure the connectivity of virtual networks - VPN authentication, BYO Key for Express Route encryption, Point to site, Site to site
- configure Network Security Groups (NSGs) and Application Security Groups (ASGs)
- create and configure Azure Firewall
- Configure Azure Front Door service as an Application Gateway
- configure a Web Application Firewall (WAF) on Azure Application Gateway
- configure Azure Bastion
- configure a firewall on a storage account, Azure SQL, KeyVault, or App Service
- implement Service Endpoints
- implement DDoS



# Configure Advanced Security for Compute

- configure endpoint protection
- configure and monitor system updates for VMs in Azure
- configure authentication for containers
- configure security for different types of containers
- implement vulnerability management
- configure isolation for AKS
- configure security for container registry
- implement Azure Disk Encryption
- configure security for Azure App Service
- configure SSL/TLS certs
- configure authentication
- configure automatic updates



# **Manage Security Operations (25-30%)**

# Manage Security Operations (25-30%)

- + Monitor Security by Using Azure Monitor services
- + Monitor Security by Using Azure Security Center
- + Monitor Security by Using Azure Sentinel
- + Configure Security Policies

# Monitor Security by Using Azure Monitor services

- create and customize alerts
- monitor security logs by using Azure Monitor
- configure diagnostic logging and log retention

# Monitor Security by Using Azure Security Center

- evaluate vulnerability scans from Azure Security Center
- configure Just in Time VM access by using Azure Security Center
- configure centralized policy management by using Azure Security Center
- configure compliance policies and evaluate for compliance by using Azure Security center

# Monitor Security by Using Azure Sentinel

- create and customize alerts
- configure data sources to Azure Sentinel
- evaluate results from Azure Sentinel
- configure a playbook for a security event by using Azure Sentinel

# Configure Security Policies

- configure security settings by using Azure Policy
- configure security settings by using Azure Blueprint



# Secure Data and Applications (20-25%)

# Secure Data and Applications (20-25%)

- + Configure Security for Storage
- + Configure Security for Databases
- + Configure and Manage Key Vault

# 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