Exam Alert: Implement Azure Security

PREPARING FOR THE EXAM

David Tucker
TECHNICAL ARCHITECT & CTO CONSULTANT
@_davidtucker_ davidtucker.net

Objectives for the Exam

Implement Azure Security

20-25%

Implement User Authentication and Authorization	Implement Secure Cloud Solutions

Implement User Authentication and Authorization

Authenticate and authorize users by using the Microsoft Identity platform

Authenticate and authorize users and apps by using Azure Active Directory

Create and implement shared access signatures

Implement Secure Cloud Solutions

Secure app configuration data by using the App Configuration in Azure Key Vault

Develop code that uses keys, secrets, and certificates in Azure Key Vault

Implement solutions that interact with Microsoft Graph

Review User Authentication and Authorization

Areas of Focus

Microsoft Identity Platform Concepts

Azure AD App Manifests

Azure Role-based Access Control

Azure Storage Shared Access Signatures

Mutual TLS Authentication

Microsoft Identity Platform

A modern identity platform consisting of several components that enable developers to integrate identity into their custom applications while also integrating with Microsoft API's.

Microsoft Identity Platform Components

Standards-based Auth Service

Open-source Libraries

Application Management Portal

App Configuration API and Powershell

Developer Content

Microsoft Identity Platform Standards

Authentication
OpenID Connect

Authorization
OAuth 2.0

Microsoft Identity Platform Concepts

Understand auth flows for single-page app, desktop app, mobile app, daemon app

Understand how the Microsoft Identity Platform uses JSON Web Tokens (JWT's)

Understand the tools you can leverage to integrate the platform with your apps

Know how to configure your applications to properly leverage the platform

Azure AD App Manifest

The definition of an application object within the Microsoft Identity platform which includes all configuration for allowed authentication and authorization integrations.

App Manifest

```
{
    "id": "058477a1-5d5f-45e7-bc71-66c059a58eff",
    "name": "SampleSPA",
     ...
    "allowPublicClient": true,
    "groupMembershipClaims": "All",
    "oauth2AllowIdTokenImplicitFlow": true,
    "oauth2AllowImplicitFlow": true,
    "oauth2Permissions": [],
    "oauth2RequirePostResponse": false,
     ...
}
```

App Manifest Attributes to Review

appRoles

groupMembershipClaims

optionalClaims

oauth2AllowImplicitFlow

oauth2Permissions

signInAudience

Core Azure RBAC Concepts

Security Principal	Role Definition
Scope	Role Assignments

“A **shared access signature** (SAS) provides secure delegated access to resources in your storage account without compromising the security of your data.”

Microsoft Azure Documentation

Shared Access Signature Types

User Delegation

Service

Account

Azure Storage SAS Forms

Ad hoc SAS

Service SAS (with stored access policy)

SAS Best Practices

- Always use HTTPS when creating or distributing an SAS
- Use user delegation SAS whenever possible
- Define a stored access policy for a service specific SAS
- Use near-term expiration on ad hoc, service, or account SAS
- Follow least-privilege access for resources to be accessed

Azure App Service Mutual TLS Auth

Not supported on free or shared tiers

Certificate is the X-ARR-ClientCert header

Certificate value is Base64 encoded

App code is required to validate certificate

Scenario Understanding

- Review different use cases for authentication approaches
- Understand the order to implement different approaches
- Know limits of services and service tiers
- Be able to spot poor security implementations

Review Secure Cloud Solutions

Areas of Focus

Microsoft Graph

Azure Key Vault

Microsoft Graph

Add a Microsoft Graph is the gateway to data and intelligence in Microsoft 365. It provides a unified programmability model that you can use to access the tremendous amount of data in Microsoft 365, Windows 10, and Enterprise Mobility + Security.

