Microsoft Azure Fundamentals (AZ-900)

Duration: 1 Day **Course Code: M-AZ-900T01**

Overview:

This one-day course will provide foundational level knowledge on Azure concepts; core Azure services; core solutions and management tools; general security and network security; governance, privacy, and compliance features; Azure cost management and service level agreements. You will not have to perform hands-on exercises in this course.
This course does not provide an Azure pass or time in the classroom for students to do any hands-on activities.

Target Audience:

This course is suitable for program managers and technical sales, with a general IT background. These students want to learn about our offerings, see how components are implemented, and ask questions about products and features.

Objectives:

- Discuss the basics of cloud computing and Azure, and how to get started with Azure's subscriptions and accounts.
- Describe the advantages of using cloud computing services, learning to differentiate between the categories and types of cloud computing, and how to examine the various concepts, resources, and terminology that are necessary to work with Azure architecture.
- Outline the core services available with Microsoft Azure.
- Discuss the core solutions that encompass a wide array of tools and services from Microsoft Azure.
- Describe the general security and network security features, and how you can use the various Azure services to help ensure that your cloud resources are safe, secure, and trusted.
- Discuss the identity, governance, privacy, and compliance features, and how Azure can help you secure access to cloud resources, what it means to build a cloud governance strategy, and how Azure adheres to common regulatory and compliance standards.
- Discuss the factors that influence cost, tools you can use to help estimate and manage your cloud spend, and how Azure's service-level agreements (SLAs) can impact your application design decisions.

Prerequisites:

There are no pre-requisites for taking this course. Technical IT experience is not required however some general IT knowledge or experience would be beneficial.

Testing and Certification

Follow-on-Courses:

- M-AZ104, Microsoft Azure Administrator
- M-AZ204, Developing Solutions for Microsoft Azure
- M-AZ303, Microsoft Azure Architect Technologies
- M-DP200, Implementing an Azure Data Solution (DP-200)

Content:

Module 1: Cloud Concepts

In this module, you'll take an entry level end-to-end look at Azure and its capabilities, which will provide you with a solid foundation for completing the available modules for Azure Fundamentals.

- Introduction to Azure fundamentals
- Fundamental Azure concepts

After completing this module, students will be able to:

- Understand the benefits of cloud computing in Azure and how it can save you time and money.
- Explain concepts such as high availability, scalability, elasticity, agility, and disaster recovery.
- Describe core Azure architecture components such as subscriptions, management groups, and resources.
- Summarize geographic distribution concepts such as Azure regions, region pairs, and availability zones.
- Understand the services available in Azure including compute, network, storage, and databases.
- Identify virtualization services such as Azure VMs, Azure Container Instances, and Azure Kubernetes.
- Compare Azure's database services such as Azure Cosmos DB, Azure SQL, and Azure Database for MySQL.
- Examine Azure networking resources such as Virtual Networks, VPN Gateways, and Azure ExpressRoute.
- Summarize Azure storage services such Azure Blob Storage, Azure Disk Storage, and Azure File Storage.
- Choose the correct Azure AI service to address different kinds of business challenges.
- Choose the best software development process tools and services for a given business scenario.
- Choose the correct cloud monitoring service to address different kinds of business challenges.
- Choose the correct Azure management tool to address different kinds of technical needs.
- Choose the right serverless computing technology for your business scenario.
- Choose the best Azure IoT service for a given business scenario.
- Strengthen your security posture and protect against threats by using Microsoft Defender for Cloud.
- Collect and act on security data from many different sources by using Microsoft Sentinel.

Module 3: Core Solutions

In this module, you'll learn about AI machine learning, Azure DevOps, monitoring fundamentals, management fundamentals, serverless computing fundamentals. and IoT fundamentals.

