ONE PAGE SUMMARY

IT & Software › Microservices › Security in Microservices

Introduction to Security in Microservices

Secure your microservices to protect data and maintain trust.

DEFINITION

> Security in microservices involves protecting applications that are built as a collection of independent services. It ensures that data is safe and services communicate securely.

KEY CONCEPTS

Authentication

Verifying the identity of users or services before granting access.

Authorization

Determining what authenticated users or services are allowed to do.

Data Encryption

Converting data into a secure format to prevent unauthorized access.

Service Mesh

An infrastructure layer that manages service-to-service communication and security.

API Gateway

A single entry point for managing and securing access to microservices.

EXAMPLES

→ Using OAuth for user authentication in a microservice.

→ Implementing TLS for secure data transmission between services.

→ Configuring an API gateway to enforce security policies.

MEMORY TIPS

★ Remember 'AAA' for Authentication, Authorization, and Accounting.

★ Think 'Encrypt to Protect' for data security.

★ Use 'Mesh for Security' to recall service mesh benefits.

COMMON MISTAKES

✗ Neglecting to secure inter-service communication.

✗ Overlooking regular security audits and updates.

✗ Confusing authentication with authorization.

QUICK RECAP

Security in microservices is crucial for protecting data and ensuring safe communication. Focus on authentication, authorization, and encryption to secure your services effectively.