

IT Fundamentals for cloud concepts – 34 classes

Explain advantages provided by cloud to stakeholders

- Describe cloud infrastructure
- Distinguish between IaaS, PaaS, and SaaS
- Show how cloud allows building applications cheaper than with traditional models
- Show how cloud allows building applications faster than with traditional models

Explain cost to stakeholders

- Identify the use case (new development or transition of existing product or service)
- Identify the resources that will be required to construct the service or product using cloud-hosted components (include compute, data, and network costs)
- Identify support plan that will be required to meet performance, availability, scalability, and reliability (PASR) criteria
- Consider factors that go into return on investment

Explain performance to stakeholders

- Identify performance criteria
- Consider what solutions meet the criteria
- Assess cost and availability of technical expertise

Explain reliability to stakeholders

- Identify reliability criteria, including network speeds
- Consider what solutions meet the criteria
- Understand service-level agreement (SLA) with cloud provider
- Consider disaster-recovery and backup plans (including backup redundancy or replication factor)

Explain availability to stakeholders

- Identify the use case (new development or transition of existing product or service)
- Identify any upstream or downstream SLAs that will govern availability requirements
- Establish availability metrics
- Assess the SLA offered by the cloud-hosted solution

Explain scalability to stakeholders

- Identify the use case (new development or transition of existing product or service)
- Understand that rules can be set to adjust resources based on need

Recommend off-the-shelf (OTS) or custom solutions as needed

- Identify the use case (new development or transition of existing product or service)
- Evaluate if existing OTS offering meets performance, availability, scalability, and reliability needs
- Evaluate technical effort needed for custom solution
- Evaluate if custom solution can exceed OTS on PASR criteria

Developing cloud architecture

Choose between public, private, and hybrid cloud implementations

- Identify the security and privacy requirements for the solution (focusing on networking options that each provides)

- Consider limits imposed by tenancy in various cloud implementations

Draw an architectural diagram (show data flows)

- Break down the proposed solution into compute, data, and networking components
- Produce logical groupings for the components
- Mark data flows between components (including the protocol)
- Identify system and component boundaries (including responsibility model)

Define requirements

- Decide whether to virtualize server, network, storage, and desktop
- Be aware of design patterns like microservices and serverless
- Consider networking infrastructure, storage devices, memory, and end-user devices required

Identify how services communicate through application programming interfaces (APIs)

- Identifying services with which the application needs to integrate
- Interact using an API 2.5 Create virtual machines
- Determine the operating system for the virtual machines
- Choose the appropriate size for the virtual machines
- Decide on geographic setting for the virtual machines (latency, legal requirements)
- Configure options (e.g., time limitations, scaling, backups) for the virtual machines

Identify data storage requirements

- Distinguish between structured and unstructured data
- Determine amount of storage needed
- Consider location of storage
- Consider storage security

Implementing the cloud development life cycle

Create content in virtual environments

- Understand that a source-code management system needs to be set up
- Install and configure the prerequisite packages in the virtual environment
- Save changes and keep track of the codes in a source code management system (such as Github)

Perform testing

- Provide different test cases, test scenarios, and test scripts
- Run the tests and report the bugs iteratively

Structure the overall cloud-based solution

- Integrate systems and applications within the selected environment
- Integrate systems and applications with legacy systems
- Integrate systems and applications with third-party applications
- Distinguish between containers and virtual machines
- Know when to choose containers over virtual machines

Deploy application on server

- Decide on the strategy to deploy a new application, replacing a previous one
- Understand version control

- Identify cloud-hosted solutions to create code and data pipelines (e.g., cloud-native CI/CD offerings and workflow automation like GitHub Actions)
- Identify existing CI/CD practices

Managing cloud operations

Manage operational costs

- Understand usage-based pricing
- Scale up and scale down to meet demand cost-effectively

Develop business continuity and disaster recovery policy

- Identify potential risks and disaster scenarios
- Establish on-premise vs offsite backup strategy

Provide support to users

- Identify protection and security policies for external and internal users
- Provide application and hardware support for internal users
- Provide training tools for internal and external users

Monitoring cloud systems

- Log events
- Monitor hardware and software (e.g., interpret graphs and dashboards)
- Understand notifications or alerts for provisioning backup

Understanding cloud governance

Comply with privacy and regulatory requirements

- Identify relevant privacy requirements based on geographical and domain constraints (e.g. BIPA, HIPAA, PDP, FERPA, COPPA, GDPR, CCPA, etc.) as well as organization-specific policies
- Identify cloud-provider compliance for these privacy regulations
- Assess types of data managed within the environment
- Assess location and storage of data
- Be aware of NIST and ISO frameworks and standards

Comply with ethical guidelines

- Consider the impact of bias, lack of transparency, and lack of accountability
- Explain potential bias and transparency challenges with prebuilt services

Managing cloud security

- Understand options and concepts for identity verification and authentication, including digital identity and multifactor authentication
- Understand access policies and authorizations (e.g., options for access, vendor-provided roles vs. custom roles and permissions, and access hygiene, including least privilege access, removal of access when not needed, disabling accounts)
- Understand the importance of data security and encryption
- Understand options to protect against unauthorized access in cloud environments (including intrusion detection and prevention, firewalls)

