Advanced Post Graduate Program In Cloud, Devops and Security

Azure | AWS | Linux | DevOps | Security

Fundamentals of Cloud Computing

Topics Covered

- Cloud Computing
  - Desktop Computing
  - Server Client Computing
  - Cluster Computing
  - Grid Computing
- Service Models of Cloud
  - Infrastructure as a Service
  - Platform as a Service
  - Software as a Service
  - Database as a Service
- Types of Cloud
  - Private Cloud
  - Public Cloud
  - Hybrid Cloud
- Advantages of Cloud Computing
- Parts of Cloud Computing
- Deployment methods of Cloud Computing
  - Cloud-based Deployment
  - Hybrid Deployment
- Virtualization
  - Hosted Virtualization
  - Bare-metal Virtualization

Azure Fundamentals

Azure Fundamentals and Core Services

- Azure Fundamentals
- Core Azure Architectural Concepts
- Azure Compute Services
- Azure Networking Services
- Azure Storage Services
- Azure Database and Analytics Services

Azure General Security and Network Security

- Protect against Security threats on Azure
- Secure Network connectivity on Azure

Azure Identity, Governance, Private and Compliance Features

- Secure access to your applications by using Azure Identify Services
- Build a cloud governance strategy on Azure
- Examine Privacy, Compliance and data protection standards on Azure

Azure Cost Management and Service Level Agreement

- Plan and manage your Azure Costs
- Choose the right Azure services by examining Service Level Agreement and service lifecycle.

Azure Administrator

Additional Resources of Azure Administrator

- Configure Azure Resources with tools
- Use Azure Resource Manager
- Configure Resources with ARM Templates
- Automate Azure Tasks using scripts with PowerShell
- Control Azure services with the Azure CLI
- Deploy Azure infrastructure by using JSON ARM Templates

Manage Identities and Governance in Azure

- Configure Azure Active Directory
- Configure User and Group accounts
- Configure Subscription
- Configure Azure Policy
- Configure Role-Based Access Control
- Create Azure Users and Groups in Azure Active Directory
- Secure your Azure Resources with Azure Role-Based Access Control
- Allow Users to reset their password with Azure Active Directory Self-Service Password Reset

Implement and Manage Storage in Azure

- Configure Storage Account
- Configure Blob Storage
- Configure Storage Security
- Configure Azure Files and Azure File Sync
- Configure Storage with tools
- Create an Azure Storage Account
- Control access to Azure Storage with shared access signature (SAS)
- Upload, download and manage data with Azure Storage Explorer

Deploy and Manage Azure Compute Resources

- Configure Virtual Machine
- Configure Virtual Machine Availability
- Configure Virtual Machine Extension
- Configure App Service Plan
- Configure Azure App Services
- Configure Azure Container Instances
- Configure Azure Kubernetes Services
- Manage Virtual Machine with Azure Command Line Interface
- Create a Windows Virtual Machine in Azure
- Host a Web application with Azure App Services
- Protect your Virtual Machine Settings with Azure Automation State Configuration

Configure and Manage Virtual Network for Azure Administrators

- Configure Virtual Networks
- Configure Network Security Groups
- Configure Azure Firewall
- Configure Azure DNS
- Configure Virtual Network Peering
- Configure VPN Gateway
- Configure ExpressRoute and Virtual WAN
- Configure Network Routing and endpoints
- Configure Azure Load Balancer
- Configure Azure Application Gateway
- Design an IP Addressing schema for your Azure Deployment
- Distribute your services across Azure Virtual Networks and Integrate them by using Virtual Network Peering
- Host your domain on Azure DNS
- Manage and control Traffic flow in your Azure Deployment with routes
- Improve application scalability and resiliency by using Azure Load Balancer

Monitor and Backup Azure Resources

- Configure file and folder backups
- Configure Virtual Machine backups
- Configure Azure Monitor
- Configure Azure Alerts
- Configure Log Analytics
- Configure Network Watcher
- Improve incident response with alerting on Azure
- Analyze your Azure infrastructure by using Azure Monitor Logs
- Monitor Performance of Virtual Machines by using Azure Monitor Virtual Machine Insight.

