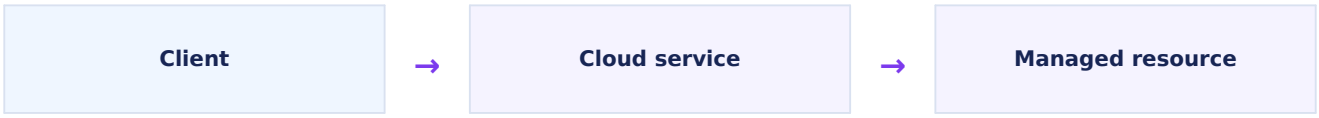
LEARNHUB / TECHNICAL COURSE LIBRARY

Cloud Computing

Revision summary

Understand how cloud platforms deliver compute, storage, networking, and managed services, and how teams choose an architecture that balances reliability and cost.



Level: Beginner · Category: Networking

Original, beginner-friendly study content designed to accompany the course syllabus and its linked video lesson.

Contents

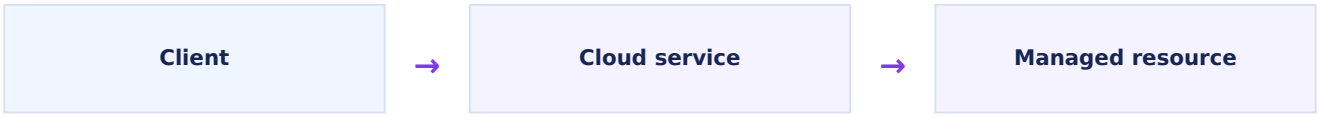
- How to use this resource
- Learning map
- Chapter 01 · Cloud concepts and deployment models
- Chapter 02 · Service models: IaaS, PaaS, and SaaS
- Chapter 03 · Compute, storage, and containers
- Chapter 04 · Networking, identity, and shared responsibility
- Chapter 05 · Architecture, resilience, and cost
- Summary and next steps

Course purpose: Understand how cloud platforms deliver compute, storage, networking, and managed services, and how teams choose an architecture that balances reliability and cost.

How to use this resource

Read the chapter titles first, then study the explanations and examples. Pause at each practice prompt before reading its suggested answer. Write down questions that remain and revisit them during revision.

Learning map



Chapter 01 · Cloud concepts and deployment models

Remember this definition

Cloud computing provides on-demand access to configurable computing resources over a network. Deployment models describe who owns or shares the underlying environment.

Key takeaway

Public clouds serve multiple customers on shared infrastructure; private clouds are dedicated to one organization; hybrid designs connect environments. Choose based on requirements for control, regulation, latency, and operations rather than labels alone.

Anchor example

A retailer keeps a regulated legacy system in a private environment but sends public product images through a public cloud content service.

Recall question

Compare public, private, and hybrid deployment for a small startup with no existing data center.

Self-check

A public cloud is often a practical starting point because it avoids building physical infrastructure. Revisit the choice as regulatory, cost, and control requirements become clear.

Chapter 02 · Service models: IaaS, PaaS, and SaaS

Remember this definition

Infrastructure as a Service offers virtualized infrastructure; Platform as a Service manages more of the application runtime; Software as a Service delivers a complete application.

Key takeaway

As service abstraction rises, the provider manages more of the stack and the customer usually has less infrastructure control. Responsibility does not disappear: customers still configure access, data, and appropriate workloads.

Anchor example

A team can rent virtual machines (IaaS), deploy code to a managed application platform (PaaS), or use a hosted email suite (SaaS).

Recall question

Classify a hosted document editor and a rented virtual machine by service model.

Self-check

> The hosted editor is SaaS because the user consumes a complete application. A rented VM is IaaS because the customer controls the guest operating system and workload.

Chapter 03 · Compute, storage, and containers

Remember this definition

Cloud compute executes workloads; object, block, and file storage expose different data access patterns. A container packages an application and its dependencies into a portable unit.

Key takeaway

Use object storage for unstructured files, block storage for disk-like access, and managed databases for structured queries. Containers improve packaging but still require decisions about image security, resource limits, and orchestration.

Anchor example

A media service stores uploaded images in object storage and keeps searchable ownership and metadata in a database.

Recall question

Choose a storage type for downloadable course PDFs and explain how to preserve their public paths.

Self-check

Object storage is suited to static documents. Keep stable object identifiers and control public access; store descriptive metadata separately if search or access rules require it.

Chapter 04 · Networking, identity, and shared responsibility

Remember this definition

Cloud networking connects services through virtual networks, routes, and security rules. The shared-responsibility model divides security tasks between provider and customer.

Key takeaway

Use identity roles rather than shared administrator keys, restrict inbound traffic, protect secrets, and log sensitive changes. The exact boundary varies by service model; managed services do not automatically guarantee secure customer configuration.

Anchor example

A public web front end reaches a private database only through an approved network path and a narrowly scoped service identity.

Recall question

Name two controls the cloud provider may handle and two the application team must still manage.

Self-check

The provider secures physical data centers and the underlying managed infrastructure. The team must still configure identity, data permissions, software, and network exposure for its chosen service.

Chapter 05 · Architecture, resilience, and cost

Remember this definition

A resilient system continues or recovers when components fail. Cloud cost is driven by provisioned resources, requests, storage, and data transfer.

Key takeaway

Design for failure with backups, health checks, and tested recovery steps. Scale only where demand requires it, set budgets or alerts, and shut down unused development resources. Measure user-facing reliability as well as infrastructure health.

Anchor example

A learning service stores PDFs durably, serves them through a cache, and keeps a tested source copy so a deployment can be rebuilt after a failure.

Recall question

Suggest a recovery and cost-control measure for a development environment used only on weekdays.

Self-check

Use backups or infrastructure definitions for recovery, and stop or scale down idle resources outside working hours. Confirm that shutdown will not delete durable data.

Summary and next steps

Cloud Computing brings together 5 connected topics. Review each definition, explain one example without looking, and then try the practice prompt again.

Key ideas to carry forward

Cloud concepts and deployment models: Cloud computing provides on-demand access to configurable computing resources over a network. Deployment models describe who owns or shares the underlying environment.

Service models: IaaS, PaaS, and SaaS: Infrastructure as a Service offers virtualized infrastructure; Platform as a Service manages more of the application runtime; Software as a Service delivers a complete application.

Compute, storage, and containers: Cloud compute executes workloads; object, block, and file storage expose different data access patterns. A container packages an application and its dependencies into a portable unit.

Networking, identity, and shared responsibility: Cloud networking connects services through virtual networks, routes, and security rules. The shared-responsibility model divides security tasks between provider and customer.

Architecture, resilience, and cost: A resilient system continues or recovers when components fail. Cloud cost is driven by provisioned resources, requests, storage, and data transfer.

A short review routine

1. Recall the main idea from each chapter before rereading. 2. Work one example by hand. 3. Explain a common mistake and how you would catch it. 4. Revisit a difficult topic after a short break.

Course outcomes

- Explain cloud computing and its service/deployment models
- Compare compute, storage, and managed platform choices
- Describe cloud networking and shared-responsibility security
- Identify basic resilience and cost controls

This revision summary is an original LearnHub learning aid. Use the referenced ideas for study, then consult the course video and the rest of the library for additional practice.