Week 1: Introduction to Cloud Systems

NT524 — Cloud Architecture and Security

PhD. Nguyen Ngoc Tu

September 10, 2025

Motivation for the Course

- **Cloud adoption is accelerating:**
  - 90%+ of enterprises use cloud in some form
  - Security remains the top concern (mối quan tâm hàng đầu)
- **Cybersecurity context (bối cảnh an ninh mạng):**
  - Threats evolve with cloud — misconfigurations, data leaks, ransomware
  - Cloud-native attacks require new defense models
- **Why this course?**
  - To equip students with both architecture design and security hardening skills
  - Foundation for roles: Cloud Security Engineer, DevSecOps Specialist

Warm-up Activity

Debate (thảo luận nhanh)

Which is more secure: On-premise datacenter or Cloud service?

Quick AWS Demo

- Launch an EC2 instance (AWS free tier)
- Explore security groups (nhóm bảo mật) vs. firewalls
- Observe responsibility boundaries

Course Overview

- **Position in Cybersecurity program**
  - Builds on Networking, Cryptography, and Operating Systems
  - Leads into Advanced topics: Incident Response, Zero Trust, Cloud Forensics
- **Structure:**
  - 15 weeks (11 lectures, 6 labs, 1 capstone project)
  - Hands-on with OpenStack (private cloud) and AWS (public cloud)
- **Integration:**
  - Security pillars link to access control, logging, monitoring, IAM
  - Capstone connects architecture + security + resilience

Academic Knowledge: Big Picture of Cloud

- **What is "Cloud"? (Điện toán đám mây)**
  - On-demand, elastic (cơ động, measured service (theo dõi/đo lường), self-service (tự phục vụ).
  - Abstraction of infra via APIs (trừu tượng hoá hạ tầng qua API).
- **Why move from Traditional IT? (Tại sao chuyển đổi)**
  - Agility (linh hoạt), time-to-value (thời gian tạo giá trị) & global reach (phạm vi toàn cầu).
  - Cost model shift: CapEx $\rightarrow$ OpEx (chuyển chi phí đầu tư sang chi phí vận hành).
  - Built-in services: IAM, monitoring, autoscaling, managed DB, CI/CD.
- **But:** Cloud *does not* eliminate responsibility—it *redistributes* it (phân bổ lại trách nhiệm).

Cloud Traits (NIST) — Cơ sở khái niệm

- On-demand self-service (Tự phục vụ theo yêu cầu)
- Broad network access (Truy cập mạng rộng)
- Resource pooling (Gộp tài nguyên)
- Rapid elasticity (Cơ động nhanh)
- Measured service (Dịch vụ đo lường được)

Shared Responsibility Model (Mô hình trách nhiệm chia sẻ)

- **Provider (Nhà cung cấp)**: Facilities, hardware, hypervisor, core services SLAs.
- **Customer (Khách hàng)**: Data classification/encryption, IAM policies, app security, configs.
- **Example (Ví dụ)**:
  - AWS manages physical security (Bảo vệ vật lý); you manage S3 bucket policies & KMS keys.
  - OpenStack operator manages control plane; tenant manages images, SGs, keypairs, patches.

Six Architecture Pillars (Sáu trụ cột) & What They Mean in Practice

1. **Operational Excellence (Tối ưu hóa vận hành)**: IaC, runbooks, game days, postmortems.
2. **Security (Bảo mật)**: Least privilege (ít quyền nhất), encryption (mã hoá), zero trust.
3. **Reliability (Tính tin cậy)**: HA, multi-AZ, backups, chaos testing.
4. **Performance Efficiency (Hiệu suất vận hành)**: Right-sizing, autoscaling, caching.
5. **Cost Optimization (Tối ưu chi phí)**: Rightsizing, lifecycle policies, spot/RI.
6. **Sustainability (Tính bền vững)**: Efficient resource use, server consolidation, telemetry.

Instructor tip: Ask students to map each pillar to one concrete control they will implement in lab.