- Choose the best Azure IoT service
- Choose the best AI service
- Choose the best Azure serverless technology
- Choose the best tools with DevOps and GitHub
- Choose the best management tools
- Choose the best Azure monitoring service

After completing this module, students will be able to:

- Understand the benefits of cloud computing in Azure and how it can save you time and money.
- Explain concepts such as high availability, scalability, elasticity, agility, and disaster recovery.
- Describe core Azure architecture components such as subscriptions, management groups, and resources.
- Summarize geographic distribution concepts such as Azure regions, region pairs, and availability zones.
- Understand the services available in Azure including compute, network, storage, and databases.
- Identify virtualization services such as Azure VMs, Azure Container Instances, and Azure Kubernetes.
- Compare Azure's database services such as Azure Cosmos DB, Azure SQL, and Azure Database for MySQL.
- Examine Azure networking resources such as Virtual Networks, VPN Gateways, and Azure ExpressRoute.
- Summarize Azure storage services such Azure Blob Storage, Azure Disk Storage, and Azure File Storage.
- Choose the correct Azure AI service to address different kinds of business challenges.
- Choose the best software development process tools and services for a given business scenario.
- Choose the correct cloud monitoring service to address different kinds of business challenges.
- Choose the correct Azure management tool to address different kinds of technical needs.
- Choose the right serverless computing technology for your business scenario.

Module 5: Identity, Governance, Privacy, and Compliance

In this module, you will learn about Azure identity services, how to build a cloud governance strategy, and privacy, compliance and data protection standards on Azure.

- Core Azure identity services
- Azure Governance Methodologies
- Privacy, Compliance, and Data Protection standards

After completing this module, students will be able to:

- Understand the benefits of cloud computing in Azure and how it can save you time and money.
- Explain concepts such as high availability, scalability, elasticity, agility, and disaster recovery.
- Describe core Azure architecture components such as subscriptions, management groups, and resources.
- Summarize geographic distribution concepts such as Azure regions, region pairs, and availability zones.
- Understand the services available in Azure including compute, network, storage, and databases.
- Identify virtualization services such as Azure VMs, Azure Container Instances, and Azure Kubernetes.
- Compare Azure's database services such as Azure Cosmos DB, Azure SQL, and Azure Database for MySQL.
- Examine Azure networking resources such as Virtual Networks, VPN Gateways, and Azure ExpressRoute.
- Summarize Azure storage services such Azure Blob Storage, Azure Disk Storage, and Azure File Storage.
- Choose the correct Azure AI service to address different kinds of business challenges.
- Choose the best software development process tools and services for a given business scenario.
- Choose the correct cloud monitoring service to address different kinds of business challenges.
- Choose the correct Azure management tool to address different kinds of technical needs.
- Choose the right serverless computing technology for your business scenario.
- Choose the best Azure IoT service for a given business scenario.
- Strengthen your security posture and protect against threats by using Microsoft Defender for Cloud.

- Manage dedicated physical servers to host your Azure VMs for Windows and Linux.
- Identify the layers that make up a *defense in depth* strategy.
- Explain how Azure Firewall enables you to control what traffic is allowed on the network.
- Configure network security groups to filter network traffic to and from Azure resources.
- Explain how Azure DDoS Protection helps protect your Azure resources from DDoS attacks.
- Explain the difference between authentication and authorization.
- Describe how Azure Active Directory provides identity and access management.
- Explain the role single sign-on (SSO), multifactor authentication, and Conditional Access play.
- Make organizational decisions about your cloud environment by using the CAF for Azure.
- Define who can access cloud resources by using Azure role-based access control.
- Apply a resource lock to prevent accidental deletion of your Azure resources.
- Apply tags to your Azure resources to help describe their purpose.
- Control and audit how your resources are created by using Azure Policy.
- Enable governance at scale across multiple Azure subscriptions by using Azure Blueprints.
- Explain the types of compliance offerings that are available on Azure.
- Gain insight into regulatory standards and compliance on Azure.
- Explain Azure capabilities that are specific to government agencies.
- Use the Total Cost of Ownership Calculator.
- Describe the different ways you can purchase Azure products and services.
- Use the Pricing calculator to estimate the monthly cost of running your cloud workloads.
- Define the major factors that affect total cost and apply recommended practices to minimize cost.
- Describe what a service-level agreement (SLA) is and why SLAs are important.
- Identify factors, such as the service tier you choose, that can affect an SLA.
- Combine SLAs to compute a composite SLA.
- Describe the service lifecycle in Azure.

Module 2: Core Azure Services

In this module, you learn about core Azure services like Azure database, Azure compute, Azure storage, and Azure Networking.