Linux – 32 classes

- How to use Linux command-line Tools

- How to manage software
- How to configure hardware devices
- How to manage files
- How to boot Linux
- How to edit files by using text and GUI editor
- Understanding basic networking configuration in Linux
- Securing a Linux system
- Experience with configuring and managing Linux servers and web servers (Nginx and Apache)

AWS Fundamentals – 50 classes

Module 1: Introduction to Amazon Web Services

- Summarize the benefits of AWS
- Describe differences between on-demand delivery and cloud deployments
- Summarize the pay-as-you-go pricing model

Module 2: Compute in the Cloud

- Describe the benefits of Amazon Elastic Compute Cloud (Amazon EC2) at a basic level
- Identify the different Amazon EC2 instance types
- Differentiate between the various billing options for Amazon EC2
- Describe the benefits of Amazon EC2 Auto Scaling
- Summarize the benefits of Elastic Load Balancing
- Give an example of the uses for Elastic Load Balancing
- Summarize the differences between Amazon Simple Notification Service (Amazon SNS) and Amazon Simple Queue Services (Amazon SQS)
- Summarize additional AWS compute options

Module 3: Global Infrastructure and Reliability

- Summarize the benefits of the AWS Global Infrastructure
- Describe the basic concept of Availability Zones
- Describe the benefits of Amazon CloudFront and Edge locations
- Compare different methods for provisioning AWS services

Module 4: Networking

- Describe the basic concepts of networking
- Describe the difference between public and private networking resources
- Explain a virtual private gateway using a real life scenario
- Explain a virtual private network (VPN) using a real life scenario
- Describe the benefit of AWS Direct Connect
- Describe the benefit of hybrid deployments
- Describe the layers of security used in an IT strategy
- Describe which services are used to interact with the AWS global network

Module 5: Storage and Databases

- Summarize the basic concept of storage and databases
- Describe benefits of Amazon Elastic Block Store (Amazon EBS)
- Describe benefits of Amazon Simple Storage Service (Amazon S3)

- Describe the benefits of Amazon Elastic File System (Amazon EFS)
- Summarize various storage solutions
- Describe the benefits of Amazon Relational Database Service (Amazon RDS)
- Describe the benefits of Amazon DynamoDB
- Summarize various database services

Module 6: Security

- Explain the benefits of the shared responsibility model
- Describe multi-factor authentication (MFA)
- Differentiate between the AWS Identity and Access Management (IAM) security levels
- Describe security policies at a basic level
- Explain the benefits of AWS Organizations
- Summarize the benefits of compliance with AWS
- Explain primary AWS security services at a basic level

Module 7: Monitoring and Analytics

- Summarize approaches to monitoring your AWS environment
- Describe the benefits of Amazon CloudWatch
- Describe the benefits of AWS CloudTrail
- Describe the benefits of AWS Trusted Advisor

Module 8: Pricing and Support

- Understand AWS pricing and support models
- Describe the AWS Free Tier
- Describe key benefits of AWS Organizations and consolidated billing
- Explain the benefits of AWS Budgets
- Explain the benefits of AWS Cost Explorer
- Explain the primary benefits of the AWS Pricing Calculator
- Distinguish between the various AWS Support Plans
- Describe the benefits of AWS Marketplace

Module 9: Migration and Innovation

- Understand migration and innovation in the AWS Cloud
- Summarize the AWS Cloud Adoption Framework (AWS CAF)
- Summarize six key factors of a cloud migration strategy
- Describe the benefits of various AWS data migration solutions, such as AWS Snowcone, AWS Snowball, and AWS Snowmobile
- Summarize the broad scope of innovative solutions that AWS offers

Module 10: The Cloud Journey

- Summarize the five pillars of the AWS Well-Architected Framework
- Explain the six benefits of cloud computing

Module 11: Security in the AWS Cloud

- Hosting the employee directory application in AWS
- Hands-On Lab: Introduction to AWS Identity and Access Management (IAM)

Module 12: AWS Compute

- Compute as a service in AWS
- Introduction to Amazon Elastic Compute Cloud
- Amazon EC2 instance lifecycle
- AWS container services
- What is serverless?
- Introduction to AWS Lambda
- Choose the right compute service
- Hands-On Lab: Launch the Employee Directory Application on Amazon EC2

Module 13: AWS Networking

- Networking in AWS
- Introduction to Amazon Virtual Private Cloud (Amazon VPC)
- Amazon VPC routing
- Amazon VPC security
- Hands-On Lab: Create a VPC and Relaunch the Corporate Directory Application in Amazon EC2

Module 14: AWS Storage

- AWS storage types
- Amazon EC2 instance storage and Amazon Elastic Block Store (Amazon EBS)
- Object storage with Amazon S3
- Choose the right storage service
- Hands-On Lab: Create an Amazon S3 Bucket

Module 15: Databases

- Explore databases in AWS
- Amazon Relational Database Service
- Purpose-built databases
- Introduction to Amazon DynamoDB
- Choose the right AWS database service
- Hands-On Lab: Implement and manage Amazon DynamoDB