Traditional vs. Cloud: What Stays the Same? (Điểm tương đồng)

- Security fundamentals: CIA triad (Tính bảo mật – Tính toàn vẹn – Tính sẵn sàng), IAM, patching, logging.
- Networking basics: IP, routing (định tuyến), segmentation, firewalls (tường lửa).
- Software lifecycle: SDLC, testing, deployment discipline.
- Compliance goals remain: Confidentiality (Tính bảo mật), Auditability (Khả năng kiểm toán), Data residency.

Traditional vs. Cloud: What Changes? (Khác biệt chính)

Dimension (khía cạnh)	**Traditional (truyền thống)**	**Cloud (đám mây)**
Provisioning (cấp phát)	Manual, ticket-driven	API-driven, IaC (hạ tầng như mã)
Elasticity (cơ động)	Fixed capacity	Auto scale (tự động mở rộng/thu hẹp)
Cost (chi phí)	CapEx-heavy	OpEx, pay-as-you-go (trả theo dùng)
Responsibility (trách nhiệm)	Org owns stack end-to-end	*Shared* with provider
Security controls	Perimeter-first	Identity-first, microsegmentation
Reliability	Vertical HA	Horizontal HA, multi-AZ/region
Ops model	Pets (máy chủ "thú cưng")	Cattle (cụm "gia súc"), immutable images
Change mgmt	Maintenance windows	Continuous delivery (liên tục)

Migration Drivers & Patterns (động lực & mẫu chuyển dịch)

- **Drivers (động lực)**: Agility, scale, cost, resilience (khả năng chống chịu), compliance, data gravity.
- **Patterns (mẫu)**:
  - Lift-and-Shift (di chuyển nguyên trạng): fastest, minimal code change; risks: legacy ops anti-patterns.
  - Replatform (tái nền tảng): adopt managed DB/cache, containers; moderate change, quick wins.
  - Refactor (tái cấu trúc): microservices, event-driven; biggest payoff, highest effort.
  - Replace/SaaS (thay thế): offload commodity capabilities.
- **Transitional Architectures (kiến trúc chuyển tiếp)**: hybrid (lai), strangler pattern, data replication.

TCO/ROI & Risk Framing (chi phí–lợi ích & rủi ro)

- Total Cost of Ownership (TCO): infra + licenses + staffing + downtime + egress + training.
- Return on Investment (ROI): speed, reliability gains, reduced undifferentiated heavy lifting.
- Risk trade-offs: vendor lock-in, misconfiguration (cấu hình sai), data residency, skills gap.
- Mitigations: multi-AZ, backups & DR (khôi phục sau thảm họa), policy-as-code, guardrails, FinOps.

Service Mapping: OpenStack & AWS (liên hệ dịch vụ)

Capability	**OpenStack**	**AWS (tương ứng)**
Compute (tính toán)	Nova	EC2
Images (ảnh máy)	Glance	AMI/ECR (for images/containers)
Networking (mạng)	Neutron	VPC, SG, NACL
Identity (định danh)	Keystone	IAM
Block storage	Cinder	EBS
Object storage	Swift	S3
Orchestration (dàn dựng)	Heat	CloudFormation
Telemetry (giám sát)	Ceilometer/Gnocchi	CloudWatch
Dashboard (bảng điều khiển)	Horizon	Console

Exercise (bài tập): Pick one workload; map its needs across both stacks (bảng yêu cầu → dịch vụ).

Case Study (nghiên cứu tình huống): Retail App Modernization

- **Start:** On-prem VM app with monolithic DB; weekend maintenance windows.
- **Step 1 (Lift-and-Shift):** Move VM to cloud; add backups & monitoring; quick win, limited agility.
- **Step 2 (Replatform):** Managed DB, cache, object storage for media; autoscaling for stateless tier.
- **Step 3 (Refactor):** Split checkout/inventory to microservices; event bus; CI/CD; blue-green (xanh–lục).
- **Security throughout:** IAM least-privilege, SG baselines, encryption, logs centralization & alerting.

