AWS Certified Solutions Architect: Associate - Overview

Overview

- Amazon Web Services Certified Solutions Architect: Associate
    - Certification provided by Amazon
    - Details available online
    - Exam Blueprint
    - Tester should have
        - 1+ years of experience with designing solutions on AWS
        - In-depth knowledge of at least one programming language
        - Ability to identify requirements for an AWS-based application
        - Experience with deploying hybrid systems with on-premises and AWS components
        - Capability to provide best practices for building secure and reliable applications on the AWS platform
    - Exam
        - Available online through Webassessor
        - Questions
            - Multiple choice
            - Multiple answer
        - 80 minutes
        - $150 USD
        - Practice exam is available for $20 USD
- Recommended Supplemental Materials
    - AWS Certification Guide
    - AWS Cloud Computing Whitepapers
        - Overview of Amazon Web Services
        - Overview of Security Processes
        - AWS Risk & Compliance Whitepaper
        - Storage Options in the Cloud
        - Architecting for the AWS Cloud: Best Practices

Exam Objectives

The latest are available online

1. Designing highly available, cost-efficient, fault-tolerant, scalable systems
    - Identify and recognize cloud architecture considerations, such as fundamental components and effective designs.
        - How to design cloud services
        - Planning and design
        - Monitoring and logging
        - Familiarity with:
            - Best practices for AWS architecture
            - Developing to client specifications, including pricing/cost
            - Architectural trade-off decisions
            - Hybrid IT architectures
            - Elasticity and scalability
2. Implementation/Deployment
    - Identify the appropriate techniques and methods using Amazon EC2, Amazon S3, AWS Elastic Beanstalk, AWS CloudFormation, AWS OpsWorks, Amazon Virtual Private Cloud (VPC), and AWS Identity and Access Management (IAM) to code and implement a cloud solution.
        - Configure an Amazon Machine Image (AMI)
        - Operate and extend service management in a hybrid IT architecture
        - Configure services to support compliance requirements in the cloud
        - Launch instances across the AWS global infrastructure
        - Configure IAM policies and best practices
3. Data Security
    - Recognize and implement secure practices for optimum cloud deployment and maintenance. Content may include the following:
        - AWS shared responsibility model
        - AWS platform compliance
        - AWS security attributes (customer workloads down to physical layer)
        - AWS administration and security services
        - AWS Identity and Access Management (IAM)
        - Amazon Virtual Private Cloud (VPC)
        - AWS CloudTrail
        - Ingress vs. egress filtering, and which AWS services and features fit
        - “Core” Amazon EC2 and S3 security feature sets
        - Incorporating common conventional security products (Firewall, VPN)
        - Design patterns
        - DoS mitigation
        - Encryption solutions (e.g., key services)
        - Complex access controls (building sophisticated security groups, ACLs, etc.)

- Amazon CloudWatch for the security architect
- Trusted Advisor
- CloudW atch Logs

- Recognize critical disaster recovery techniques and their implementation. Content may include the following:
  - Disaster recovery
    - Recovery time objective
    - Recovery point objective
    - Amazon Elastic Block Store
  - AWS Import/Export
  - AWS Storage Gateway
  - Amazon Route53
  - Validation of data recovery method

4. Troubleshooting
   - General troubleshooting information and questions

Show Outline

1. Introduction to AWS
2. Amazon S3 and Glacier Storage
3. Amazon EC2 and EBS
4. Amazon Virtual Private Cloud
5. ELB, CloudWatch and Auto Scaling
6. AWS Identity and Access Management
7. Databases and AWS
8. SQS, SWF, and SNS
9. DNS and Amazon Route 53
10. Amazon ElastiCache
11. Additional Key Services
12. Security on AWS
13. AWS Risk and Compliance
14. Architecture Best Practices