Designing Azure Infrastructure Solutions

Design, Identity, Governance and Monitor Solutions

- Design Governance
- Design Authentication and Authorization solutions
- Design a solution to log and monitor Azure Resource

Design business continuity Solutions

- Design for high Availability
- Design a solution for backup and disaster recovery.

Design data storage Solutions

- Design a data storage solution for non-relational data.
- Design a data storage solution for Relational data
- Design data integration

Design Infrastructure Solutions

- Design a compute solution
- Design an application architecture
- Design network solutions
- Design migrations

Build great solutions with the Microsoft Azure Well

Architected Framework

- Introduction to the Microsoft Azure Well Architected Framework
- Cost Optimization
- Operational Excellence
- Performance Efficiency
- Reliability
- Security

Accelerate Cloud adoption with the Microsoft Cloud Adoption Framework for Azure

- Getting started with Microsoft Cloud Adoption Framework for Azure
- Prepare for successful cloud adoption with well-defined strategy
- Prepare for cloud adoption with a data driven plan
- Choose the best Azure Landing Zone to support your requirements for cloud operations
- Migrate to Azure through repeatable processes and common tools
- Address tangible risks with the govern methodology of the cloud adoption Framework for Azure
- Ensure stable operations and optimization across all supported workloads deployed to the cloud
- Innovate applications by using Azure Cloud Technologies

AWS Cloud Concepts-Practitioner

Define the AWS Cloud and its value proposition

- Define the benefits of the AWS
- Explain how the AWS cloud allows users to focus on business value

Identify aspects of AWS Cloud economics

- Define items that would be part of a Total cost of Ownership Proposal
- Identify which operations will reduce costs by moving the cloud

Explain the different cloud architecture design principles

- Explain the design principles

AWS Security and Compliance

Define the AWS shared responsibility model

- Recognize the elements of the shared responsibility model
- Describe the customers responsibility model
- Describe AWS responsibilities

Define AWS Cloud security and compliance concepts

- Identify where to find AWS compliance information
- At a high level, describe how customers achieve compliance on AWS
- Describe who enables encryption on AWS for a given services
- Recognize there are services that will aid in auditing and reporting
- Explain the concept of least privileged access

Identify AWS access management capabilities

- Understand the purpose of User and Identity Management

Identify resources for security support

- Recognize there are different network security capabilities
- Recognize there is documentation and where to find it
- Know that security checks are a component of AWS Trusted Advisor

Define methods of deploying and operating in the AWS cloud

- Identify at a high level different ways of provisioning and operating in the AWS cloud
- Identify different types of cloud deployment models
- Identify connectivity options

Define the AWS Global Infrastructure

- Describe the relationships among Regions, Availability Zones, and Edge Locations
- Describe how to achieve high availability through the use of multiple Availability Zones
- Describe when to consider the use of multiple AWS Regions
- Describe at a high level the benefits of Edge Locations

Identify the core AWS services

- Describe the categories of services on AWS (Compute, Storage, Network, Database)
- Identify AWS compute services
- Identify different AWS storage services
- Identify different AWS storage services
- Identify AWS networking Services
- Identify different AWS database services

Identify resources for technology support

- Recognize there is documentation (best practices, whitepapers, AWS knowledge center, forums, blogs)
- Identify the various levels and scope of AWS support
- Recognize there is a partner network including independent software vendors and system integrators
- Identify sources of AWS technical assistance and knowledge including professional services, solution architects, training and certification and the AWS Partner Network
- Identify the benefits of using AWS Trusted Advisor

Billing and Pricing

Compare and contrast the various pricing models for AWS

- Identify scenarios fit for On-Demand Instance pricing
- Identify scenarios fit for Reserved-Instance pricing
- Identify scenarios fit for Spot Instance pricing

Recognize the various account structures in relation to

AWS billing and pricing

- Recognize that consolidated billing is a feature of AWS Organizations
- Identify how multiple accounts aid in allocating costs across departments

Identify resources available for billing support

- Identify ways to get billing support and information
- Identify where to find pricing information on AWS services
- Recognize that alarms and alerts exist
- Identify how tags are used in cost allocation

