**Course Duration:** 8 hours (1 Day)

# Zero Trust Architectures on AWS

This course provides a comprehensive understanding of **Zero Trust Architecture (ZTA) principles** and their implementation within **AWS environments**. It covers the fundamental security model of "never trust, always verify" and how AWS services and best practices can be used to enforce Zero Trust policies. The course includes hands-on labs, real-world use cases, and architectural patterns to help participants design and deploy secure cloud workloads using Zero Trust principles.

## Course objectives

By the end of this course, participants will be able to:

- Understand the core principles of Zero Trust and its necessity in modern cloud security.
- Design and implement Zero Trust security architectures using AWS services.
- Utilize AWS Identity and Access Management (IAM), AWS Verified Access, AWS PrivateLink, and other AWS security tools.
- Apply network segmentation, identity-based policies, and continuous authentication.
- Secure applications and data while minimizing the attack surface.
- Monitor and automate security policies to enforce Zero Trust principles.

## Prerequisites

- Completed AWS Cloud Practitioner Essentials, or AWS Technical Essentials, and Security Engineering on AWS.
- Familiarity with the **Linux command line** and basic terminal commands
- Familiarity with cloud computing concepts

## Target Audience

- Cloud Security Engineers
- Solutions Architects
- DevSecOps Engineers
- Security Analysts
- IT Managers and Compliance Officers

- Anyone responsible for securing cloud environments using Zero Trust principles

## Course outline

**Module 1: Introduction to Zero Trust**

- What is Zero Trust?
- Why is it necessary in cloud environments?
- Key Zero Trust principles
- Differences between traditional security and Zero Trust

**Module 2: AWS Security Services for Zero Trust**

- Overview of AWS security services
- AWS Identity and Access Management (IAM)
- AWS Organizations and Service Control Policies (SCPs)
- AWS Verified Access

**Module 3: Identity and Access Management in Zero Trust**

- Identity as the new perimeter
- Implementing least privilege access using AWS IAM
- AWS IAM Policies, Roles, and Permissions Boundaries
- AWS Cognito for identity federation

**Lab 1: Implementing IAM Zero Trust Policies**

**Module 4: Network Security and Zero Trust Implementation**

- AWS PrivateLink and VPC Endpoints for secure communications
- Network segmentation and micro-segmentation with AWS Security Groups and Network ACLs

**Module 5: Data Protection and Zero Trust**

- AWS Key Management Service (KMS) for encryption
- Amazon Macie for sensitive data detection
- AWS Secrets Manager for credentials security

- Zero Trust for S3 buckets and AWS data stores

**Module 6: Monitoring, Logging, and Automation**

- AWS Security Hub and AWS Config for continuous compliance
- AWS CloudTrail and Amazon GuardDuty for security monitoring
- Automating security policies with AWS Lambda and AWS Step Functions

**Lab 2: Automating Security Enforcement Using AWS Lambda**

**Module 7: Best Practices and Next Steps**

- Zero Trust adoption roadmap for AWS
- Common pitfalls and how to avoid them
- Compliance and regulatory considerations