

THE PEARSON DIGITAL ENTERPRISE SERIES FROM THOMAS ERL 

Foreword by **David Linthicum**

SECOND EDITION

Cloud Computing

Concepts, Technology, Security & Architecture



by Top-Selling Author **Thomas Erl**
with Eric Barceló Monroy

with contributions from Professor Zaigham Mahmood and Dr. Ricardo Puttini



human



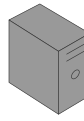
administrator



manager



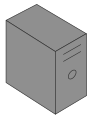
attacker



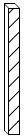
physical
server



virtual
server



server
(attacker)



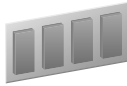
physical
firewall



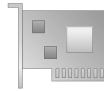
virtual
firewall



CPU



memory



network
adapter



physical
network



virtual
network



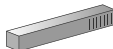
VI manager



hypervisor



virtualization
platform



physical
network
device



virtual
network
device



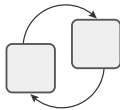
connection ports
or virtual switch



container



internal container
logic



container
cluster



container
engine



container
image



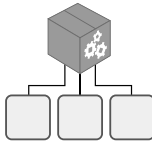
container image
layers



package



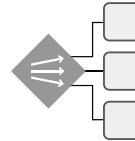
image
registry



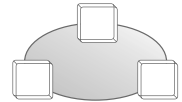
container package
manager



package
repository



deployment
optimizer



container
network



router



core switch



top-of-rack
switch



container
build file



schema or
data model



policy



general machine
processable
document



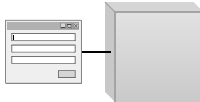
human
readable
document



ready-made
environment



management
system



remote administration
system



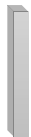
actively
processing



software program
or application



product, system
or application



agent or
intermediary

Cloud Computing: Concepts, Technology, Security, and Architecture

Table of Contents

Cover

Title Page

Copyright Page

Contents at a Glance

Contents

Foreword

About the Authors

Acknowledgments

Chapter 1: Introduction

1.1 Objectives of This Book

1.2 What This Book Does Not Cover

1.3 Who This Book Is For

1.4 How This Book Is Organized

Part I: Fundamental Cloud Computing

Chapter 3: Understanding Cloud Computing

Chapter 4: Fundamental Concepts and Models

Chapter 5: Cloud-Enabling Technology

Chapter 6: Understanding Containerization

Chapter 7: Understanding Cloud Security and Cybersecurity

Part II: Cloud Computing Mechanisms

Chapter 8: Cloud Infrastructure Mechanisms

Chapter 9: Specialized Cloud Mechanisms

Chapter 10: Cloud Security and Cybersecurity Access-Oriented Mechanisms

Table of Contents

Chapter 11: Cloud Security and Cybersecurity Data-Oriented Mechanisms

Chapter 12: Cloud Management Mechanisms

Part III: Cloud Computing Architecture

Chapter 13: Fundamental Cloud Architectures

Chapter 14: Advanced Cloud Architectures

Chapter 15: Specialized Cloud Architectures

Part IV: Working with Clouds

Chapter 16: Cloud Delivery Model Considerations

Chapter 17: Cost Metrics and Pricing Models

Chapter 18: Service Quality Metrics and SLAs

Part V: Appendices

Appendix A: Case Study Conclusions

Appendix B: Common Containerization Technologies

1.5 Resources

Pearson Digital Enterprise Book Series

Thomas Erl on YouTube

The Digital Enterprise Newsletter on LinkedIn

Cloud Certified Professional (CCP) Program

Chapter 2: Case Study Background

2.1 Case Study #1: ATN

Technical Infrastructure and Environment

Business Goals and New Strategy

Roadmap and Implementation Strategy

2.2 Case Study #2: DTGOV

Technical Infrastructure and Environment

Business Goals and New Strategy

Roadmap and Implementation Strategy

2.3 Case Study #3: Innovartus Technologies Inc

Technical Infrastructure and Environment

Business Goals and Strategy

Table of Contents

Roadmap and Implementation Strategy

PART I: FUNDAMENTAL CLOUD COMPUTING

Chapter 3: Understanding Cloud Computing

3.1 Origins and Influences

- A Brief History

- Definitions

- Business Drivers

 - Cost Reduction

 - Business Agility

- Technology Innovations

 - Clustering

 - Grid Computing

 - Capacity Planning

 - Virtualization

 - Containerization

 - Serverless Environments

3.2 Basic Concepts and Terminology

- Cloud

- Container

- IT Resource

- On Premises

- Cloud Consumers and Cloud Providers

- Scaling

 - Horizontal Scaling

 - Vertical Scaling

- Cloud Service

- Cloud Service Consumer

3.3 Goals and Benefits

- Increased Responsiveness

- Reduced Investments and Proportional Costs

- Increased Scalability

- Increased Availability and Reliability

3.4 Risks and Challenges

Table of Contents

Increased Vulnerability Due to Overlapping Trust Boundaries
Increased Vulnerability Due to Shared Security Responsibility
Increased Exposure to Cyber Threats
Reduced Operational Governance Control
Limited Portability Between Cloud Providers
Multiregional Compliance and Legal Issues
Cost Overruns

