Microsoft Azure technologies for AWS architects

Certificate: Yes	**Language:** English
Duration: 4-Day	**Credits:** 32 PDUs
Course Delivery: Classroom/ Virtual	

Course Description:

This course teaches Solutions Architects who have previously designed for Amazon Web Services how to translate business requirements into secure, scalable, and reliable solutions for Azure. Lessons include virtualization, automation, networking, storage, identity, security, data platform, and application infrastructure. This course outlines how decisions in each theses area affects an overall solution.

Learning Objectives:

After the training, you will be able to:

- Secure identities with Azure Active Directory and users and groups.
- Implement identity solutions spanning on-premises and cloud-based capabilities
- Apply monitoring solutions for collecting, combining, and analyzing data from different sources.
- Manage subscriptions, accounts, Azure policies, and Role-Based Access Control.
- Administer Azure using the Resource Manager, Azure portal, Cloud Shell, and CLI.
- Configure intersite connectivity solutions like VNet Peering, and virtual network gateways.
- Administer Azure App Service, Azure Container Instances, and Kubernetes.

Course Outline:

Module 1: Introduction to Azure

- Subscriptions and accounts
- Resource groups and templates in Azure Resource Manager

After completing this module you will be able to:

- Determine the type of account and subscription best suited to your solution.
- Create resource groups and templates to standardize and manage solutions.

Module 2: Azure global infrastructure

- Azure regions
- Azure Availability Zones
- Comparison with AWS

After completing this module you will be able to:

- Implement an architecture that provides the availability and reliability required by your solution.

Module 3: Implement Azure Active Directory

- Introduction to Azure Active Directory
- Domains and custom domains
- Safety features
- Guest users in Azure Active Directory
- Manage multiple directories
- Comparison with AWS

After completing this module you will be able to:

- Secure identities with Azure Active Directory.
- Implement users and groups.

Module 4: Implement and manage hybrid identities

- Introduction to Azure AD Connect
- Comparison with AWS

After completing this module you will be able to:

- Use your on-premise Active Directory account to authenticate to your cloud solution.
- Sync accounts between on-premise and the cloud.

Module 5: Implement virtual networking

- Azure Virtual Network and VNet peering
- VPN and ExpressRoute connections
- Comparison with AWS

After completing this module you will be able to:

- Design virtual networks with security in mind.

Module 6: Implement VMs for Windows and Linux

- Configure high availability
- Comparison with AWS

After completing this module you will be able to:

- Implement VMs to create high availability solutions.
- Deploy and configure scale sets.

Module 7: Implement load balancing and network security

- Implement Azure Load Balancer
- Implement an Azure Application Gateway

- Implement Azure Firewall
- Implement network security groups and application security groups
- Comparison with AWS

After completing this module you will be able to:

- Implement the components of load balancing.
- Set up network and application security groups.

Module 8: Implement container-based applications

- Configure Azure Kubernetes Service
- Publish a solution on an Azure Container Instance
- Comparison with AWS

After completing this module you will be able to:

- Configure Azure Kubernetes Service for your solution.
- Publish your solution on an Azure Container Instance.

Module 9: Implement an application infrastructure

- Create an App Service plan
- Create and configure Azure App Service
- Configure networking for an App Service
- Introduction to Logic Apps and Azure Functions
- Comparison with AWS

After completing this module you will be able to:

- Select an App Service plan suitable for your solution.
- Configure the App Service.
- Incorporate Logic Apps and Azure Functions into your solution.

Module 10: Implement storage accounts

- Azure Storage core concepts
- Managing the Azure Blob storage lifecycle

- Working with Azure Blob storage
- Comparison with AWS

After completing this module you will be able to:

- Select an appropriate Azure Storage account for your solution.
- Configure your storage account.

Module 11: Implement NoSQL databases

- Introduction to Azure Cosmos DB
- Consistency
- Select appropriate CosmosDB APIs
- Set up replicas in CosmosDB
- Comparison with AWS DynamoDB

After completing this module you will be able to:

- Configure a NoSQL database solution by using Azure Cosmos DB.

Module 12: Implement Azure SQL databases

- Configure Azure SQL database settings
- Implement Azure SQL Database managed instances
- Configure high availability for an Azure SQL database
- Comparison with AWS

After completing this module you will be able to:

- Implement managed instances of Azure SQL database.
- Configure your database for high availability.

Module 13: Implement cloud infrastructure monitoring

- Monitor security
- Monitor cost
- Configure a Log Analytics workspace
- Comparison with AWS

After completing this module you will be able to:

- Set up security monitoring for your solution.
- Monitor costs by analyzing logs.

Module 14: Implement and manage Azure governance solutions

- Assign RBAC roles
- Configure management access to Azure
- Implement and configure an Azure Policy
- Comparison with AWS

After completing this module you will be able to:

- Configure RBAC roles for governance access.
- Configure an Azure Policy to enforce compliance with governance requirements.

Module 15: Manage security for applications

- Implement Azure Key Vault
- Implement and configure Azure AD Managed Identities
- Register and manage applications in Azure AD
- Comparison with AWS

After completing this module you will be able to:

- Register your app in Azure Active Directory.
- Configure Azure Active Directory for managed identities used by your app to access data.

Module 16: Migration, backup, and disaster recovery management

- Migrate workloads
- Implement Azure Backup for VMs
- Implement disaster recovery
- Comparison with AWS

After completing this module you will be able to:

- Migrate workloads to the cloud and across VMs.
- Implement cloud backups.
- Implement disaster recovery options.
- Implement update strategies that avoid negative impacts to availability and performance.

Prerequisites:

- Experience (>1year) as an AWS Architect designing secure and scalable AWS cloud solutions across storage structures, compute, networking, and the interaction with external resources/services.
- Understanding of on-premises virtualization technologies, including: VMs, virtual networking, and virtual hard disks.
- Understanding of network configuration, including TCP/IP, Domain Name System (DNS), virtual private networks (VPNs), firewalls, and encryption technologies.
- Understanding of Active Directory concepts, including domains, forests, domain controllers, replication, Kerberos protocol, and Lightweight Directory Access Protocol (LDAP).
- Understanding of resilience and disaster recovery, including backup and restore operations.
- Understanding of programming fundamentals and use of a scripting language.

Candidates will benefit from familiarity with Azure administration, Azure development processes, and DevOps processes.

Exam: [AZ-303](AZ-303)

Who can Attend?

This course is for AWS Cloud Architects with expertise in designing and implementing solutions running on AWS who now want to design for Microsoft Azure.