

**Cloud Security
Summer Camp
Accelerator Program**

Contents

Microsoft Azure Cloud Technology	3
Associate Level	3
Microsoft Azure Administrator Associate	3
Key Competencies Overview	3
Module 1: Managing Azure Identities and Governance	3
Module 2: Implementing and Managing Storage	3
Module 3: Deploying and Managing Azure Compute Resources	4
Module 4: Implementing and Managing Virtual Networking	4
Module 5: Monitoring and Maintaining Azure Resources	4
Consultant Level	5
Microsoft Azure Security Technologies	5
Key Competencies Overview	5
Module 1: Manage Identity and Access	5
Module 2: Secure Networking	6
Module 3: Secure Compute, Storage, and Databases	6
Module 4: Manage Security Operations	6
Get Career Ready	7
Prepare for Soft Skills	7
Job Roles	7

Cloud Technology

Cloud is a leading technology that offers a wide range of services to help organizations build, deploy, and manage applications and services. With its scalability, reliability, and comprehensive set of features, the cloud is a popular choice for businesses of all sizes.

Cloud Security Engineer – Associate Level

Microsoft Azure Administrator Associate

The Azure Administrator Associate certification is designed for IT professionals responsible for implementing, managing, and monitoring Microsoft Azure environments. This certification validates expertise in various aspects of Azure administration, including virtual networks, storage, compute, identity, security, and governance.

Key Competencies Overview

- Manage Azure identities and governance
- Implement and manage storage
- Deploy and manage Azure compute resources
- Implement and manage virtual networking
- Monitor and maintain Azure resources

Module 1: Managing Azure Identities and Governance

- Introduction to Azure Active Directory (AD) Users and Groups
- Managing User and Group Properties
- License Management in Azure AD
- Managing External Users and Guest Access
- Configuring Self-Service Password Reset (SSPR)
- Access Management to Azure Resources
- Implementing and Managing Azure Roles
- Assigning Roles at Different Scopes
- Azure Subscriptions and Governance
- Implementing and Managing Azure Policy
- Resource Locks and Tagging
- Managing Resource Groups and Subscriptions
- Cost Management and Optimization Strategies
- Configuring Management Groups

Module 2: Implementing and Managing Storage

- Configuring Access to Azure Storage
- Azure Storage Firewalls and Virtual Networks

- Shared Access Signature (SAS) Tokens
- Stored Access Policies and Access Keys
- Identity-Based Access for Azure Files
- Configuring and Managing Storage Accounts
- Azure Storage Redundancy and Object Replication
- Storage Account Encryption
- Data Management with Azure Storage Explorer and AzCopy
- Azure Files and Azure Blob Storage Configuration
- Storage Tiers and Lifecycle Management
- Blob Versioning and Snapshots

Module 3: Deploying and Managing Azure Compute Resources

- Automating Deployment with Azure Resource Manager (ARM) Templates and Bicep Files
- Virtual Machine Management
- Azure Disk Encryption
- Virtual Machine Deployment and Migration
- Managing Virtual Machine Sizes and Disks
- Availability Zones and Sets
- Azure Virtual Machine Scale Sets
- Container Provisioning and Management
- Azure Container Registry
- Azure Container Instances and Container Apps
- Azure App Service Configuration
- App Service Scaling and Networking
- Deployment Slots and Backup Configuration

Module 4: Implementing and Managing Virtual Networking

- Virtual Networks and Subnets Configuration
- Virtual Network Peering
- Public IP Addresses and User-Defined Routes
- Network Connectivity Troubleshooting
- Secure Access to Virtual Networks
- Network Security Groups (NSGs) and Application Security Groups
- Azure Bastion Implementation
- Service Endpoints and Private Endpoints
- Name Resolution and Load Balancing
- Azure DNS Configuration
- Internal and Public Load Balancers
- Load Balancer Troubleshooting

Module 5: Monitoring and Maintaining Azure Resources

- Monitoring with Azure Monitor
- Azure Metrics and Logs
- Alert Configuration and Management