Chapter 4: Fundamental Concepts and Models

4.1 Roles and Boundaries

Cloud Provider
Cloud Consumer
Cloud Broker
Cloud Service Owner
Cloud Resource Administrator
Additional Roles
Organizational Boundary
Trust Boundary

4.2 Cloud Characteristics

On-Demand Usage
Ubiquitous Access
Multitenancy (and Resource Pooling)
Elasticity
Measured Usage
Resiliency

4.3 Cloud Delivery Models

Infrastructure as a Service (IaaS)
Platform as a Service (PaaS)
Software as a Service (SaaS)
Comparing Cloud Delivery Models
Combining Cloud Delivery Models
 IaaS + PaaS
 IaaS + PaaS + SaaS
Cloud Delivery Submodels

Table of Contents

4.4 Cloud Deployment Models

- Public Clouds
- Private Clouds
- Multiclouds
- Hybrid Clouds

Chapter 5: Cloud-Enabling Technology

5.1 Networks and Internet Architecture

- Internet Service Providers (ISPs)
- Connectionless Packet Switching (Datagram Networks)
- Router-Based Interconnectivity
 - Physical Network
 - Transport Layer Protocol
 - Application Layer Protocol
- Technical and Business Considerations
 - Connectivity Issues
 - Network Bandwidth and Latency Issues
 - Wireless and Cellular
 - Cloud Carrier and Cloud Provider Selection

5.2 Cloud Data Center Technology

- Virtualization
- Standardization and Modularity
- Autonomic Computing
- Remote Operation and Management
- High Availability
- Security-Aware Design, Operation, and Management
- Facilities
- Computing Hardware
- Storage Hardware
- Network Hardware
 - Carrier and External Networks Interconnection
 - Web-Tier Load Balancing and Acceleration
 - LAN Fabric
 - SAN Fabric
 - NAS Gateways
- Serverless Environments

Table of Contents

- NoSQL Clustering

- Other Considerations

5.3 Modern Virtualization

- Hardware Independence

- Server Consolidation

- Resource Replication

- Operating SystemBased Virtualization

- Hardware-Based Virtualization

- Containers and Application-Based Virtualization

- Virtualization Management

- Other Considerations

5.4 Multitenant Technology

5.5 Service Technology and Service APIs

- REST Services

- Web Services

- Service Agents

- Service Middleware

- Web-Based RPC

5.6 Case Study Example

Chapter 6: Understanding Containerization

6.1 Origins and Influences

- A Brief History

- Containerization and Cloud Computing

6.2 Fundamental Virtualization and Containerization

- Operating System Basics

- Virtualization Basics

- Physical Servers

- Virtual Servers

- Hypervisors

- Virtualization Types

- Containerization Basics

- Containers

- Container Images

Table of Contents

Container Engines

Pods

Hosts

Host Clusters

Host Networks and Overlay Networks

Virtualization and Containerization

Containerization on Physical Servers

Containerization on Virtual Servers

Containerization Benefits

Containerization Risks and Challenges

6.3 Understanding Containers

Container Hosting

Containers and Pods

Container Instances and Clusters

Container Package Management

Container Orchestration

Container Package Manager vs. Container Orchestrator

Container Networks

Container Network Scope

Container Network Addresses

Rich Containers

Other Common Container Characteristics

6.4 Understanding Container Images

Container Image Types and Roles

Container Image Immutability

Container Image Abstraction

Operating System Kernel Abstraction

Operating System Abstraction Beyond the Kernel

Container Build Files

Container Image Layers

How Customized Container Images Are Created

6.5 Multi-Container Types

Sidecar Container

Adapter Container

Ambassador Container

Table of Contents

Using Multi-Containers Together

6.6 Case Study Example

Chapter 7: Understanding Cloud Security and Cybersecurity

7.1 Basic Security Terminology

Confidentiality

Integrity

Availability

Authenticity

Security Controls

Security Mechanisms

Security Policies

7.2 Basic Threat Terminology

Risk

Vulnerability

Exploit

Zero-Day Vulnerability

Security Breach

Data Breach

Data Leak

Threat (or Cyber Threat)

Attack (or Cyber Attack)