From Similarities to Differences: What to Watch (lưu ý chuyển dịch)

- **Anti-patterns**:
  - "VM sprawl" in cloud; copying on-prem VLAN mindset into flat SGs.
  - Single-AZ deployments; no backups; secrets in AMIs or images.
- **Good patterns**:
  - IaC + immutable images; per-env accounts/projects; blast-radius reduction.
  - Policy-as-code (chính sách như mã), automated guardrails (bảo vệ tự động).
- **Readiness checklist** (kiểm tra sẵn sàng): Identity model, network plan, data plan, observability, DR.

Case Study: SMEs vs. Enterprises (Thực tế)

- **SME Example: Airbnb**
  - Adopted AWS early to scale from small start-up to global platform.
  - Motivations: agility (linh hoạt), global reach, minimal infra team.
  - Services: EC2, S3, RDS; later expanded to data analytics on EMR.
  - Source: AWS Customer Success Story (Airbnb)[1]
- **Enterprise Example: Capital One (Banking)**
  - First major U.S. bank to go all-in on AWS.
  - Motivations: improve security, agility in product delivery, DR (khôi phục sau thảm họa).
  - Strategy: hybrid transition $\rightarrow$ eventually full public cloud with strict compliance controls.
  - Source: AWS Case Study (Capital One)[2]

[1] https://aws.amazon.com/solutions/case-studies/airbnb/
[2] https://aws.amazon.com/solutions/case-studies/capital-one/

Why Did They Adopt Cloud?

Drivers across both cases:

1. **Agility (linh hoạt):** Faster launch of new features and global scale.
2. **Cost Efficiency (tiết kiệm chi phí):** Reduced upfront CapEx, shift to OpEx.
3. **Security & Compliance (bảo mật & tuân thủ):** AWS certified for PCI-DSS, SOC, GDPR, HIPAA.
4. **Resilience (khả năng chống chịu):** Multi-region failover, automated DR drills.
5. **Innovation (đổi mới):** Leverage managed AI/ML, analytics, and serverless services.

Discussion: SMEs focus on agility/cost; Enterprises focus on compliance/risk mitigation.

Comparative Insights

	Airbnb (SME)	**Capital One (Enterprise)**
Scale at adoption	Small start-up	Large regulated bank
Main drivers	Agility, global scale, low ops cost	Security, compliance, DR, innovation
Cloud model	Public AWS	Hybrid $\rightarrow$ Public AWS
Services adopted	EC2, S3, RDS, EMR	EC2, S3, Lambda, Redshift, KMS
Compliance burden	Low	High (PCI-DSS, SOX, GDPR)
Transformation impact	Scaled to millions of users worldwide	Faster product cycles, stronger security posture

Case Study: Vietnamese Context — MoMo (Ví điện tử)

- **Background:**
  - MoMo is Vietnam's leading e-wallet (ví điện tử), serving $>$ 30 million users.
  - Operates under strict State Bank of Vietnam (Ngân hàng Nhà nước) regulations.
- **Cloud Adoption:**
  - Leveraged AWS for scalability, high availability (tính sẵn sàng cao), and security certifications.
  - Integrated hybrid approach to ensure compliance with local data residency rules.
  - Used AWS KMS for encryption (mã hoá), VPC for secure network isolation, and CloudWatch for monitoring.
- **Source:** AWS MoMo Case Study[3]

[3] https://aws.amazon.com/solutions/case-studies/momo/

Why Did MoMo Move to Cloud?

1. **Scalability (khả năng mở rộng):** Handle transaction peaks during Tet holiday (Tết).
2. **Security (bảo mật):** PCI-DSS certification for payment security.
3. **Compliance (tuân thủ):** Balance between local data residency and global AWS infrastructure.
4. **Innovation (đổi mới):** Faster release of mobile payment features, AI-driven services.
5. **Resilience (khả năng chống chịu):** Multi-region deployment ensures continuity.

Discussion: MoMo's case highlights *local regulation challenges* and the need for hybrid deployment strategies.

