INFOSECTRAIN

AWS COMBO COURSE

AWS SECURITY – SPECIALTY (SCS-C01)
+
AWS ARCHITECT – ASSOCIATE (SAA-C03)

KEY FEATURES

- 60 Hrs of instructor-led training
- Post Training support
- Access to the recorded sessions
- Certified & Experienced Instructors

OVERVIEW

AWS Combo Course (Architect Associate + Security-Specialty) aims to help you get through AWS certification (Fundamental + Advanced level) in the first attempt. It has been designed to help you learn how to architect, deploy secure and robust applications on AWS Cloud, and train you on the major components in AWS technology. This course will help you to enhance your overall AWS architecture knowledge. It will give you opportunities to look into various Real-World scenarios so that you can understand the reasons behind the hacking of the websites and how to deal with such situations. You will be able to:

- Define and design architectural solutions on the basis of customer requirements.
- Offer best implementation practices and guidance throughout the project life-cycle.
- Understand the reasons behind the hacking of the websites and how to deal withsuch situations
- Become a qualified AWS security specialist eligible enough to handle the real-world environment.

Along with the right kind of theoretical knowledge to achieve the certification, you will also receive hands-on experience working with cloud computing during this AWS architect training.

INFOSECTRAIN

Target Audience

AWS Combo Course has been designed for:

- Absolute beginners for AWS thus, no prior AWS experience necessary
- Professionals working as Solutions Architects
- Programmers who wish to learn deploying Applications on AWS
- Anyone interested in hosting highly scaleable, fault-tolerant applications (such as WordPress and Joomla) on the AWS cloud
- Anyone interested in gaining the AWS Security Specialty Certification
- Anyone wishing to enhance deep security knowledge related to AWS

Pre-Requisite

AWS Certified Solutions Architect- Associate is a basic level exam, and there is no prerequisite for it, but it is suggested to have:

- Basic IT technical knowledge
- Basic understanding of IT services and their usefulness in the AWS Cloud platform
- A minimum of six months of experience with the AWS Cloud in any role, including technical, managerial, sales, purchasing, or financial, is beneficial.
- Preferably 2+ years of experience in AWS Cloud Platform
- Understanding of basic security concepts and practices
- Security controls for workloads on AWS
- Skillset measuring to any AWS Associate level Certification (Certification not mandatory)

Exam Information

Since this is a combo course, there will be two different exams for AWS Certified Solutions Architect- Associate and AWS Certified Security – Specialty. Both the exams follow the pattern of Multiple-Choice Questions.

To achieve the highly valued credentials of the AWS Combo course, you need to pass the following exams:

Certification Name	AWS Certified Solutions Architect - Associate (AWS SAA-C03)
Number of Questions	65
Test Duration	130 minutes

Certification Name	Security-Speciality (SCS-C01)
Number of Questions	65
Test Duration	170 minutes

Why Infosec Train?

INFOSECTRAIN

- Certified & Experienced Instructor
- Flexible Schedule
- Access to the recorded sessions
- Post Training Support
- Tailor Made Training
- 4 hrs/day in Weekend/ Weekday

Our Expert Instructors

"

Krish is a senior technical consultant and passionate trainer. He has more than 15 years of experience in various IT domains including Cloud Computing, Security, Linux & Infrastructure Design. He has trained almost 400+ professionals worldwide on various IT domains.

KRISH

CCSP | CCSK | AWS-Sec | AWS CSA-P | MCT | Azure Sec | CEH | MCTS

"

As a Head of Security Testing, Abhi is an enthusiastic professional and an excellent trainer. He is unique with his skills of handling the security of the company's digital assets from unauthorised access.

ABHI

CCSP I CISSP I CCSK I AWS security specialty I Azure security I OSWP I OSCP

INFOSECTRAIN

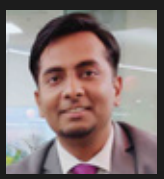
HAPPY LEARNERS FROM THE WORLD

Kennedy
AWS Combo | USA

Great session. The trainer has excellent knowledge and went above and beyond of typical training session to make sure that all attendees understand the topics very well. Trainer also provided really valuable guidelines and those are industry best practices.