Attacker and Intruder

Attack Vector and Surface

7.3 Threat Agents

Anonymous Attacker

Malicious Service Agent

Trusted Attacker

Malicious Insider

7.4 Common Threats

Traffic Eavesdropping

Malicious Intermediary

Denial of Service

Insufficient Authorization

Table of Contents

- Virtualization Attack
- Overlapping Trust Boundaries
- Containerization Attack
- Malware
- Insider Threat
- Social Engineering and Phishing
- Botnet
- Privilege Escalation
- Brute Force
- Remote Code Execution
- SQL Injection
- Tunneling
- Advanced Persistent Threat (APT)

7.5 Case Study Example

7.6 Additional Considerations

- Flawed Implementations
- Security Policy Disparity
- Contracts
- Risk Management

7.7 Case Study Example

PART II: CLOUD COMPUTING MECHANISMS

Chapter 8: Cloud Infrastructure Mechanisms

8.1 Logical Network Perimeter

- Case Study Example

8.2 Virtual Server

- Case Study Example

8.3 Hypervisor

- Case Study Example

8.4 Cloud Storage Device

- Cloud Storage Levels
- Network Storage Interfaces
- Object Storage Interfaces

Table of Contents

Database Storage Interfaces

Relational Data Storage

Non-Relational Data Storage

Case Study Example

8.5 Cloud Usage Monitor

Monitoring Agent

Resource Agent

Polling Agent

Case Study Example

8.6 Resource Replication

Case Study Example

8.7 Ready-Made Environment

Case Study Example

8.8 Container

Chapter 9: Specialized Cloud Mechanisms

9.1 Automated Scaling Listener

Case Study Example

9.2 Load Balancer

Case Study Example

9.3 SLA Monitor

Case Study Example

SLA Monitor Polling Agent

SLA Monitoring Agent

9.4 Pay-Per-Use Monitor

Case Study Example

9.5 Audit Monitor

Case Study Example

9.6 Failover System

ActiveActive

ActivePassive

Case Study Example

9.7 Resource Cluster

Table of Contents

Case Study Example

9.8 Multi-Device Broker

Case Study Example

9.9 State Management Database

Case Study Example

Chapter 10: Cloud Security and Cybersecurity Access-Oriented Mechanisms

10.1 Encryption

Symmetric Encryption

Asymmetric Encryption

Case Study Example

10.2 Hashing

Case Study Example

10.3 Digital Signature

Case Study Example

10.4 Cloud-Based Security Groups

Case Study Example

10.5 Public Key Infrastructure (PKI) System

Case Study Example

10.6 Single Sign-On (SSO) System

Case Study Example

10.7 Hardened Virtual Server Image

Case Study Example

10.8 Firewall

Case Study Example

10.9 Virtual Private Network (VPN)

Case Study Example

10.10 Biometric Scanner

Case Study Example

10.11 Multi-Factor Authentication (MFA) System

Case Study Example

Table of Contents

10.12 Identity and Access Management (IAM) System

Case Study Example

10.13 Intrusion Detection System (IDS)

Case Study Example

10.14 Penetration Testing Tool

Case Study Example

10.15 User Behavior Analytics (UBA) System

Case Study Example

10.16 Third-Party Software Update Utility

Case Study Example

10.17 Network Intrusion Monitor

Case Study Example

10.18 Authentication Log Monitor

Case Study Example

10.19 VPN Monitor

Case Study Example

10.20 Additional Cloud Security Access-Oriented Practices and Technologies

Chapter 11: Cloud Security and Cybersecurity Data-Oriented Mechanisms

11.1 Digital Virus Scanning and Decryption System

Generic Decryption

Digital Immune System

Case Study Example

11.2 Malicious Code Analysis System

Case Study Example

11.3 Data Loss Prevention (DLP) System

Case Study Example

11.4 Trusted Platform Module (TPM)

Case Study Example

11.5 Data Backup and Recovery System

Table of Contents

Case Study Example

11.6 Activity Log Monitor

Case Study Example

11.7 Traffic Monitor

Case Study Example

11.8 Data Loss Protection Monitor

Case Study Example

Chapter 12: Cloud Management Mechanisms

12.1 Remote Administration System

Case Study Example

12.2 Resource Management System

Case Study Example

12.3 SLA Management System

Case Study Example

12.4 Billing Management System

Case Study Example

PART III: CLOUD COMPUTING ARCHITECTURE

Chapter 13: Fundamental Cloud Architectures

13.1 Workload Distribution Architecture

13.2 Resource Pooling Architecture

13.3 Dynamic Scalability Architecture

13.4 Elastic Resource Capacity Architecture

13.5 Service Load Balancing Architecture

13.6 Cloud Bursting Architecture

13.7 Elastic Disk Provisioning Architecture

13.8 Redundant Storage Architecture

13.9 Multicloud Architecture

13.10 Case Study Example

Chapter 14: Advanced Cloud Architectures

14.1 Hypervisor Clustering Architecture

Table of Contents

- 14.2 Virtual Server Clustering Architecture
- 14.3 Load-Balanced Virtual Server Instances Architecture
- 14.4 Nondisruptive Service Relocation Architecture
- 14.5 Zero Downtime Architecture
- 14.6 Cloud Balancing Architecture
- 14.7 Resilient Disaster Recovery Architecture
- 14.8 Distributed Data Sovereignty Architecture
- 14.9 Resource Reservation Architecture
- 14.10 Dynamic Failure Detection and Recovery Architecture
- 14.11 Rapid Provisioning Architecture
- 14.12 Storage Workload Management Architecture
- 14.13 Virtual Private Cloud Architecture
- 14.14 Case Study Example

