Radical TECHNOLOGIES

AWS CERTIFIED CLOUD PRACTITIONER

DURATION: 24 HOURS

AWS Certified Cloud Practitioner

The AWS Certified Cloud Practitioner certification is an entry-level credential offered by Amazon Web Services (AWS) that provides a solid foundation in cloud computing concepts and AWS services. It is ideal for beginners and professionals from non-technical backgrounds who want to understand how AWS supports businesses through cloud solutions.

KEY LEARNING OUTCOMES:

- **Understand the fundamental concepts of cloud computing and AWS global infrastructure**
- **Learn core AWS services such as compute, storage, database, and networking**
- **Explore AWS pricing models, billing, and account management**
- **Gain insights into AWS security, compliance, and shared responsibility model**
- **Prepare effectively for the AWS Certified Cloud Practitioner exam**

WHY CHOOSE US:

- **Industry-recognized curriculum aligned with AWS standards**
- **Practical learning with case studies and live demos**
- **Flexible scheduling for working professionals**
- **Continuous mentor support and certification guidance**

AWS Certified Cloud Practitioner
Duration of Training : 24 Hours
Batch type : Weekdays/Weekends
Mode of Training : Classroom/Online/Corporate Training

Cloud concepts

DEFINE THE AWS CLOUD AND ITS VALUE PROPOSITION

– define the benefits of the aws cloud including:

- Security
- Reliability
- High availability
- Elasticity
- Agility
- Pay-as-you go pricing
- Scalability
- Global reach
- Economy of scale

– explain how the aws cloud allows users to focus on business value

Shifting technical resources to revenue-generating activities as opposed to managing infrastructure

IDENTIFY ASPECTS OF AWS CLOUD ECONOMICS

– define items that would be part of a total cost of ownership proposal

- Understand the role of operational expenses (opex)
- Understand the role of capital expenses (capex)
- Understand labor costs associated with on-premises operations
- Understand the impact of software licensing costs when moving to the cloud

– identify which operations will reduce costs by moving to the cloud

- Right-sized infrastructure
- Benefits of automation
- Reduce compliance scope (for example, reporting)

Managed services (for example, rds, ecs, eks, dynamodb)

Explain the different cloud architecture design principles

– explain the design principles

- Design for failure
- Decouple components versus monolithic architecture
- Implement elasticity in the cloud versus on-premises
- Think parallel

Security and compliance

DEFINE THE AWS SHARED RESPONSIBILITY MODEL

– recognize the elements of the shared responsibility model
– describe the customer's responsibly on aws
- Describe how the customer's responsibilities may shift depending on the service used (for example with rds, lambda, or ec2)

– describe aws responsibilities

Define aws cloud security and compliance concepts
– identify where to find aws compliance information
- Locations of lists of recognized available compliance controls (for example, hippa, socs)
- Recognize that compliance requirements vary among aws services

– at a high level, describe how customers achieve compliance on aws
- Identify different encryption options on aws (for example, in transit, at rest)

– describe who enables encryption on aws for a given service
– recognize there are services that will aid in auditing and reporting
- Recognize that logs exist for auditing and monitoring (do not have to understand the logs)
- Define amazon cloudwatch, aws config, and awscloudtrail

– explain the concept of least privileged access

IDENTIFY AWS ACCESS MANAGEMENT CAPABILITIES

– understand the purpose of user and identity management

- Access keys and password policies (rotation, complexity)
- Multi-factor authentication (mfa)
- Aws identity and access management (iam)
- – groups/users
- – roles
- – policies, managed policies compared to custom policies
- Tasks that require use of root accounts

Protection of root accounts

Identify resources for security support

– recognize there are different network security capabilities

- Native aws services (for example, security groups, network acls, awswaf)
- 3rd party security products from the aws marketplace

– recognize there is documentation and where to find it (for example, best practices, whitepapers, official documents)

- Aws knowledge center, security center, security forum, and security blogs
- Partner systems integrators

– know that security checks are a component of aws trusted advisor

Technology

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

- Programmatic access, apis, sdks, aws management console, cli, infrastructure as code

– identify different types of cloud deployment models

- All in with cloud/cloud native
- Hybrid
- On-premises

– identify connectivity options

- Vpn
- Aws direct connect

Public internet

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

- Recall that high availability is achieved by using multiple availability zones
- Recognize that availability zones do not share single points of failure

– describe when to consider the use of multiple aws regions

- Disaster recovery/business continuity
- Low latency for end-users
- Data sovereignty

– describe at a high level the benefits of edge locations

- Amazon cloudfront

Aws global accelerator

IDENTIFY THE CORE AWS SERVICES

– describe the categories of services on aws (compute, storage, network, database)

– identify aws compute services

- Recognize there are different compute families
- Recognize the different services that provide compute (for example, aws lambda compared to amazon elastic container service (amazon ecs), or amazon ec2, etc.)
- Recognize that elasticity is achieved through auto scaling
- Identify the purpose of load balancers

– identify different aws storage services

- Describe amazon s3
- Describe amazon elastic block store (amazon ebs)
- Describe amazon s3 glacier
- Describe aws snowball
- Describe amazon elastic file system (amazon efs)
- Describe aws storage gateway

– identify aws networking services

- Identify vpc
- Identify security groups
- Identify the purpose of amazon route 53
- Identify vpn, aws direct connect

– identify different aws database services

- Install databases on amazon ec2 compared to aws managed databases
- Identify amazon rds
- Identify amazon dynamodb
- Identify amazon redshift

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

- Aws abuse
- Aws support cases
- Premium support
- Technical account managers

– recognize there is a partner network (marketplace, third-party) 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 amazon partner network
– identify the benefits of using aws trusted advisor

Billing and pricing

COMPARE AND CONTRAST THE VARIOUS PRICING MODELS FOR AWS (FOR EXAMPLE, ON-DEMAND INSTANCES, RESERVED INSTANCES, AND SPOT INSTANCE PRICING)

– identify scenarios/best fit for on-demand instance pricing
– identify scenarios/best fit for reserved-instance pricing

- Describe reserved-instances flexibility

Describe reserved-instances behavior in aws organizations
– identify scenarios/best 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

- Cost explorer, aws cost and usage report, amazon quicksight, third-party partners, and aws marketplace tools
- Open a billing support case
- The role of the concierge for aws enterprise support plan customers

– identify where to find pricing information on aws services

- Aws simple monthly calculator
- Aws services product pages
- Aws pricing api

– recognize that alarms/alerts exist
– identify how tags are used in cost allocation

CONTACT US

+91-8055223360

www.radicaltechnologies.co.in

PUNE | BANGALORE | KERALA | UK

training@radicaltechnologies.co.in