VARUN N
AWS Combo | India

I really enjoyed the training. This is my second training with Infosectrain first one was CISSP. Krish is really helpful throughout. The best part is it is not limited to only certification but more focussed on learning the concepts which I am sure would help me in my organization. Looking forward to have longer association with Infosectrain.



Prince kumar
AWS Combo | India

The course was presented in an enthusiastic way, this has more than met my expectations, A wonderfully practical course.

Govinda Agrawal
AWS Combo | India

Having great experience with Infosec Train training team, Team provides hands on experience and support if required during the Lab's.

AWS CERTIFIED SECURITY - SPECIALTY (SCS-C01)

Domain 1: Incident Response

1.1 Given an AWS abuse notice, evaluate the suspected compromised instance or exposed access keys. 1.2Verify that the Incident Response plan includes relevant AWS services.

1.3 Evaluate the configuration of automated alerting, and execute possible remediation of security-related incidents and emerging issues.

Domain 2: Logging and Monitoring

2.1 Design and implement security monitoring and alerting.

2.2 Troubleshoot security monitoring and alerting.

2.3 Design and implement a logging solution.

2.4 Troubleshoot logging solutions.

Domain 3: Infrastructure Security

3.1 Design edge security on AWS.

3.2 Design and implement a secure network infrastructure.

3.3 Troubleshoot a secure network infrastructure.

3.4 Design and implement host-based security.

Domain 4: Identity and Access Management

4.1 Design and implement a scalable authorization and authentication system to access AWS resources.

4.2 Troubleshoot an authorization and authentication system to access AWS resources.

Domain 5: Data Protection

5.1 Design and implement key management and use.

5.2 Troubleshoot key management.

5.3 Design and implement a data encryption solution for data at rest and data in transit.

INFOSECTRAIN

DETAILED TRAINING SCHEDULE

Introduction to Cloud Computing

- Introduction to Cloud Computing
- Traditional vs. Cloud
- Cloud Service Models (IAAS, PAAS, SAAS)
- Cloud Deployment Models (Public, Private, Hybrid, Community)
- Scaling & Types
- Cloud Computing Issues
- Costing Model

Virtualization Concepts

- Virtualization and cloud computing
- Types of virtualization
- Virtualization terminologies
- Hypervisor, types & features

Cloud Security Fundamentals

- Cloud Security fundamentals & Challenges
- Shared responsibility model
- Multi tenancy and other security risk factors
- Risk assessment & Incident response
- AWS Security and Shared responsibility model

Architectural Concepts & Design Requirements

- Cloud computing concepts & definitions based on the ISO/IEC 17788 standard
- Understand Cloud Computing Concepts
- Cloud Reference Architecture
- Security Concepts Relevant to Cloud Computing
- Design Principles of Secure Cloud Computing
- Identify Trusted Cloud Services
- SLA, Legal and compliance
- Cloud Interoperability Issues
- Migration process

Amazon Web Services (AWS)

- Introduction to AWS Cloud Platform
- Benefits of choosing AWS comparison with other CSPs.
- Global infrastructure, Regions & Availability Zones
- Signing up for AWS
- AWS Free usage tier & support plans

EC2 Instances

- Introduction to creating scalable instances using AWS EC2
- Instances & Types
- Instance purchasing options
- Amazon Machine Images (AMI)
- Instance store & EBS Volumes
- Managing Volumes, adding additional volumes, modifying the root volume
- Troubleshooting issues with volumes, snapshots and AMIs
- Launching your first AWS Windows Server & Linux Instances
- Setting up security
- Firewall & Security Groups
- Choosing & Creating custom AMIs
- Snapshots & Recovery, snapshot scheduling
- Usage reports & limits
- Creating a new AMI
- Deploying a new instance from the custom AMI
- Elastic IP, BYOIP
- Key Pairs
- Load balancing concepts
- Creating an ALB web server
- Auto Scaling
- Troubleshooting Issues

AWS Command Line Interface (CLI)

- Introduction to AWS CLI
- Installation
- Connecting to your AWS account via CLI
- Other functionalities with CLI

Light Sail

- Difference between EC2 & LightSail
- creating a instance & connecting to it
- Snapshots
- DNS records
- Elastic IPs
- Generating default key pair
- Troubleshooting