Comparative Insights: Airbnb, Capital One, MoMo

	Airbnb (SME)	**Capital One (Enterprise)**	**MoMo (Vietnam)**
Scale at adoption	Start-up	Fortune 500 bank	Leading e-wallet in VN
Drivers	Agility, low ops cost	Security, compliance, DR	Scalability, security, local compliance
Cloud model	Public AWS	Hybrid $\rightarrow$ AWS	Hybrid AWS + local DC
Services adopted	EC2, S3, RDS, EMR	EC2, Lambda, Redshift, KMS	EC2, VPC, KMS, CloudWatch
Compliance burden	Low	Very high	High (State Bank, PCI-DSS)
Transformation impact	Global platform scale	Faster innovation, stronger security	Nationwide scale, resilient payments

Case Study: Facebook / Meta

- **Background:**
  - Social media giant with billions of users worldwide.
  - Unique scale requirements: latency in milliseconds, billions of photos/videos per day.
- **Cloud Strategy:**
  - Did not adopt public cloud at early stage — instead built own global infrastructure.
  - Developed **Open Compute Project (OCP)** for open-source hardware (máy chủ mã nguồn mở).
  - Built hyperscale data centers with cloud-native principles: elasticity, virtualization, SDN, automation.
  - In parallel, leverages public cloud selectively for AI/ML workloads and global collaborations.
- **Source:** Meta Open Compute Project[4]

[4] https://www.opencompute.org/

Why Facebook Took This Approach?

1. **Scale (quy mô):** Public cloud costs would be prohibitive for billions of daily active users.
2. **Performance (hiệu suất):** Custom hardware and network to meet latency-sensitive workloads.
3. **Control (kiểm soát):** Full control over data centers, hardware, and energy efficiency.
4. **Innovation (đổi mới):** Developed OCP servers, storage, and networking — influencing industry standards.
5. **Cost Optimization (tối ưu chi phí):** Reduced energy consumption and TCO through custom design.

Note: Unlike SMEs (Airbnb), enterprises (Capital One), or fintech (MoMo), Meta *is the cloud*.

Comparative Insights: Airbnb, Capital One, MoMo, Facebook

	Airbnb (SME)	**Capital One (Enterprise)**	**MoMo (Vietnam)**	**Facebook / Meta**
Scale at adoption	Start-up	Fortune 500 bank	Leading e-wallet in VN	Global hyperscale
Drivers	Agility, low ops cost	Security, compliance, DR	Scalability, compliance	Scale, performance, control
Cloud model	Public AWS	Hybrid → AWS	Hybrid AWS + local DC	Private hyperscale infra (OCP)
Services adopted	EC2, S3, RDS	EC2, Lambda, Redshift	EC2, VPC, KMS, CloudWatch	OCP servers, custom DC, SDN
Compliance burden	Low	Very high	High (SBV, PCI-DSS)	Global, internal standards
Transformation impact	Global platform scale	Faster innovation, stronger security	Nationwide resilient payments	Industry-wide innovation, OCP standards

Case Study: HBO Films / WarnerMedia

- **Background:**
  - Global entertainment company delivering movies and series (HBO Max, HBO Films).
  - Business challenge: unpredictable demand spikes during premieres (e.g., Game of Thrones).
- **Cloud Adoption:**
  - Leveraged AWS for global streaming infrastructure.
  - Adopted cloud-native delivery (CDN, autoscaling clusters, content protection).
  - Used Amazon CloudFront, S3, Elastic Transcoder for media delivery.
  - Hybrid integration with on-prem editing and production pipelines.
- **Source:** AWS Media Case Studies (WarnerMedia)[5]

[5] https://aws.amazon.com/solutions/case-studies/

Why HBO Films Moved to Cloud?