- Core Azure architectural components
- Core Azure workload products
- Choose the best Azure IoT service for a given business scenario.
- Strengthen your security posture and protect against threats by using Microsoft Defender for Cloud.
- Collect and act on security data from many different sources by using Microsoft Sentinel.
- Manage dedicated physical servers to host your Azure VMs for Windows and Linux.
- Identify the layers that make up a *defense in depth* strategy.
- Explain how Azure Firewall enables you to control what traffic is allowed on the network.
- Configure network security groups to filter network traffic to and from Azure resources.
- Explain how Azure DDoS Protection helps protect your Azure resources from DDoS attacks.
- Explain the difference between authentication and authorization.
- Describe how Azure Active Directory provides identity and access management.
- Explain the role single sign-on (SSO), multifactor authentication, and Conditional Access play.
- Make organizational decisions about your cloud environment by using the CAF for Azure.
- Define who can access cloud resources by using Azure role-based access control.
- Apply a resource lock to prevent accidental deletion of your Azure resources.
- Apply tags to your Azure resources to help describe their purpose.
- Control and audit how your resources are created by using Azure Policy.
- Enable governance at scale across multiple Azure subscriptions by using Azure Blueprints.
- Explain the types of compliance offerings that are available on Azure.
- Gain insight into regulatory standards and compliance on Azure.
- Explain Azure capabilities that are specific to government agencies.
- Use the Total Cost of Ownership Calculator.
- Describe the different ways you can purchase Azure products and services.
- Use the Pricing calculator to estimate the monthly cost of running your cloud workloads.
- Define the major factors that affect total cost and apply recommended practices to minimize cost.
- Describe what a service-level agreement (SLA) is and why SLAs are important.
- Identify factors, such as the service tier
- Collect and act on security data from many different sources by using Microsoft Sentinel.
- Manage dedicated physical servers to host your Azure VMs for Windows and Linux.
- Identify the layers that make up a *defense in depth* strategy.
- Explain how Azure Firewall enables you to control what traffic is allowed on the network.
- Configure network security groups to filter network traffic to and from Azure resources.
- Explain how Azure DDoS Protection helps protect your Azure resources from DDoS attacks.
- Explain the difference between authentication and authorization.
- Describe how Azure Active Directory provides identity and access management.
- Explain the role single sign-on (SSO), multifactor authentication, and Conditional Access play.
- Make organizational decisions about your cloud environment by using the CAF for Azure.
- Define who can access cloud resources by using Azure role-based access control.
- Apply a resource lock to prevent accidental deletion of your Azure resources.
- Apply tags to your Azure resources to help describe their purpose.
- Control and audit how your resources are created by using Azure Policy.
- Enable governance at scale across multiple Azure subscriptions by using Azure Blueprints.
- Explain the types of compliance offerings that are available on Azure.
- Gain insight into regulatory standards and compliance on Azure.
- Explain Azure capabilities that are specific to government agencies.
- Use the Total Cost of Ownership Calculator.
- Describe the different ways you can purchase Azure products and services.
- Use the Pricing calculator to estimate the monthly cost of running your cloud workloads.
- Define the major factors that affect total cost and apply recommended practices to minimize cost.
- Describe what a service-level agreement (SLA) is and why SLAs are important.
- Identify factors, such as the service tier you choose, that can affect an SLA.
- Combine SLAs to compute a composite SLA.
- Describe the service lifecycle in Azure.

Module 6: Azure Pricing and Lifecycle

In this module, you will learn how to plan and

- Azure networking services
- Azure storage services
- Azure database services

After completing this module, students will be able to:

- Understand the benefits of cloud computing in Azure and how it can save you time and money.
- Explain concepts such as high availability, scalability, elasticity, agility, and disaster recovery.
- Describe core Azure architecture components such as subscriptions, management groups, and resources.
- Summarize geographic distribution concepts such as Azure regions, region pairs, and availability zones.
- Understand the services available in Azure including compute, network, storage, and databases.
- Identify virtualization services such as Azure VMs, Azure Container Instances, and Azure Kubernetes.
- Compare Azure's database services such as Azure Cosmos DB, Azure SQL, and Azure Database for MySQL.
- Examine Azure networking resources such as Virtual Networks, VPN Gateways, and Azure ExpressRoute.
- Summarize Azure storage services such Azure Blob Storage, Azure Disk Storage, and Azure File Storage.
- Choose the correct Azure AI service to address different kinds of business challenges.
- Choose the best software development process tools and services for a given business scenario.
- Choose the correct cloud monitoring service to address different kinds of business challenges.
- Choose the correct Azure management tool to address different kinds of technical needs.
- Choose the right serverless computing technology for your business scenario.
- Choose the best Azure IoT service for a given business scenario.
- Strengthen your security posture and protect against threats by using Microsoft Defender for Cloud.
- Collect and act on security data from many different sources by using Microsoft Sentinel.
- Manage dedicated physical servers to host your Azure VMs for Windows and Linux.
- Identify the layers that make up a *defense in depth* strategy.
- Explain how Azure Firewall enables you to control what traffic is allowed on the network.
- Configure network security groups to filter network traffic to and from Azure resources.
- Explain how Azure DDoS Protection helps you choose, that can affect an SLA.
- Combine SLAs to compute a composite SLA.
- Describe the service lifecycle in Azure.

