

**AWS Security Best Practices**

**Course Number:** AWS-174  
**Duration:** 1 day

**Overview**

AWS Security Best Practices training is essential for anyone who wants to ensure their organization’s data is kept safe and secure on the AWS platform. Participants learn how to protect their AWS accounts and keep user data safe from malicious attacks by using AWS's security features to implement proper protective measures before threats emerge.

Accelebrate is an AWS Training Partner (ATP) and this hands-on official AWS Classroom Training course is taught by an accredited Amazon Authorized Instructor (AAI).

**Prerequisites**

All students must have taken [AWS Security Fundamentals](https://explore.skillbuilder.aws/learn/course/external/view/elearning/48/aws-security-fundamentals) (a self-paced course from AWS) and [AWS Security Essentials](file:////training/aws-security-essentials).

**Materials**

All Security in AWS training students will receive comprehensive courseware.

**Software Needed on Each Student PC**

A modern web browser and an Internet connection free of restrictive firewalls, so that the student can connect by SSH or Remote Desktop (RDP) into AWS virtual machines.

**Objectives**

All students will learn how to design and implement:

* A secure network infrastructure
* Compute security
* A logging solution

**Outline**

* Introduction
* AWS Security Overview
  + Shared responsibility model
  + Customer challenges
  + Frameworks and standards
  + Establishing best practices
  + Compliance in AWS
* Securing the Network
  + Flexible and secure
  + Security inside the Amazon Virtual Private Cloud (Amazon VPC)
  + Security services
  + Third-party security solutions
  + Controlling the Network
    - Create a three-security zone network infrastructure
    - Implement network segmentation using security groups, Network Access Control Lists (NACLs)
    - and public and private subnets
    - Monitor network traffic to Amazon Elastic Compute Cloud (EC2) instances using VPC flow logs
* Amazon EC2 Security
  + Compute hardening
  + Amazon Elastic Block Store (EBS) encryption
  + Secure management and maintenance
  + Detecting vulnerabilities
  + Using AWS Marketplace
  + Securing the starting point (EC2)
    - Create a custom Amazon Machine Image (AMI).
    - Deploy a new EC2 instance from a custom AMI.
    - Patch an EC2 instance using AWS Systems Manager.
    - Encrypt an EBS volume.
    - Understand how EBS encryption works and how it impacts other operations.
    - Use security groups to limit traffic between EC2 instances to only that which is encrypted
* Monitoring and Alerting
  + Logging network traffic
  + Logging user and Application Programming Interface (API) traffic
  + Visibility with Amazon CloudWatch
  + Enhancing monitoring and alerting
  + Verifying your AWS environment
  + Security Monitoring
    - Configure an Amazon Linux 2 instance to send log files to Amazon CloudWatch
    - Create Amazon CloudWatch alarms and notifications to monitor for failed login attempts
    - Create Amazon CloudWatch alarms to monitor network traffic through a Network Address
    - Translation (NAT) gateway
* Conclusion