1. **Scalability (khả năng mở rộng):** Handle tens of millions of concurrent viewers worldwide.
2. **Reliability (độ tin cậy):** Guarantee uptime during high-profile premieres.
3. **Cost Optimization (tối ưu chi phí):** Pay-as-you-go infra vs. overprovisioning data centers.
4. **Global Reach (phạm vi toàn cầu):** Distribute content closer to users with CDN nodes.
5. **Security & DRM (bảo mật & quản lý quyền số):** Protect intellectual property with encryption and key management.

Note: For HBO, cloud is about *delivering media at scale securely and reliably*.

Comparative Insights: Airbnb, Capital One, MoMo, Facebook, HBO

	Airbnb (SME)	**Capital One (Finance)**	**MoMo (Vietnam)**	**Facebook / Meta**	**HBO Films**
Scale at adoption	Start-up	Fortune 500 bank	Leading e-wallet	Global hyperscale	Global media giant
Drivers	Agility, speed	Security, compliance	Scalability, regulation	Scale, performance, control	Streaming scale, reliability
Cloud model	Public AWS	Hybrid $\rightarrow$ AWS	Hybrid AWS + local DC	Private OCP infra	Public AWS (media services)
Services adopted	EC2, S3, RDS	EC2, Lambda, Redshift	EC2, VPC, KMS, CloudWatch	OCP, custom DC	CloudFront, S3, Transcoder
Compliance burden	Low	Very high	High (SBV, PCI-DSS)	Internal standards	DRM, IP protection
Transformation impact	Global scale	Faster innovation	Nationwide payments	Industry-wide infra innovation	Reliable global streaming

Industry Perspective — Public Cloud Case Study (AWS)

MoMo (Ví điện tử, Việt Nam)

- **Bối cảnh (background):** Ví điện tử dẫn đầu tại VN, khối lượng giao dịch cao, tuân thủ NHNN.
- **Động lực (drivers):**
  - Khả năng mở rộng (scalability) trong dịp cao điểm (Tết).
  - Bảo mật & tuân thủ (PCI-DSS, mã hoá end-to-end).
  - Độ sẵn sàng cao (high availability) & khôi phục sau thảm hoạ (DR).
- **Kiến trúc tiêu biểu trên AWS (highlights):**
  - Amazon EC2 (compute), Amazon VPC (cô lập mạng), Security Groups (nhóm bảo mật).
  - Amazon S3 (object storage) + KMS (quản lý khoá), CloudWatch (giám sát).
  - Tích hợp mô hình lai (hybrid) để đáp ứng yêu cầu vị trí dữ liệu (data residency).
- **Kết quả (outcomes):** Xử lý đột biến tải ổn định, rút ngắn thời gian ra mắt tính năng, tăng cường thế trận bảo mật.

Tham khảo: AWS Customer Stories (MoMo).

Industry Perspective — Cloud Provider Landscape (bức tranh nhà cung cấp)

Provider	Điểm mạnh (strengths)	Dịch vụ tiêu biểu (tương ứng)
AWS	Hệ sinh thái rộng, trưởng thành, toàn cầu	EC2 (compute), S3 (object), IAM (định danh), KMS (khoá), EKS (K8s), CloudFront (CDN)
Azure	Tích hợp doanh nghiệp/Windows tốt	Azure VMs, Blob Storage, Entra ID (IAM), Key Vault, AKS, Front Door/CDN
Google Cloud	Dữ liệu/ML mạnh, SRE tư duy	Compute Engine, Cloud Storage, IAM, Cloud KMS, GKE, BigQuery
Alibaba Cloud	Hiện diện mạnh tại châu Á	ECS, OSS, RAM (IAM), KMS, ACK (K8s), CDN
Oracle Cloud (OCI)	CSDL doanh nghiệp, hiệu năng I/O	OCI Compute, Object Storage, IAM/-Vault, OKE, Autonomous DB

Góc nhìn khoá học: Tuần 1 ưu tiên AWS (động lực thực hành); các tuần sau mở rộng tư duy kiến trúc/nhà cung cấp.