Module 4: General security and networking features

In this module, you will learn how to protect yourself against security threats, and secure your networks with Azure.

- Security Tools and Features
- Secure Network Connectivity

After completing this module, students will be able to:

- Understand the benefits of cloud computing in Azure and how it can save you time and money.
- Explain concepts such as high availability, scalability, elasticity, agility, and disaster recovery.
- Describe core Azure architecture components such as subscriptions, management groups, and resources.
- Summarize geographic distribution concepts such as Azure regions, region pairs, and availability zones.
- Understand the services available in Azure including compute, network, storage, and databases.
- Identify virtualization services such as Azure VMs, Azure Container Instances, and Azure Kubernetes.
- Compare Azure's database services such as Azure Cosmos DB, Azure SQL, and Azure Database for MySQL.
- Examine Azure networking resources such as Virtual Networks, VPN Gateways, and Azure ExpressRoute.
- Summarize Azure storage services such Azure Blob Storage, Azure Disk Storage, and Azure File Storage.
- Choose the correct Azure AI service to address different kinds of business challenges.
- Choose the best software development process tools and services for a given business scenario.
- Choose the correct cloud monitoring service to address different kinds of business challenges.
- Choose the correct Azure management tool to address different kinds of technical needs.
- Choose the right serverless computing technology for your business scenario.
- Choose the best Azure IoT service for a given business scenario.
- Strengthen your security posture and protect against threats by using Microsoft Defender for Cloud.

manage Azure costs, and how to choose the right Azure services though SLAs and service lifecycle.

- Planning and Cost Management
- Azure Service Level Agreements (SLAs) and Lifecycle

After completing this module, students will be able to:

- Understand the benefits of cloud computing in Azure and how it can save you time and money.
- Explain concepts such as high availability, scalability, elasticity, agility, and disaster recovery.
- Describe core Azure architecture components such as subscriptions, management groups, and resources.
- Summarize geographic distribution concepts such as Azure regions, region pairs, and availability zones.
- Understand the services available in Azure including compute, network, storage, and databases.
- Identify virtualization services such as Azure VMs, Azure Container Instances, and Azure Kubernetes.
- Compare Azure's database services such as Azure Cosmos DB, Azure SQL, and Azure Database for MySQL.
- Examine Azure networking resources such as Virtual Networks, VPN Gateways, and Azure ExpressRoute.
- Summarize Azure storage services such Azure Blob Storage, Azure Disk Storage, and Azure File Storage.
- Choose the correct Azure AI service to address different kinds of business challenges.
- Choose the best software development process tools and services for a given business scenario.
- Choose the correct cloud monitoring service to address different kinds of business challenges.
- Choose the correct Azure management tool to address different kinds of technical needs.
- Choose the right serverless computing technology for your business scenario.
- Choose the best Azure IoT service for a given business scenario.
- Strengthen your security posture and protect against threats by using Microsoft Defender for Cloud.
- Collect and act on security data from many different sources by using Microsoft Sentinel.
- Manage dedicated physical servers to host your Azure VMs for Windows and Linux.
- Identify the layers that make up a *defense in depth* strategy.
- Explain how Azure Firewall enables you to