- Monitoring Virtual Machines, Storage Accounts, and Networks
- Azure Network Watcher and Connection Monitor
- Backup and Recovery Implementation
- Recovery Services and Azure Backup Vaults
- Backup Policy Configuration
- Azure Site Recovery Setup and Failover
- Backup Reports and Alerts Interpretation

Cloud Security Engineer – Consultant Level

The Microsoft Azure Security Technologies course (AZ-500) covers essential topics related to securing Microsoft Azure environments. Students learn to implement and manage security controls, detect, and respond to security threats, and protect data, applications, and networks in Azure. Key areas of focus include identity and access management, data protection, threat protection, and security operations. Through hands-on labs and practical exercises, participants gain the skills needed to design and implement robust security solutions in Azure, ensuring the integrity and confidentiality of cloud-based assets.

Key Competencies Overview

- Manage identity and access
- Secure networking
- Secure compute, storage, and databases
- Manage security operations

Module 1: Manage Identity and Access

- Securing Microsoft Entra Identities
- Microsoft Entra ID Protection Implementation
- Microsoft Entra Authentication Configuration
- Multi-Factor Authentication (MFA) Implementation
- Passwordless Authentication Setup
- Single Sign-On (SSO) Configuration
- Microsoft Entra Authorization Management
- Role Permissions Configuration
- Microsoft Entra Built-In Roles Assignment
- Custom Role Creation and Assignment
- Microsoft Entra Permissions Management
- Conditional Access Policies Implementation
- Microsoft Entra Application Access Management
- Enterprise Applications Access Control
- Microsoft Entra App Registrations Management
- Service Principals and Managed Identities
- Microsoft Entra Application Proxy Configuration

Module 2: Secure Networking

- Virtual Network Security Planning and Implementation
- Network Security Groups (NSGs) and Application Security Groups (ASGs)
- User-Defined Routes (UDRs)
- Virtual Network Peering and VPN Gateway
- Virtual WAN Implementation
- VPN Connectivity Security
- Encryption Over ExpressRoute
- Firewall Settings Configuration for PaaS Resources
- Private Access to Azure Resources Planning and Implementation
- Virtual Network Service Endpoints
- Private Endpoints Configuration
- Private Link Services Implementation
- Network Security Configurations for Azure Services
- Azure Firewall and Azure Firewall Manager Setup
- Azure Application Gateway and Azure Front Door Implementation
- Web Application Firewall (WAF) Configuration

Module 3: Secure Compute, Storage, and Databases

- Advanced Security Planning for Compute
- Remote Access Configuration with Azure Bastion and JIT VM Access
- Network Isolation for Azure Kubernetes Service (AKS)
- AKS Security Monitoring and Authentication
- Security Monitoring for Azure Container Instances (ACIs) and Azure Container Apps (ACAs)
- Access Management for Azure Container Registry (ACR)
- Disk Encryption Configuration
- Security Configurations for Azure API Management
- Storage Security Planning and Implementation
- Access Control for Storage Accounts
- Methods for Access to Azure Files, Blob Storage, Tables, and Queues
- Data Security Threat Protection Strategies
- Azure SQL Database and Azure SQL Managed Instance Security Planning and Implementation

Module 4: Manage Security Operations

- Governance for Security with Azure Policy
- Security Settings Configuration with Azure Blueprints
- Secure Infrastructures Deployment using Landing Zones
- Azure Key Vault Configuration and Management
- Key Rotation and Backup for Certificates, Secrets, and Keys
- Security Posture Management with Microsoft Defender for Cloud
- Threat Protection Configuration with Microsoft Defender for Cloud
- Security Monitoring and Automation Solutions Configuration
- Security Event Monitoring with Azure Monitor
- Data Connectors Configuration in Microsoft Sentinel

- Analytics Rules Creation and Customization in Microsoft Sentinel
- Security Alerts and Incidents Management in Microsoft Sentinel
- Workflow Automation Configuration in Microsoft Sentinel

Get Career Ready

Prepare For Soft Skills

- LinkedIn Profile Building
- Resume Writing
- Communication skills as per industry needs
- Analytics skills
- Time management

Job Roles

- Cloud Security Engineer
- Presales Security Engineer
- Security Consultant