Module 16: Monitoring, Optimization, and Serverless

- Monitoring
- Optimization
- Alternate serverless employee directory application architecture
- Hands-On Lab: Configure High Availability for Your Application

Module 17: Exploring the Security Pillar

- AWS Well-Architected Framework: Security Pillar

Module 18: Security of the Cloud

- Shared responsibility model
- AWS Global Infrastructure
- Compliance and governance

Module 19: Identity and Access Management

- Identity and access management

- Data access and protection essentials
- Lab: Introduction to Security Policies

Module 20: Protecting Infrastructure and Data

- Protecting your network infrastructure
- Edge Security
- DDoS Mitigation
- Protecting compute resources
- Lab: Securing VPC Resources with Security Groups

Module 21: Detection and Response

- Monitoring and detective controls
- Incident response essentials

Module 22: Course Wrap-Up

AWS System Architecture and Operations – 80 classes

Module 1: Architecting Fundamentals

- AWS services
- AWS infrastructure
- AWS Well-Architected Framework
- Hands-on lab: Explore and interact with the AWS Management Console and AWS Command Line Interface

Module 2: Account Security

- Principals and identities
- Security policies
- Managing multiple accounts

Module 3: Networking 1

- IP addressing
- VPC fundamentals
- VPC traffic security

Module 4: Compute

- Compute services
- EC2 instances
- Storage for EC2 instances
- Amazon EC2 pricing options
- AWS Lambda
- Hands-On Lab: Build your Amazon VPC infrastructure

Module 5: Storage

- Storage services
- Amazon S3
- Shared file systems
- Data migration tools

Module 6: Database Services

- Database services
- Amazon RDS
- Amazon DynamoDB
- Database caching
- Database migration tools
- Hands-on Lab: Create a database layer in your Amazon VPC infrastructure

Module 7: Monitoring and Scaling

- Monitoring
- Alarms and events
- Load balancing
- Auto scaling
- Hands-on Lab: Configure high availability in your Amazon VPC

Module 8: Automation

- AWS CloudFormation
- Infrastructure management

Module 9: Containers

- Microservices
- Containers
- Container services

Module 10: Networking 2

- VPC endpoints
- VPC peering
- Hybrid networking
- AWS Transit Gateway

Module 11: Serverless

- What is serverless?
- Amazon API Gateway
- Amazon SQS
- Amazon SNS
- Amazon Kinesis
- AWS Step Functions
- Hands-on Lab: Build a serverless architecture

Module 12: Edge Services

- Edge fundamentals
- Amazon Route 53
- Amazon CloudFront
- DDoS protection
- AWS Outposts
- Hands-On Lab: Configure an Amazon CloudFront distribution with an Amazon S3 origin

Module 13: Backup and Recovery

- Disaster planning
- AWS Backup
- Recovery strategies
- Hands-on Lab: Capstone lab – Build an AWS Multi-Tier architecture. Participants review the concepts and services learned in class and build a solution based on a scenario. The lab environment provides partial solutions to promote analysis and reflection. Participants deploy highly available architecture. The instructor is available for consultation.

Module 14: Architecting on AWS – Jam Session - hackaton

Module 15: Getting Started with Databases

- Describe the key components of DynamoDB
- Explain how to connect to DynamoDB
- Describe how to build a request object
- Explain how to read a response object
- List the most common troubleshooting exceptions

Module 16: Processing Your Database Operations

- Develop programs to interact with DynamoDB using AWS SDKs
- Perform CRUD operations to access tables, indexes, and data
- Describe developer best practices when accessing DynamoDB
- Review caching options for DynamoDB to improve performance
- Perform DynamoDB operations using SDK

Module 17: Building a Modern Application

- Describe the challenges with traditional architectures
- Describe the microservice architecture and benefits
- Explain various approaches for designing microservice applications
- Explain steps involved in decoupling monolithic applications
- Demonstrate the orchestration of Lambda Functions using AWS Step Functions

Module 18: Continuous integration and continuous delivery (CI/CD) with development tools

- CI/CD Pipeline and Dev Tools
- Demonstration: CI/CD pipeline displaying some actions from AWS CodeCommit, AWS CodeBuild, AWS CodeDeploy and AWS CodePipeline
- AWS CodePipeline
- Demonstration: AWS integration with Jenkins

Module 19: Introduction to Microservices

- Introduction to Microservices

Module 20: DevOps and containers

- Deploying applications with Docker
- Amazon Elastic Container Service and AWS Fargate
- Amazon Elastic Container Registry and Amazon Elastic Kubernetes service
- Demonstration: CI/CD pipeline deployment in a containerized application

Total technical training is 196 classes.

SOFT SKILLS

- Analytical skills
- Design skills,
- Communication skills;
- Presentations skills;
- Basics of time management;
- Various types of online outsourcing marketplaces that exist and their utilization in the context of Kosovo;
- How to approach and communicate with different types of clients; Basics of project management (use of project management and communication software);
- Making a resume, project portfolio.