Citation: Microsoft Documentation

Identity and Access Management

Productivity

Collaboration

People and Workspace Intelligence

Device Management

Security

Cross-device Experiences

User Notifications

Usage Reports

Education

Business Applications

Microsoft Graph Services

Integrating with Microsoft Graph

Register an application with Azure AD

Leverage the Microsoft Identity Platform authorize endpoint with defined scopes

User signs in with credentials and accepts the scopes

App receives an authorization code

Authorization code can be used to get a token from the token endpoint

Token can be leveraged to access Microsoft Graph

Azure Key Vault Deletion Protection

Soft-delete

Purge Protection

```
# Create a Key Vault using PowerShell
New-AzKeyVault -Name ‘Sample-Vault' -ResourceGroupName
'SampleResourceGroup' -Location 'East US’

# Create a Key Vault using Azure CLI
az keyvault create --name "Sample-Vault2" --resource-group
"SampleResourceGroup" --location eastus
```

Creating an Azure Key Vault

PowerShell and CLI Commands

Example Scenarios

Scenario 1

Sylvia's company is building a prototype for a new internal React web application

One of the requirements is that users can manage their profile information

The user's Microsoft 365 profile will be leveraged

Sylvia plans to use Azure AD for identity

How can she accomplish this approach?

Scenario 2

Edward currently has a .NET Core application running as a Function app

He is storing a connection string for Cosmos DB in his application settings

He wants to avoid redeployments for his Function app

What is the most efficient approach he can take to improve security?

Scenario 3

Cindy's company is implementing a new App Service app in Node.js

The app will leverage Mutual TLS for authentication

Cindy is responsible for writing the code to validate the client certificate

How can she access the certificate that the client has used for the request?

Scenario 4

William is creating an application that will use Azure AD for authentication

He wants to allow users from his company's directory to login

He wants to retrieve group membership for groups assigned to the app

How should William configure his app manifest for these requirements?

App Manifest

```
{
    "id": "058477a1-5d5f-45e7-bc71-66c059a58eff",
    "name": "SampleSPA",
     ...
    "allowPublicClient": true,
    "groupMembershipClaims": [redacted],
    “oauth2Permissions": [],
    "signInAudience": [redacted],
     ...
}
```

Scenario 5

Oscar's is creating an application to track customer rebates

Part of the application is storing the customer submitted receipt images

The app currently uses an account SAS that is stored in app configuration

How can Oscar ensure the most secure access to storage resources?

Scenario 6

James's company processes healthcare data for billing analysis

They have a requirement that all data must be encrypted using managed keys

They require leveraging hardware encryption (HSM) **for key storage**

James has moved all encryption keys to Azure Key Vault (standard tier)

Does his approach meet the criteria?

Scenario Answers

Scenario 1

Sylvia's company is building a prototype for a new internal React web application

One of the requirements is that users can manage their profile information

The user's Microsoft 365 profile will be leveraged

Sylvia plans to use Azure AD for identity

How can she accomplish this approach?

Solution: Utilize Microsoft Graph with the Microsoft Graph Toolkit and MSAL v2

Scenario 2

Edward currently has a .NET Core application running as a Function app

He is storing a connection string for Cosmos DB in his application settings

He wants to avoid redeployments for his Function app

What is the most efficient approach he can take to improve security?

Solution: Utilize an Azure Key Vault Reference for the Cosmos DB connection

Scenario 3

Cindy's company is implementing a new App Service app in Node.js

The app will leverage Mutual TLS for authentication

Cindy is responsible for writing the code to validate the client certificate

How can she access the certificate that the client has used for the request?

Solution: Access the X-ARR-ClientCert header and decode the Base64 string

Scenario 4

William is creating an application that will use Azure AD for authentication

He wants to allow users from his company's directory to login

He wants to retrieve group membership for groups assigned to the app

How should William configure his app manifest for these requirements?

App Manifest

```
{
    "id": "058477a1-5d5f-45e7-bc71-66c059a58eff",
    "name": "SampleSPA",
     ...
    "allowPublicClient": true,
    "groupMembershipClaims": "ApplicationGroup",
    “oauth2Permissions": [],
    "signInAudience": "AzureADMyOrg",
     ...
}
```

Scenario 5

Oscar's is creating an application to track customer rebates

Part of the application is storing the customer submitted receipt images

The app currently uses an account SAS that is stored in app configuration

How can Oscar ensure the most secure access to storage resources?

Solution: Utilize a user-delegation SAS, which uses Azure AD credentials

Scenario 6

James's company processes healthcare data for billing analysis

They have a requirement that all data must be encrypted using managed keys

They require leveraging hardware encryption (HSM) **for key storage**

James has moved all encryption keys to Azure Key Vault (standard tier)

Does his approach meet the criteria?

Solution: No. He will need to utilize the Premium Tier for Azure Key Vault