الوحدة 18: السحابة والمحاكاة الافتراضية

المحاكاة الافتراضية (Virtualization) و Hypervisors

Hypervisor (Type 1 - Bare metal): يعمل مباشرة على العتاد (مثل VMware ESXi, Hyper-V, Proxmox). أداء عالٍ لأنه لا يحتاج لنظام تشغيل وسيط.

Hypervisor (Type 2 - Hosted): يعمل فوق نظام تشغيل (مثل VirtualBox, VMware Workstation). مناسب للاختبار والتعليم، لكنه أقل أداءً.

فوائد المحاكاة: عزل الأجهزة الافتراضية عن بعضها، إنشاء snapshots للاستعادة، توفير الطاقة والمساحة.

مثال: إدارة حاويات Docker

```
docker ps -a
docker run -d -p 80:80 --name web nginx
docker stop web
docker rm web
```

`docker ps -a` - عرض جميع الحاويات (العاملة والمتوقفة). `docker ps` فقط يعرض العاملة.

`docker run -d -p 80:80 --name web nginx` - تشغيل حاوية جديدة: `-d` (خلفية)، `-p 80:80` (ربط المنفذ 80 للمضيف بالحاوية)، `--name web` (اسم مخصص)، `nginx` (صورة الحاوية).

`docker stop web` - إيقاف الحاوية web بأمان (إشارة SIGTERM ثم SIGKILL بعد مهلة).

`docker rm web` - حذف الحاوية المتوقفة نهائياً لتحرير الموارد.

مثال: أوامر Kubernetes الأساسية

```
kubectl get pods
kubectl get services
kubectl describe pod my-pod
```

`kubectl get pods` - عرض قائمة Pods في الكتلة. Pod هو أصغر وحدة في K8s (حاوية واحدة أو أكثر).

`kubectl get services` - عرض الخدمات (Services) التي توفر عناوين IP ثابتة للـ Pods. توازن التحميل مدمج.

`kubectl describe pod my-pod` - تفاصيل كاملة عن Pod: الحالة، الأحداث، IP، السجلات.

نماذج الخدمات السحابية (IaaS, PaaS, SaaS)

IaaS (Infrastructure as a Service): بنية تحتية (خوادم، تخزين، شبكات). أنت تدير نظام التشغيل والتطبيقات. مثال: AWS EC2, Azure VM.

PaaS (Platform as a Service): منصة تطوير (قاعدة بيانات، بيئة تشغيل). أنت تكتب الكود فقط. مثال: Google App Engine, Heroku.

SaaS (Software as a Service): برنامج جاهز (مثل Office 365, Gmail). المستخدم النهائي لا يدير شيئاً.

Shared Responsibility Model: المزود يؤمن السحابة، المستخدم يؤمن ما بداخل السحابة. يختلف حسب النموذج.

CASB و CSPM

CASB (Cloud Access Security Broker): وسيط أمني بين المستخدمين ومزودي الخدمات السحابية. يوفر رؤية للاستخدام والتحكم في التطبيقات المسموح بها (Shadow IT).

CSPM (Cloud Security Posture Management): يراقب التهيئة الخاطئة للسحابة (مثل دلو S3 مفتوح). يكتشف المخاطر قبل استغلالها. أساسي في DevSecOps.

مثال: أوامر AWS S3 (باستخدام AWS CLI)

```
aws s3 ls
aws s3 cp myfile.txt s3://my-bucket/
aws s3 ls s3://my-bucket/ --recursive
```

`aws s3 ls` - عرض جميع دلاء S3 في الحساب. مفيد للتأكد من أن الدلاء مسموح بها فقط.

`/aws s3 cp myfile.txt s3://my-bucket` - رفع ملف myfile.txt إلى الدلو. `cp` يمكن استخدامه عكسياً للتحميل.

`--recursive` - سرد جميع الملفات والمجلدات بشكل متكرر. مفيد لتدقيق المحتوى والتحقق من عدم وجود بيانات حساسة.

Quick Quiz (MCQ)

1. Which cloud service model gives customers control over the operating system, storage, and deployed applications?
   a) SaaS
   b) PaaS
   c) IaaS
   d) DaaS

   Answer: c

2. What type of hypervisor runs directly on the host hardware without a host operating system?
   (a) Type 2 (Hosted
   (b) Type 1 (Bare-metal

(c) Type 3 (Embedded

(d) Type 0 (Kernel

Answer: b

.3 ?(What is a CASB (Cloud Access Security Broker

a) A cloud storage provider

b) A security policy enforcement point between cloud consumers and providers

c) A load balancer for cloud servers

d) A DNS resolver for cloud services

Answer: b

.4 Which cloud service model abstracts the underlying infrastructure and allows developers to focus on ?writing and deploying code

a) IaaS

b) SaaS

c) PaaS

d) NaaS

Answer: c

.5 ?What is a key security advantage of container virtualization over traditional virtual machines

a) Stronger encryption

b) Smaller attack surface and faster startup

c) Better hardware compatibility

d) Higher memory usage

Answer: b