Elastic Beanstalk

- Fundamentals
- Comparison with EC2, Lightsail & Elastic Beanstalk
- Hosting a sample application in EB
- Common issues & troubleshooting

Overview of Other Compute Services

- ECS (Elastic Container Service)
- EKS (Amazon Elastic Container Service for Kubernetes)
- Lambda

Storage

- Introduction to storage
- AWS Storage Tiers
- Use cases

Simple Storage Service (AWS S3)

- Buckets & Objects
- Encryption, Logging
- S3 durability and redundancy
- S3 Permissions
- Hosting a static website in AWS S3
- Access Control Lists & Bucket Policies
- S3 Object Versioning
- S3 Lifecycle Policies
- Cross Region Replication
- EC2-S3 Integration
- S3 Storage tiers (IT, IA, One-Zone IA, RRS, Glacier, Glacier Deep Archive)
- S3 storage class analysis

Instance Store & Elastic Block Storage (EBS) Volumes

- Difference & features
- Use cases & capacity limits
- Creating & Managing EBS volumes
- Delete EBS Volumes
- Attach, detach & extend EBS volumes
- Mounting and unmounting EBS volume
- Termination protection
- Troubleshooting & recovery

Elastic File System (EFS)

- Concepts of Network File System (NFS)
- Creating an EFS storage
- Difference between EFS and other storage options
- Mounting EFS
- Troubleshooting issues regarding permissions

Overview of Other Storage Services

- AWS FSx
- AWS Storage Gateway

AWS Database Services

Relational Database Service (RDS)

- Selecting the Database type
- Configuring & creating the database
- DB Security groups
- Snapshots
- Recovering a DB instance from snapshot
- Configuring backups
- Connecting to the database
- Read Replicas

Dynamo DB

- Creating a dynamo DB
- Advantages of using DynamoDB
- Configuring alarms
- Connecting to Dynamo DB

Other DB Services Overview

- Elasticache
- Neptune
- Redshift

Migration & Transfer

- AWS Server Migration Service
- AWS Database Migration Service
- Best Practices & Challenges

Identity access management (IAM)

- IAM introduction
- Importance of IAM
- Creating & managing Users and Groups
- Credentials (MFA, Passwords, Access Keys & Secret Keys)
- IAM policies (Types, Custom policies)
- Password Policy
- Roles
- Configure role to connect an EC2 to S3

AWS Organizations

- Importance of creating and managing multiple accounts in a corporate scenario
- Creating an organization
- Adding OUs
- Billing & management

Cloud Watch

- Cloud watch dashboard
- Configuring Monitoring services
- Setting thresholds
- Configuring actions
- Creating a cloud watch alarm
- Getting statistics for ec2 instances
- Monitoring other AWS services
- Configuring Notifications
- Integrating cloud watch with Auto scaling

CloudTrail

- Introduction to Logging
- Creating a trail
- Event History
- Pushing CloudTrail logs to S3 bucket

Cloud Front

- Use of cloud front
- Creating a cloud front distribution
- Hosting a website of cloud front distribution
- Invalidations

AWS Route53

- DNS Concepts and Working
- Configuring record set
- Configuring DNS with web servers & CDN
- Routing Tables
- Troubleshooting

Other Management & Governance Services

Incidence Response

- Incidence response in cloud
- Phases of IR
- AWS EC2 Abuse Notice
- Dealing with exposed credentials
- Compromised EC2 Instances
- AWS Guard Duty
- Penetration testing in AWS
- Preauthorized Scanning Tools

Logging and Monitoring

- Continuous Security Monitoring
- Vulnerability Assessment
- AWS Inspector
- Inspector Assessment Targets
- EC2 Systems Manager
- Run command, Patch Compliance, Patch manager
- AWS Config
- Configuring AWS Config with rules
- CloudWatch
- Trusted Advisor
- AWS Macie
- S3 Event notifications
- VPC Flow logs

Infrastructure Security

- AWS Organizations
- Managing Organizational Units
- Cloud Front security & logging
- AWS Virtual Private Cloud (VPC)
- Subnets, Public & Private

- Security Groups and NACLs
- Internet Gateway, NAT instance & gateway
- Routers & routing tables
- VPC security
- Network segmentation
- Bastion Hosts / Jump Servers
- VPC Peering & Inter VPC Communication
- VPN, Gateways, Endpoints
- IDS & IPS on Cloud
- Web Application Firewall (WAF)
- AWS Shield
- API Gateway
- EC2 Tenancy
- Lambda fundamentals