Chapter 15: Specialized Cloud Architectures

- 15.1 Direct I/O Access Architecture
- 15.2 Direct LUN Access Architecture
- 15.3 Dynamic Data Normalization Architecture
- 15.4 Elastic Network Capacity Architecture
- 15.5 Cross-Storage Device Vertical Tiering Architecture
- 15.6 Intra-Storage Device Vertical Data Tiering Architecture
- 15.7 Load-Balanced Virtual Switches Architecture
- 15.8 Multipath Resource Access Architecture
- 15.9 Persistent Virtual Network Configuration Architecture
- 15.10 Redundant Physical Connection for Virtual Servers Architecture
- 15.11 Storage Maintenance Window Architecture
- 15.12 Edge Computing Architecture
- 15.13 Fog Computing Architecture
- 15.14 Virtual Data Abstraction Architecture
- 15.15 Metacloud Architecture

Table of Contents

15.16 Federated Cloud Application Architecture

PART IV: WORKING WITH CLOUDS

Chapter 16: Cloud Delivery Model Considerations

16.1 Cloud Delivery Models: The Cloud Provider Perspective

Building IaaS Environments

Data Centers

Scalability and Reliability

Monitoring

Security

Equipping PaaS Environments

Scalability and Reliability

Monitoring

Security

Optimizing SaaS Environments

Security

16.2 Cloud Delivery Models: The Cloud Consumer Perspective

Working with IaaS Environments

IT Resource Provisioning Considerations

Working with PaaS Environments

IT Resource Provisioning Considerations

Working with SaaS Services

16.3 Case Study Example

Chapter 17: Cost Metrics and Pricing Models

17.1 Business Cost Metrics

Up-Front and Ongoing Costs

Additional Costs

Case Study Example

Product Catalog Browser

On-Premises Up-Front Costs

On-Premises Ongoing Costs

Cloud-Based Up-Front Costs

Cloud-Based Ongoing Costs

17.2 Cloud Usage Cost Metrics

Network Usage

Table of Contents

Inbound Network Usage Metric

Outbound Network Usage Metric

Intra-Cloud WAN Usage Metric

Server Usage

On-Demand Virtual Machine Instance Allocation Metric

Reserved Virtual Machine Instance Allocation Metric

Cloud Storage Device Usage

On-Demand Storage Space Allocation Metric

I/O Data Transferred Metric

Cloud Service Usage

Application Subscription Duration Metric

Number of Nominated Users Metric

Number of Transactions Users Metric

17.3 Cost Management Considerations

Pricing Models

Multicloud Cost Management

Additional Considerations

Case Study Example

Virtual Server On-Demand Instance Allocation

Virtual Server Reserved Instance Allocation

Cloud Storage Device

WAN Traffic

Chapter 18: Service Quality Metrics and SLAs

18.1 Service Quality Metrics

Service Availability Metrics

Availability Rate Metric

Outage Duration Metric

Service Reliability Metrics

Mean Time Between Failures (MTBF) Metric

Reliability Rate Metric

Service Performance Metrics

Network Capacity Metric

Storage Device Capacity Metric

Server Capacity Metric

Web Application Capacity Metric

Instance Starting Time Metric

Table of Contents

Response Time Metric

Completion Time Metric

Service Scalability Metrics

Storage Scalability (Horizontal) Metric

Server Scalability (Horizontal) Metric

Server Scalability (Vertical) Metric

Service Resiliency Metrics

Mean Time to Switchover (MTSO) Metric

Mean Time to System Recovery (MTSR) Metric

18.2 Case Study Example

18.3 SLA Guidelines

18.4 Case Study Example

Scope and Applicability

Service Quality Guarantees

Definitions

Usage of Financial Credits

SLA Exclusions

PART V: APPENDICES

Appendix A: Case Study Conclusions

A.1 ATN

A.2 DTGOV

A.3 Innovartus

Appendix B: Common Containerization Technologies

B.1 Docker

Docker Server

Docker Client

Docker Registry

Docker Objects

Docker Swarm (Container Orchestrator)

B.2 Kubernetes

Kubernetes Node (Host)

Kubernetes Pod

Table of Contents

Kubelet
Kube-Proxy
Container Runtime (Container Engine)
Cluster
Kubernetes Control Plane

Index