

AWS SECURITY ESSENTIALS

AWS-SE

Duration: 1 day; Instructor-led (ILT) | Virtual Instructor-led Training (VILT)

OVERVIEW

AWS Security Essentials covers fundamental AWS cloud security concepts, including AWS access control, data encryption methods, and how network access to your AWS infrastructure can be secured. Based on the AWS Shared Security Model, you learn where you are responsible for implementing security in the AWS Cloud and what security-oriented services are available to you and why and how the security services can help meet the security needs of your organization. This course enables you to dive deep, ask questions, work through solutions, and get feedback from AWS accredited instructors with deep technical knowledge. This is a fundamental level course and is a part of the AWS Security learning path.

- Course level: Fundamental

AUDIENCE

This course is intended for:

- IT business-level professionals interested in cloud security practices
- Security professionals with minimal working knowledge of AWS

PREREQUISITES

We recommend that attendees of this course have:

- Working knowledge of IT security practices and infrastructure concepts, familiarity with cloud computing concepts

METHODOLOGY

This course includes presentations, class activities, and knowledge checks.

COURSE OBJECTIVES

In this course, you will:

- Identify security benefits and responsibilities when using the AWS Cloud
- Describe the access control and management features of AWS
- Understand the different data encryption methods to secure sensitive data
- Describe how to secure network access to your AWS resources
- Determine which AWS services can be used for security logging and monitoring

COURSE CONTENTS

Module 1: Security on AWS

- Security design principles in the AWS Cloud
- AWS Shared Responsibility Model

Module 2: Security OF the Cloud

- AWS Global Infrastructure
- Data Center Security
- Compliance and Governance

Module 3: Security IN the Cloud – Part 1

- Identity and Access Management
- Data Protection
- Lab 01 – Introduction to Security Policies

Module 4: Security IN the Cloud – Part 2

- Securing your infrastructure
- Monitoring and detective controls
- Lab 02 – Securing VPC Resources with Security Groups

Module 5: Security IN the Cloud – Part 3

- DDoS mitigation
- Incident response essentials
- Lab 03 – Automating Incident Response with AWS Config and AWS Lambda

Module 6: Course Wrap Up

- AWS Well-Architected tool overview