

ExamLabs

**Microsoft Azure Architect
Technologies
Study Guide
Exam AZ-303**

Table of Contents

Chapter 1: Setting Expectations

What Is Azure?

What Is Cloud Computing?

Types of Cloud Computing

Public

Private

Hybrid

Types of Cloud Services

Azure Free Account

Setting the Budget

Azure Subscriptions and Resources

Azure Subscription Options

Azure Blueprints

Azure Accounts

Roles and Permissions

Azure Policy

Subscriptions with Resources

Permissions and Reporting

Tagging

Azure Services

Azure Availability

Chapter 2: Virtual Machines

Creating a VM

High Availability

Availability Zone

Virtual Machine Scale Set

Dedicated Hosts

High Availability Considerations

Creating a Host Group

Creating a Dedicated Host

Requesting a Quota Increase

Setting Up a Bastion Host

Chapter 3: ARM Templates

Creating a VM with an ARM Template

Deploying a VM

Chapter 4: Virtual Machine Encryption

Creating a Key Vault

Creating Keys

Enabling Encryption

Encrypting an OS Disk

Enabling Encryption Using PowerShell

Chapter 5: Azure Monitoring

Opening Azure Monitor

Enabling Guest-Level Monitoring

Creating a Baseline for Resources

Setting Up Alerts and Metrics

Creating an Alert

Understanding Metrics

Setting Up a Metric

Managing Actions

Managing Costs

Chapter 6: Azure Recommendations

Creating a Recommendation

Using Log Analytics

Chapter 7: Storage Solutions

Configuring an Endpoint

Configuring a Container

Access Keys

Shared Access Signatures

Using Azure Storage Explorer

Setting Up Log Analytics for Storage

Setting Up Azure AD Authentication for Storage

Replicating Data

Setting Up Failover for Storage Accounts

Chapter 8: Managing Virtual Networks

Creating a Virtual Network

Setting Up Public and Private IP Addresses

Creating a Route Table

Associating a Subnet

Creating Application Security Groups

Assigning an Application Security Group to a Resource

Updating Inbound Rules

Chapter 9: Connecting Networks

Setting Up Peering

Configuring Global Peering

Forwarded Traffic

VNet Pricing

Creating a Gateway Subnet

Network Gateways

VNet-to-VNet Connection

VPN Pricing

Virtual Private Networks

Point-to-Site Connection

Site-to-Site Connection

ExpressRoute

ExpressRoute Direct

Chapter 10: Azure Active Directory

Pricing

Creating an Azure Active Directory

Creating a User

Adding Custom Domain Names

Creating a Group

Using Identity Protection

Creating a User Risk Policy

Setting Up a Sign-in Risk Policy

MFA Registration Policy

Setting Up a Self-Service Password Reset

Testing the AD Flow

Conditional Access

Identity Governance

Using Access Reviews

Creating an Azure AD Hybrid Identity

Azure AD B2C

Configuring Azure AD B2B

Deleting an Active Directory

Chapter 11: Implement and Manage Hybrid Identities

Azure AD Connect

Password Hash Synchronization

Pass-Through Synchronization

Benefits of Using Pass-Through Authentication

Federation Integration

Synchronization

Azure AD Connect Health

Chapter 12: Migrate Servers to Azure

Creating a Recovery Service

Enabling Resource Providers

Creating a New Replication Item

Creating a Disaster Recovery Plan

Creating a Virtual Network

Testing the Failover Strategy

Deleting a Recovery Service

Chapter 13: Serverless Computing

Function App

Creating a New Function

Testing the Function App

Function Integration with Azure Blob

Testing the Integrated Function

Logic Apps

Creating a New Logic App

Event Grid

Creating a New Event Grid

Service Bus

Creating a New Service Bus

Chapter 14: Load Balancing

Creating a Load Balancer

Creating Virtual Machines

Configuring a Backend Pool

Configuring a Health Probe

Creating a Load Balancing Rule

Configuring a Front-End IP Address

Creating a Secondary Health Probe

Creating a Second Load Balancing Rule

Using Application Gateway

Creating a Gateway

Editing a Backend Pool

Adding a Listener

Adding a Path-Based Rule

Using Front Door

Using Front Door

Chapter 15: Multifactor Authentication

Adding a Guest User

Enabling Multifactor Authentication

Setting Up Fraud Alerts

Creating a One-Time Bypass

Using Role-Based Access Control

Chapter 16: App Services

Creating an App Service

Scale Up/Out Options

Deployment Center

Deployment Slots

App Services for Containers

Background Jobs

Web Jobs

Autoscaling

Scale Rule

Chapter 17: Service Fabric

Service Fabric Containers

Creating a Service Fabric

Creating a Service Fabric Using the CLI

Managing the Service Fabric on a Local Machine

Deployment

Programming Models

Chapter 18: Apps with Containers

Using the Azure Kubernetes Service

Deploying a Kubernetes Cluster

Using the Kubernetes Dashboard

Running Containers Locally

Chapter 19: Data Security

Encryption

Azure Key Vault

Storing Azure Resource Manager Template Secrets

ExamLabs

Creating a Key Vault

Creating a Secret

Chapter 20: Cosmos DB

Creating a Cosmos DB

Georeplication

Creating an Items Container

Creating a Cosmos DB Collection

Adding Records to the Database

Querying Records from the Database

Default Consistency

Chapter 21: Relational Databases

Creating a SQL Database

Georeplication

Database Firewalls

Setting Up an Active Directory Admin

Query Editor

SQL Server Management Studio

Chapter 22: Exercises

Exercise 1

Exercise 2

Exercise 3

Exercise 4

Exercise 5

Exercise 6

Exercise 7

Exercise 8

Exercise 9

Chapter 23: Practice Questions

Questions

Answers

Chapter 24: Azure Architectural Practices

Technology Choices

Compute Service

Data Stores

Messaging Technology

Design the Architecture

Design Principles

Design Patterns

What Is Azure?