protect your Azure resources from DDoS attacks.
- Explain the difference between authentication and authorization.
- Describe how Azure Active Directory provides identity and access management.
- Explain the role single sign-on (SSO), multifactor authentication, and Conditional Access play.
- Make organizational decisions about your cloud environment by using the CAF for Azure.
- Define who can access cloud resources by using Azure role-based access control.
- Apply a resource lock to prevent accidental deletion of your Azure resources.
- Apply tags to your Azure resources to help describe their purpose.
- Control and audit how your resources are created by using Azure Policy.
- Enable governance at scale across multiple Azure subscriptions by using Azure Blueprints.
- Explain the types of compliance offerings that are available on Azure.
- Gain insight into regulatory standards and compliance on Azure.
- Explain Azure capabilities that are specific to government agencies.
- Use the Total Cost of Ownership Calculator.
- Describe the different ways you can purchase Azure products and services.
- Use the Pricing calculator to estimate the monthly cost of running your cloud workloads.
- Define the major factors that affect total cost and apply recommended practices to minimize cost.
- Describe what a service-level agreement (SLA) is and why SLAs are important.
- Identify factors, such as the service tier you choose, that can affect an SLA.
- Combine SLAs to compute a composite SLA.
- Describe the service lifecycle in Azure.

- Collect and act on security data from many different sources by using Microsoft Sentinel.
- Manage dedicated physical servers to host your Azure VMs for Windows and Linux.
- Identify the layers that make up a *defense in depth* strategy.
- Explain how Azure Firewall enables you to control what traffic is allowed on the network.
- Configure network security groups to filter network traffic to and from Azure resources.
- Explain how Azure DDoS Protection helps protect your Azure resources from DDoS attacks.
- Explain the difference between authentication and authorization.
- Describe how Azure Active Directory provides identity and access management.
- Explain the role single sign-on (SSO), multifactor authentication, and Conditional Access play.
- Make organizational decisions about your cloud environment by using the CAF for Azure.
- Define who can access cloud resources by using Azure role-based access control.
- Apply a resource lock to prevent accidental deletion of your Azure resources.
- Apply tags to your Azure resources to help describe their purpose.
- Control and audit how your resources are created by using Azure Policy.
- Enable governance at scale across multiple Azure subscriptions by using Azure Blueprints.
- Explain the types of compliance offerings that are available on Azure.
- Gain insight into regulatory standards and compliance on Azure.
- Explain Azure capabilities that are specific to government agencies.
- Use the Total Cost of Ownership Calculator.
- Describe the different ways you can purchase Azure products and services.
- Use the Pricing calculator to estimate the monthly cost of running your cloud workloads.
- Define the major factors that affect total cost and apply recommended practices to minimize cost.
- Describe what a service-level agreement (SLA) is and why SLAs are important.
- Identify factors, such as the service tier you choose, that can affect an SLA.
- Combine SLAs to compute a composite SLA.
- Describe the service lifecycle in Azure.

control what traffic is allowed on the network.
- Configure network security groups to filter network traffic to and from Azure resources.
- Explain how Azure DDoS Protection helps protect your Azure resources from DDoS attacks.
- Explain the difference between authentication and authorization.
- Describe how Azure Active Directory provides identity and access management.
- Explain the role single sign-on (SSO), multifactor authentication, and Conditional Access play.
- Make organizational decisions about your cloud environment by using the CAF for Azure.
- Define who can access cloud resources by using Azure role-based access control.
- Apply a resource lock to prevent accidental deletion of your Azure resources.
- Apply tags to your Azure resources to help describe their purpose.
- Control and audit how your resources are created by using Azure Policy.
- Enable governance at scale across multiple Azure subscriptions by using Azure Blueprints.
- Explain the types of compliance offerings that are available on Azure.
- Gain insight into regulatory standards and compliance on Azure.
- Explain Azure capabilities that are specific to government agencies.
- Use the Total Cost of Ownership Calculator.
- Describe the different ways you can purchase Azure products and services.
- Use the Pricing calculator to estimate the monthly cost of running your cloud workloads.
- Define the major factors that affect total cost and apply recommended practices to minimize cost.
- Describe what a service-level agreement (SLA) is and why SLAs are important.
- Identify factors, such as the service tier you choose, that can affect an SLA.
- Combine SLAs to compute a composite SLA.
- Describe the service lifecycle in Azure.

Further Information:

For More information, or to book your course, please call us on Head Office 01189 123456 / Northern Office 0113 242 5931

info@globalknowledge.co.uk

www.globalknowledge.com/en-gb/

Global Knowledge, Mulberry Business Park, Fishponds Road, Wokingham Berkshire RG41 2GY UK