

# AWS Essentials - Security

Duration: 1 day

Audience: Professionnel TI

## Who is this training for?

- IT professionals interested in cloud security practices
- Security professionals with little working knowledge of AWS

## Training objectives

- Identify the security benefits and responsibilities of using the AWS Cloud
- Describe the built-in access management and control capabilities of AWS
- Understand data encryption methods to protect sensitive data
- Explain how to secure network access to your AWS resources

## Summary

AWS Essentials - Security covers the fundamental security concepts of the AWS Cloud, 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, this course covers implementing security on the AWS Cloud. You'll also learn about the security services available and see how and why they can help you meet your company's security needs. This course allows you to dive deeper, ask questions, find solutions, and get feedback from AWS-accredited instructors with deep technical knowledge. This foundation-level course is part of the AWS Training and Certification Security learning path.

## Course outline

### Module: Security on AWS

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

### Module: Security OF the Cloud

-

AWS Global Infrastructure

- Data Center Security
- Compliance and Governance

### **Module: Security in the Cloud - Part 1**

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

### **Module: Security in the Cloud - Part 2**

- Securing Your Infrastructure
- Monitoring and Detection Controls
- Lab - Securing VPC Resources with Security Groups

### **Module: Security in the Cloud - Part 3**

- Mitigating DDoS Attacks
- Incident Response Essentials
- Hands-on - Automating Incident Response with AWS Config and AWS Lambda

### **Module: Course Recap**

- Introduction to the AWS Well-Architected Tool

## **Approach and methodology**

The training is based on a structured approach combining theoretical presentations, demonstrations and practical work in an AWS environment. It allows participants to apply safety concepts through guided labs and hands-on exercises. The facilitator accompanies the learning by providing technical explanations and answering questions from practical cases.

## **Prerequisites**

Master the concepts of cloud computing

## **Recommendations**

- Familiarity with IT security practices and infrastructure concepts
- Have an interest in cybersecurity and cloud security
- Understand issues related to data and access protection Be involved in IT, cloud or security projects
- Have a general understanding of identity or access management (asset) • Experience in systems administration, Networks or Cloud (asset)