Azure, which is Microsoft's cloud offering, is a pay-as-you-go computing platform with tons of services. Azure is an ever-expanding set of cloud services to enable organizations to meet their business challenges. It offers the opportunity to build, manage, and deploy applications on a massive, global network utilizing your favorite tools and frameworks. You can find more details about Azure at

<https://azure.microsoft.com/en-in/overview/what-is-azure/>.

What Is Cloud Computing?

Cloud computing is the delivery of computing services—including servers, storage, databases, etc.—over the Internet (“the cloud”) to offer faster innovation, flexible resources, and economies of scale. You pay only for the cloud services you use, which helps you lower your operating costs, run your infrastructure more efficiently, and scale as your business needs change. The following are the top benefits of cloud computing:

- Cost
- Speed
- Global scale
- Productivity
- Performance
- Reliability
- Security
- And many more, which we will cover in depth in this book

Types of Cloud Computing

There are three types of cloud computing available on the market: public, private, and hybrid. Before getting started, you should know which offering suits you or your company best.

Public

In simple terms, according to Microsoft, “Public clouds are the most common way of deploying cloud computing. The cloud resources (like servers and storage) are owned and operated by a third-party cloud service provider and delivered over the Internet. Azure is an example of a public cloud. With a public cloud, all hardware, software, and other supporting infrastructure is owned and managed by the cloud provider. In a public cloud, you share the same hardware, storage, and network devices with other organizations or cloud tenants.”

These are a few high-level advantages of a public cloud:

- Lower costs—no need to purchase hardware or software, and you pay only for the service you use.
- No maintenance—your service provider provides the maintenance.
- Near-unlimited scalability—on-demand resources are available to meet your business needs.
- High reliability—a vast network of servers ensures against failure.

Private

A private cloud consists of computing resources used exclusively by one business or organization. The private cloud can be physically located at your organization’s on-site data center, or it can be hosted by a third-party service provider. But in a private cloud, the services and infrastructure are always maintained on a private network, and the hardware and software are dedicated solely to your organization. In this way, a private cloud can make it easier for an organization to customize its resources to meet specific IT requirements. Private clouds are often used by government agencies, financial institutions, or any other mid- to large-size organization with business-critical operations seeking enhanced control over their environment.

The following are advantages of private clouds:

- More flexibility—your organization can customize its cloud environment to meet specific business needs.
- Improved security—resources are not shared with others, so higher levels of control and security are possible.
- High scalability—private clouds still afford the scalability and efficiency of a public cloud.
- More flexibility—the Azure stack can be downloaded into private data centers, which means your own private data center will be boosted by Azure's private cloud.

Hybrid

Often referred to as “the best of both worlds,” hybrid clouds combine on-premises infrastructure, or private clouds, with public clouds so organizations can reap the advantages of both. In a hybrid cloud, data and applications can move between private and public clouds for greater flexibility and more deployment options. For instance, you can use the public cloud for high-volume, lower-security needs such as web-based email and then use the private cloud (or other on-premises infrastructure) for sensitive, business-critical operations such as financial reporting. In a hybrid cloud, “cloud bursting” is also an option.

The following are advantages of hybrid clouds:

- Control—your organization can maintain a private infrastructure for sensitive assets.
- Flexibility—you can take advantage of additional resources in the public cloud when you need them.
- Cost-effectiveness—with the ability to scale to the public cloud, you pay for extra computing power only when needed.
- Ease—transitioning to the cloud doesn't have to be overwhelming because you can migrate gradually, phasing in workloads over time.

Types of Cloud Services

Most cloud computing is categorized into four broad categories.

Infrastructure as a service (IaaS) is where you rent the IT infrastructure—servers and virtual machines (VMs), storage, networks, etc.—from a cloud provider on a pay-as-you-go basis.

Platform as a service (PaaS) refers to cloud computing services that supply an on-demand environment for developing, testing, delivering, and managing software applications. PaaS is designed to make it easier for developers to quickly create web or mobile apps, without worrying about setting up or managing the underlying infrastructure.

Software as a service (SaaS) is a method for delivering software applications over the Internet, on demand and typically on a subscription basis. With SaaS, cloud providers host and manage the software application and underlying infrastructure, and they also handle any maintenance, such as software upgrades and security patching.

Serverless computing focuses on building app functionality without spending time continually managing the servers and infrastructure required. The cloud provider handles the setup, capacity planning, and server management for you. Serverless architectures are highly scalable and event-driven.

These are the high-level classification of categories. All these categories are explained in more detail in the coming chapters.

Azure Free Account

To get started, you need either a subscription or a free account. You can visit <https://azure.microsoft.com/en-us/free/> to sign up and get a free credit worth \$200 for one month. Check the website for the most up-to-date list of free offerings.