AWS Solutions Architect- Associate/Professional

Design secure access to AWS resources

- Access controls and management across multiple accounts
- AWS federated access and identity services - IAM | AWS SSO
- AWS global infrastructure
- AWS shared responsibility model

Design secure workloads and applications

- Application configuration and credentials security
- AWS service endpoints
- Control ports, protocols, and network traffic on AWS
- Secure application access
- Security services with appropriate use cases
- Threat vectors external to AWS

Determine appropriate data security controls

- Data access and governance
- Data recovery
- Data retention and classification
- Encryption and appropriate key management

Design Resilient Architectures

Design scalable and loosely coupled architectures

- API creation and management
- AWS managed services with appropriate use cases
- Caching strategies
- Design principles for microservices
- Event-driven architectures
- Horizontal scaling and vertical scaling
- How to appropriately use edge accelerators
- How to migrate applications into containers
- Load balancing concepts
- Multi-tier architectures
- Queuing and messaging concepts
- Serverless technologies and patterns
- Storage types with associated characteristics
- The orchestration of containers with Elastic Kubernetes Services
- When to use read replicas
- Workflow orchestration

Design High available and fault-tolerant architectures

- AWS global infrastructure
- AWS managed services with appropriate use cases
- Basic networking concepts
- Disaster recovery strategies
- Distributed design patterns
- Failover strategies
- Immutable infrastructure
- Load balancing concepts
- Proxy concepts
- Service quotas and throttling
- Storage options and characteristics
- Workload visibility

Design High-Performing Architectures

Determine high-performing and scalable storage solutions

- Hybrid storage solutions to meet business requirements
- Storage services with appropriate use cases
- Storage types with associated characteristics

Design High-performance and elastic compute solutions

- AWS compute services with appropriate use cases
- Distributed computing concepts supported by AWS global infrastructure and edge services
- Queuing and messaging concepts
- Scalability capabilities with appropriate use cases
- Serverless technologies and patterns
- The orchestration of containers

Determine high-performing database solutions

- Caching strategies and services
- Data access pattern
- Database capacity planning
- Database engines with appropriate use cases
- Database replication
- Database types and services

Determine high-performing and scalable network architectures

- Edge networking services with appropriate use cases
- How to design network architecture
- Network connection options

Determine high-performing data ingestion and transformation solutions

- Data analytics and visualization services with appropriate use cases
- Data ingestion patterns
- Data transfer services with appropriate use cases
- Data transformation services with appropriate use cases
- Secure access to ingestion access points
- Sizes and speeds indeed to meet business requirements
- Streaming data service with appropriate use cases

Design Cost-Optimized Architecture

Design cost-optimized storage solutions

- Access options : S3 bucket with Requester pays object storage
- AWS cost management service features
- AWS cost management with appropriate use cases
- AWS storage service with appropriate use cases
- Backup strategies
- Block storage options
- Data lifecycles
- Hybrid storage options
- Storage access patterns
- Storage tiering
- Storage types with associated characteristics

Design cost-optimized compute solutions

- AWS cost management service features
- AWS cost management tools with appropriate use cases
- AWS purchasing options
- Distributed compute strategies
- Hybrid compute options
- Instance types, families and sizes
- Optimization of compute utilization
- Scaling strategies

Design cost-optimized database solutions

- Data retention policies
- Database capacity planning
- Database connections and proxies
- Database engines with appropriate use cases
- Database replication
- Database types and services

Design cost-optimized network architectures

- AWS cost management service features
- NAT gateway
- Network connectivity
- Network routing, topology and peering
- Network services with appropriate use cases

Linux Administration

Getting Started with Linux

- What is Linux and Open Source
- Linux Basic Shell commands
- Globbing
- Process Management
- Archive and Compressions

Users and Permissions

- Local Linux Users, Password Properties, Group
- Substitute User and Sudo Command
- Basics Permissions – chmod, chown, chgrp
- Access Control List
- Special Permissions

Networking

- Managing IP Properties Using IP Command
- Network Manager – NMTUI and NMCLI

Software and Service Management

- Connecting to Repository for Installing, Updating, Upgrading and Removing Software Packages Using YUM and DNF
- Managing Services Using Service and Systemctl commands