Industry Perspective — Common Implementation Challenges (thách thức thường gặp)

- **Bảo mật & IAM (identity-first):** Chính sách rối, quyền quá rộng, quản lý khoá kém.
  - *Mitigation:* Mô hình tài khoản/dự án chuẩn (landing zone), nguyên tắc *ít quyền nhất*, MFA, quay vòng khoá.
- **Cấu hình sai (misconfiguration):** S3 public, SG mở rộng, thiếu mã hoá lưu trữ/lưu thông.
  - *Mitigation:* Policy-as-Code, kiểm tra tự động (guardrails), template IaC đã chuẩn hoá.
- **Mạng (network) & phân đoạn:** Sao chép tư duy VLAN on-prem, thiếu tường lửa lớp ứng dụng.
  - *Mitigation:* Thiết kế VPC theo miền tin cậy, microsegmentation, WAF/CDN đúng chỗ.
- **Quan sát hệ thống (observability):** Thiếu log/metrics chuẩn, alert nhiễu (alert fatigue).
  - *Mitigation:* "Golden signals", chuẩn hoá log, SLO/SLI, runbook phản ứng sự cố.
- **Chi phí (FinOps):** Thiếu hiển thị chi phí, overprovision, egress bất ngờ.
  - *Mitigation:* Tagging bắt buộc, ngân sách/cảnh báo (budget & alert), rightsizing, lifecycle policies.
- **Di trú ứng dụng (migration):** Ràng buộc di sản (legacy), lock-in, thiếu kỹ năng.
  - *Mitigation:* Đánh giá 7R (Rehost/Replatform/Refactor/Repurchase/Retain/Retire/Relocate), thí điểm theo lớp, đào tạo DevSecOps.

Mini Activity (AWS) — Từ góc nhìn ngành đến thực hành

- **Nhiệm vụ:** Chọn một thách thức ở slide trước (ví dụ: IAM, chi phí, cấu hình sai).
- **Thực hiện trên AWS:**
  - Tạo một Security Group tối thiểu (ít quyền nhất) cho EC2.
  - Bật CloudTrail/CloudWatch log cơ bản và một cảnh báo (alarm).
  - Áp dụng tag chi phí: `Project=Week1`, `Owner=TeamX`.
- **Kết quả nộp (deliverable):** 3 ảnh chụp màn hình + 5 gạch đầu dòng "bài học rút ra".

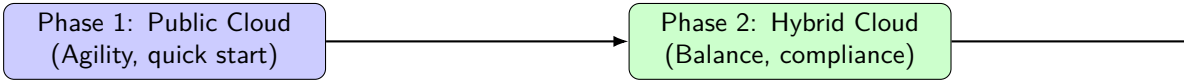
Modes of Cloud Adoption (các mô hình tiếp cận)

- **Public Cloud (đám mây công cộng):**
  - Fastest entry, no infra ownership.
  - Pay-as-you-go (trả theo mức sử dụng), global scale.
  - Challenges: compliance (tuân thủ), lock-in, data residency.
- **Private Cloud (đám mây riêng):**
  - Full control, on-premises (tại chỗ).
  - Sensitive workloads (PCI-DSS, HIPAA).
  - Challenges: high CapEx, limited elasticity.
- **Hybrid Cloud (đám mây lai):**
  - Mix of public + private.
  - Best for regulated industries, phased migration.
  - Requires networking, identity federation (liên kết định danh).

Shift from Public to Hybrid to Optimal Assets

1. **Phase 1: Public-first**
   - SMEs adopt AWS/Azure/GCP for agility (linh hoạt).
   - Typical use: dev/test, web apps, DR (khôi phục sau thảm hoạ).
2. **Phase 2: Hybrid**
   - Enterprises add private cloud (OpenStack, VMware) for regulated workloads.
   - Integrate on-prem DC with AWS/Azure via VPN/Direct Connect.
3. **Phase 3: Optimal Assets (tối ưu tài sản)**
   - Workload placement based on cost, compliance, performance.
   - **Examples:** AI/ML training → Public GPU Cloud, Payment core → Private, Media CDN → Public Edge.
   - Use multi-cloud (đa đám mây) + FinOps to avoid waste.

