

€ TRAINING

Principles of Cloud Management and
Security





Principles of Cloud Management and Security

Introduction:

The Principles of Cloud Management and Security training program covers essential practices for effectively managing and securing cloud infrastructures. Participants learn to deploy, maintain, and protect cloud environments through practical exercises and theoretical instruction. Gain skills to ensure efficient and secure operations in the cloud.

Program Objectives:

At the end of this program the participants will be able to:

- Recognize the benefits of cloud computing and common misconceptions, as well as its drawbacks.
- Describe the structure, attributes, and management services of clouds and make a plan for implementing the cloud.
- Describe the primary criteria to transition from the present cloud's unreliable architecture to a reliable internet-scale cloud computing infrastructure.
- Examine the main dangers connected to the various cloud services and deployment models.
- Discuss the key tenets, methods, and recommended procedures for handling cloud risks.
- Showcase the principles covered utilizing real-world examples, business simulations, and industrial instruments.

Targeted Audience:

- Leaders in IT and infrastructure.
- CxOs, risk analysts.
- Strategic planners.
- Architects.
- Administrators.
- Software developers.
- Project managers are all needed.

Program Outline:

Unit1:

A cloud overview:

- Defined clouds, common misconceptions, and their evolution.
- Services and deployment styles in the cloud.
- Challenges.

Unit2:

Cloud administration:

- Structure and characteristics of clouds.
- Services for managing the application and virtual layers.
- Challenges posed by the dynamic nature of clouds.
- Integration and development of applications for clouds.
- Automating cloud infrastructure management security recommended practices.
- Using commercial channels to make the principles clear.

Unit3:

Establishing trust in clouds

- Defining cloud trustworthiness.
- Assessing cloud trustworthiness.
- Establishing trust in: Private, Hybrid and Public cloud deployment types.
- Establishing trust in: IaaS, PaaS and SaaS.
- Clarifying the concepts using openstack management platform.

Unit4:

Identification and access control:

- Authentication, Authorization and Access control.
- Managed federated access.
- Attackers versus insiders.

- Analysis and management by insiders.
- Associated industrial equipment
- Insider cloud treatments and Strong cloud authentication.

Unit5:

Cloud provenance:

- Definition and characteristics and difficulties encountered.
- Using provenance to reduce security risks.
- Case studies for applying provenance.
- forensic analysis and Bill assurance.
- reliable operational management.
- proactive and anticipatory management.