Identity & Access Management

- IAM policies (Identity based; Resource based)
- Understanding the principle for least privilege
- Overview of JSON policies & policy elements
- Troubleshooting conflicting policies
- Delegation
- Temporary security Credentials
- Federation, SSO
- AWS Cognito fundamentals
- AWS Directory services
- S3 Security
- S3 Pre signed URLs
- Versioning
- MFA Delete

Data Protection

- Cryptography fundamentals
- Hardware security module (HSM)
- AWS Key Management Service (KMS)
- Implementing KMS
- Key administrators & key users

- Using CMK with custom key materials
- Envelope encryption
- KMS authentication and access control
- Cloud Trail logs and encryption
- EBS Encryption
- S3 Encryption
- AWS Certificate manager
- AWS Secrets manager
- Database security
- Docker fundamentals and basics of container security
- Discussion and Wrap-up

AWS Architect – Associate (SAA-C03)

> Cloud Computing Concepts
> Virtualization Concepts

Compute and Serverless:

> Amazon EC2
> AWS Elastic Beanstalk
> AWS Lambda

Other Compute Services for review

> AWS Outposts
> VMware Cloud on AWS
> AWS Fargate

Storage

> AWS Simple Storage Service (S3)
> AWS S3 Glacier
> AWS Elastic Block Store (Amazon EBS)
> AWS Elastic File System (Amazon EFS)
> AWS FSx
> AWS Storage Gateway
> AWS Backup

Database

> AWS DynamoDB
> AWS RDS
> AWS Aurora
> AWS Elasticache

Other DB Services for Review

> AWS DocumentDB
> AWS Aurora Serverless
> AWS Keyspaces for Apache Cassandra
> AWS Redshift

Containers

> Containerization Concepts and setup
> AWS Elastic Container Registry (ECR)
> AWS Elastic Container Service (ECS)

Networking and Content Delivery

> AWS CloudFront
> AWS Global Accelerator
> AWS Route 53
> AWS VPC

Other Networking and Content Delivery Topics for review

> AWS API Gateway
> AWS Direct Connect
> AWS Private Link
> AWS Transit Gateway

Security, Identity, and Compliance

> AWS Identity and Access Management (IAM)
> AWS License Manager
> AWS Certificate Manager (ACM)
> AWS Directory Service
> AWS GuardDuty
> AWS Inspector
> AWS Key Management Service (AWS KMS)
> AWS Macie
> AWS Secrets Manager
> AWS WAF & Shield
> AWS Single Sign-On
> AWS Artifact
> AWS Audit Manager
> AWS Cloud HSM and KMS
> AWS Cognito
> AWS RAM
> AWS Detective

Migration and Transfer Overview

> AWS Database Migration Service (AWS DMS)
> AWS Server Migration Service (AWS SMS)

WS Snow Family
AWS DataSync
AWS Application Migration Service
AWS Migration Hub
AWS Transfer Family

AWS Billing and Cost Management

> AWS Budgets
> Cost Explorer
> AWS Cost and Usage Report
> Savings Plans

Analytics

> Amazon Athena
> AWS Kinesis
> AWS Glue

Other Application Integration Services for Review

> Amazon Elasticsearch

Application Integration

> AWS Simple Notification Service (Amazon SNS)
> AWS Simple Queue Service (Amazon SQS)
> AWS EventBridge (Amazon CloudWatch Events)

Management and Governance

> AWS CloudFormation
> AWS CloudTrail
> AWS CloudWatch
> AWS CLI
> AWS Config
> AWS Organizations
> AWS Personal Health Dashboard
> AWS Systems Manager
> AWS Trusted Advisor

Other Management and Governance Services for review

> AWS Compute Optimizer
> AWS Control Tower
> AWS License Manager
> AWS Service Catalog
> AWS Well-Architected Tool

Media Services Review

> Amazon Elastic Transcoder
> Amazon Kinesis Video Streams

Developer Tools

> AWS X-Ray

Front-End Web and Mobile Service Overview

> AWS Amplify
> Amazon API Gateway

www.infosectrain.com | sales@infosectrain.com