Basic Services

- Remote Access Using SSH and Remote Copy Using SCP
- Synchronizing Time Using NTP – Chronyd
- Scheduling Tasks with at and cron
- Managing OS Firewall – Firewalld

Storage Management

- Introduction to Storage in Linux and Creating Partition
- Swap
- Managing Disks using Logical Volume Manager
- Stratis Local Storage
- Virtual Data Optimizer

Advanced Services

- Sharing Files Using NFS
- Sharing Files Using SMB
- Apache Web Server – Basic, Virtual Hosting, TLS
- Server Booting Concepts and Troubleshooting

Introductions DevOps

Understanding DevOps

- What is DevOps?
- Why DevOps?
- Dev Challenges
- Ops Challenges
- Stages of DevOps Lifecycle
    - Continuous Development
    - Continuous Testing
    - Continuous Integration
    - Continuous Deployment
    - Continuous Monitoring
    - The Various DevOps Tools Introduction
    - Roles and Responsibilities of a DevOps Engineer
    - How DevOps fits in the whole Software Development Lifecycle

Git and Github- Version Control System

- Why Version Control System
- VCS tools
- Distributed VCS
- What is Git and Why Git?
- Features of Git
- Git Workflow
- Git Configurations
- Creating Git Repository
- Syncing Repositories
- Adding Origin
- Pushing changes
- Pulling changes
- Clone operation
- Concepts of Branches
- Merge requests
- Deleting Branches
- Resolving Merge Conflicts
- Git Ignore
- Git Stash
- Merging Branches

Continuous Integration with Jenkins

- Challenges before Continuous Integration
- What is Continuous Integration?
- Benefits of Continuous Integration
- Tools of Continuous Integration
- Jenkins Plugins
- Introduction to Jenkin
- Build setup in Jenkins
- Jenkins Pipeline
- Create a simple Pipeline Job
- Full Jenkins file Syntax Demo
- Create a full Pipeline Job
- Build Java App
- Build Docker Image
- Push to Private DockerHub
- Create a Multi-Branch Pipeline Job
- Credentials in Jenkins

Docker - Containerization

- Virtualization vs Containerization
- What are Containers and Advantages of Containers
- Architecture of Docker Container
- Components of Docker - Images | Registries
- Managing Docker Service
- Running a Container
- Starting | Stopping | Restarting Containers
- Container Networking | Bridge | Host | Overlay
- Managing Storage for Containers
- Understanding Docker File
- Docker Hub - Pushing Images to Repository

Containerization Orchestration

- Introduction to Kubernetes
- Understand the Main Kubernetes Components
- Node, Pod, Service, Ingress, ConfigMap, Secret, Volume, Deployment, StatefulSet
- Kubernetes Architecture
- Minikube and Kubectl - Local Setup

- Main Kubectl Commands - K8s CLI
- Create and Debug Pod in a Minicluster
- Kubernetes YAML Configuration File
- Create and Configure Deployment and Service Components
- Organizing your components with K8s Namespaces
- Kubernetes Service Types
- Making your App accessible from outside with Kubernetes Ingress
- Persisting Data in Kubernetes with Volumes
- Persistent Volume
- Persistent Volume Claim
- Storage Class
- ConfigMap and Secret Kubernetes Volume Types
- Deploying Stateful Apps with StatefulSet
- Deploying Kubernetes cluster on a Managed Kubernetes Service (K8s-on Cloud)
- Helm - Package Manager of Kubernetes
- Creating a ECS Cluster
- Creating a EKS Cluster

Automation with Ansible

- What is Ansible, Uses and How Ansible Works.
- Architecture
- Control Node
- Managed Node
- Inventory
- Module
- Play and Playbook
- Managing Static Inventory
- Creating Ansible Project Directory and Configurations
- Understanding Ansible Ad-hoc Commands
- Privilege Escalation Configuration
- Understanding YAML and Writing Simple Ansible Playbook
- Using Variables in Ansible Playbook
- Using Loop
- Using Conditions
- Ansible Roles from Ansible Galaxy

Automation with Terraform

- What is IAC and Terraform and Installation
- Understanding Provider, Resource Type, Terraform LifeCycle
- Terraform State File
- Output Value
- Attribute Reference
- Variables
- Variable DataTypes
- Count and Count Index
- Conditional expression
- Local Value
- Terraform Functions and Data Sources
- Terraform Provisioner
- Local exec and Remote exec
- Terraform Modules and Workspace
- Terraform Cloud