Visualizing the Shift (Hành trình chuyển dịch)



Discussion: Where is your organization (or university) today? Where should it aim to be?

Workload Placement (ra quyết định nhanh)

- **Latency/Residency nghiêm ngặt** ⇒ Private/Hybrid trước.
- **Burst/AI Training/Analytics** ⇒ Public (GPU/managed).
- **Chi phí ổn định, ít tuân thủ** ⇒ so sánh NPV 3 năm.
- **Luôn** cân nhắc egress + độ trưởng thành dịch vụ quản lý.

Hands-on Guide: AWS First!

Step 1: Launch an EC2 Instance

- Use AWS Console (Free Tier).
- Choose Amazon Linux or Ubuntu AMI.
- Select t2.micro instance type.

Step 2: Configure Security (Nhóm bảo mật)

- Add inbound rule: SSH (port 22) from your IP only.
- Add HTTP (port 80) to test web server later.
- Emphasize “least privilege” rule design.

Step 3: Attach Monitoring

- Enable AWS CloudWatch metrics: CPU, Network, Disk.
- Create a simple alarm (e.g., CPU $>$ 70%).

Migration Patterns — 7R (mẫu di trú)

Mẫu	Mô tả (vi)
Rehost	Di chuyển nguyên trạng (lift&shift) để nhanh có kết quả.
Replatform	Thay thành dịch vụ quản lý (DBaaS, cache) để giảm vận hành.
Refactor	Vi tách vi dịch vụ, sự kiện hoá để tối ưu dài hạn.
Repurchase/Replace	Chuyển sang SaaS thay vì tự vận hành.
Retain	Giữ nguyên on-prem do ràng buộc/giá trị còn lại.
Retire	Loại bỏ hệ thống/dịch vụ không còn cần thiết.
Relocate	Di chuyển hạ tầng máy ảo nguyên cụm (vMotion/VMware Cloud, v.v.).

Preview: OpenStack (Next Labs)

- In upcoming weeks, you will build your **own cloud** using OpenStack:
  - Deploy minimal Nova + Glance with Ansible.
  - Launch a VM from a base image.
  - Install node exporter for monitoring.
- AWS gives you the *consumer view* of cloud; OpenStack will give you the *provider/architect view*.

AWS Safety & Guardrails (bảo vệ căn bản)

- **Tài khoản:** Bật MFA, không dùng root cho tác vụ thường ngày.
- **Chi phí (FinOps):** Tạo Budget & Alert; bắt buộc tag: `Project=Week1`, `Owner=TeamX`.
- **Bảo mật:** SG *ít quyền nhất*; không mở 0.0.0.0/0 cho SSH.
- **Vùng (Region):** Chọn 1 region duy nhất cho toàn buổi lab.
- **Teardown:** Stop/Terminate EC2, xóa SG/KeyPair/Elastic IP, kiểm tra CloudWatch/CloudTrail.

Threat Model Lite (STRIDE) cho EC2

- Spoofing: khoá/credentials $\Rightarrow$ quản lý keypair chặt, không reuse.
- Tampering: trôi SG $\Rightarrow$ lưu SG JSON baseline; so sánh sau lab.
- Repudiation: CloudTrail phải có log API create-instance.
- Information Disclosure: tránh public S3/metadata; không nhúng secrets vào AMI.
- DoS: giới hạn SG; alarm CPU $> 70\%$ để phát hiện bất thường.
- Elevation of Privilege: tránh IAM wild-card; kế hoạch role cho Tuần 11.

Wrap-up and Deliverables

- **Security Emphasis (Bảo mật):**
  - Identify shared responsibility boundaries.
  - Apply least-privilege to Security Groups.
- **Deliverable (Bài nộp):**
  - Checklist: Six Pillars applied to your AWS EC2 setup.
  - Screenshot of EC2 instance, Security Group, CloudWatch alarm.
- **Suggested Reading:**
  - Erl & Barcelo (2024), Chapters 1–2
  - Kavis (2014), Chapter 1