Cloud Security:

Module 1 - Incident Response

- What is Incident Response in Cloud
- Foundation of Incident Response
- Prepare for Cloud Security – People and Technology
- Simulate Incident Response
- Shared Responsibility Model and AWS CAF
- Where do CloudSecurity Events occur
- Amazon Guard Duty and its concepts
- Incident Response Plan
- CloudEndure Disaster Recovery
- Amazon Detective

Module 2 - Logging and Monitoring

- Introduction to CloudWatch
- Metrics and namespaces
- CloudWatch architecture
- Dashboards in CW
- CloudWatch alarms
- CloudWatch logs
- Pricing and design patterns
- Introduction to CloudTrail
- Accessing CloudTrail and tracking API usage

Module 3 - Infrastructure Security

- Network Security
- Network Monitoring and Protection
- Firewalls and DDoS
- Content Delivery Networks and Edge Locations
- Intrusion Detection and Prevention systems
- AWS Shield
- AWS CloudFront and Signed URLs
- Lambda@Edge
- AWS Network Firewall

Module 4 - Identity and Access Management

- Pre-IAM and why access management?
- Amazon Resource Name (ARN) and IAM features
- Multi-factor authentication (MFA) in IAM and JSON
- IAM policies and IAM permissions
- IAM roles
- Identity federation and pricing

Module 5 - Data Protection

- Introduction to Cryptography
- Cryptography Terminologies and Concepts
- Symmetric and Asymmetric Key Encryption
- CloudHSM
- AWS KMS
- Data Protection in KMS

- KMS Policy Evaluation Logic
- AWS Secrets Manager

Module 6 - Cloud Concepts

- Cloud Concepts, Architecture, and Design Principles.
- Understand cloud computing concepts, models, and service architectures.
- Identify cloud deployment models (e.g., public, private, hybrid, community).
- Explain the principles of cloud security architecture.
- Assess cloud service provider architecture and security capabilities.
- Design security for cloud data centers, infrastructure, and applications.
- Implement identity and access management controls in cloud environments.

Module 7 - Cloud Data Security

- Understand data classification and protection requirements in the cloud.
- Apply data encryption techniques for data in transit and at rest.
- Implement data masking and anonymization techniques.
- Design and implement cloud-based data loss prevention (DLP) controls.
- Manage data retention and deletion in cloud environments.
- Ensure compliance with relevant data protection regulations (e.g., GDPR, HIPAA) in the cloud.

Module 8 - Cloud Platform & Infrastructure Security

- Understand cloud infrastructure components (e.g., virtualization, containers).
- Secure cloud storage solutions (e.g., object storage, block storage).
- Implement network security controls in cloud environments.
- Manage cloud-based compute resources securely.
- Implement secure configuration management and patch management practices.
- Design and implement disaster recovery and business continuity plans for cloud services.

Module 9 - Cloud Application Security

- Understand secure software development principles and practices.
- Implement security controls in cloud-based applications.
- Secure APIs and microservices in cloud environments.
- Assess and mitigate security risks in serverless computing environments.
- Implement security testing and assurance techniques for cloud applications.
- Ensure compliance with relevant regulations and standards in cloud application development.

Module 10 - Cloud Security Operations

- Understand cloud security operations and management processes.
- Implement and manage cloud security monitoring and logging solutions.
- Design and implement threat detection and incident response procedures for cloud environments.
- Implement cloud-based identity and access management (IAM) solutions.
- Manage security configurations and compliance in cloud environments.
- Conduct security assessments and audits of cloud service providers.

Module 11 - Legal, Risk, and Compliance

- Understand legal and regulatory requirements relevant to cloud security.
- Assess and manage risks associated with cloud adoption.
- Implement cloud security governance frameworks and controls.
- Ensure compliance with industry standards and best practices (e.g., ISO 27001, NIST Cybersecurity Framework).
- Understand the shared responsibility model and contractual agreements in cloud computing.
- Address legal and compliance issues related to cloud data privacy and sovereignty.