



Luca Cabibbo  
**Architettura  
dei Sistemi  
Software**

# Macchine virtuali e virtualizzazione di sistema

Hai seguito ma non hai seguito il filo al 100%, riascolta  
**dispensa asw620**  
ottobre 2024

*Reality is merely an illusion,  
albeit a very persistent one.*

*Albert Einstein*

1

Macchine virtuali e virtualizzazione di sistema

Luca Cabibbo ASW



## - Riferimenti

- ❑ Luca Cabibbo. **Architettura del Software: Strutture e Qualità**. Edizioni Efestò, 2021.
  - Capitolo 35, **Macchine virtuali e virtualizzazione di sistema**
- ❑ Tanenbaum, A.S. and Bos, H. **Modern Operating Systems**, fourth edition. Pearson, 2015.
- ❑ Coulouris, G, Dollimore, J., Kindberg, T., and Blair, G. **Distributed Systems: Concepts and Design**, fifth edition. Pearson, 2012.
- ❑ Bass, L., Weber, I., and Zhu, L. **DevOps: A Software Architect's Perspective**. Addison-Wesley, 2015.
- ❑ Richardson, C. **Microservices Patterns: With examples in Java**. Manning, 2019.
- ❑ Siti web di diversi sistemi di virtualizzazione

2

Macchine virtuali e virtualizzazione di sistema

Luca Cabibbo ASW

Il documento esplora il concetto di virtualizzazione di sistema e delle macchine virtuali (VM), analizzandone caratteristiche, tecnologie e applicazioni. Ecco un riassunto:

#### Definizione

- La virtualizzazione di sistema permette a un computer fisico di ospitare uno o più macchine virtuali, che emulano l'hardware di un computer reale e possono eseguire sistemi operativi (OS) e applicazioni indipendenti.
- La virtualizzazione è realizzata tramite un hypervisor (o Virtual Machine Monitor), che gestisce le risorse fisiche e virtuali.

#### Tipi di Hypervisor

1. Tipo 1 (bare-metal): Si installa direttamente sull'hardware (es. VMware ESXi, Xen).
2. Tipo 2 (hosted): Funziona come applicazione sopra un OS host (es. VirtualBox, VMware Workstation).

#### Tecniche di Virtualizzazione

- Processore: Può essere emulato o virtualizzato con assistenza hardware (es. Intel VT-x, AMD SVM) per migliorare l'efficienza.
- Memoria: Le VM ricevono aree di memoria isolate. Tecniche come deduplicazione delle pagine e ballooning ottimizzano l'uso della memoria.
- I/O e Storage: Dispositivi virtuali (es. dischi o schede di rete virtuali) semplificano la configurazione e il funzionamento, ma possono introdurre overhead.
- Rete: Include schede di rete virtuali (vNIC) e switch virtuali per collegare le VM tra loro e con la rete esterna.

#### Gestione delle VM

- Immagini di VM: Entità statiche che definiscono lo stato iniziale di una VM.
- Snapshot: Salvataggi dello stato attuale della VM (memoria, processore, storage), utili per ripristini rapidi o migrazioni.
- Migrazione: Spostamento di VM da un host fisico a un altro, con possibilità di live migration senza interruzioni.

#### Applicazioni

- Server consolidation: Riduzione del numero di server fisici, ottimizzando l'uso delle risorse hardware.
- Testing e sviluppo: Creazione di ambienti isolati per test multipli.
- Cloud computing: Fondamentale per scalabilità e gestione flessibile di risorse distribuite.
- Sicurezza e sandboxing: Esecuzione sicura di applicazioni non affidabili.

#### Benefici

- Riduzione dei costi: Migliore utilizzo delle risorse hardware.
- Isolamento e sicurezza: Le VM sono indipendenti l'una dall'altra e dall'host.
- Scalabilità e agilità: Creazione rapida di ambienti virtuali.
- Supporto al cloud: Migliora la portabilità e l'efficienza dei servizi cloud.

#### Inconvenienti

- Overhead prestazionale: La virtualizzazione introduce un sovraccarico che può influire sulle prestazioni.
- Gestione complessa: Aggiornamenti e manutenzione richiedono risorse amministrative.
- Uso inefficiente delle risorse: Servizi leggeri distribuiti in molte VM possono aumentare il consumo complessivo.

#### Discussione

La virtualizzazione di sistema è una tecnologia chiave per i sistemi distribuiti e il cloud computing, consentendo flessibilità, isolamento e utilizzo efficiente delle risorse. Tuttavia, il suo utilizzo deve essere pianificato per minimizzare gli inconvenienti.



# - Obiettivi e argomenti

Un ambiente è un insieme di nodi, questi nodi possono essere fisici o virtuali

## □ Obiettivi

- introdurre la virtualizzazione di sistema e le macchine virtuali
- descrivere alcune tecniche e opzioni di virtualizzazione
- presentare alcuni sistemi di virtualizzazione
- discutere le macchine virtuali come opzione per il rilascio del software

## □ Argomenti

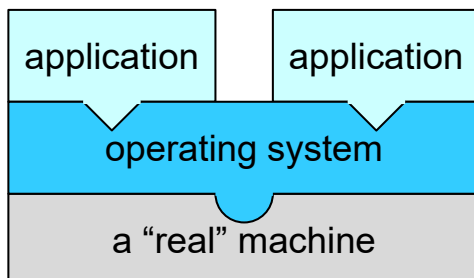
- virtualizzazione di sistema e macchine virtuali
- tecniche per la virtualizzazione di sistema
- sistemi di virtualizzazione
- applicazioni e benefici della virtualizzazione di sistema
- macchine virtuali e rilascio del software
- discussione



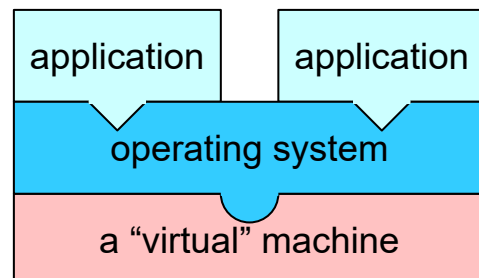
## \* Virtualizzazione di sistema e macchine virtuali

- La **virtualizzazione di sistema** consente a un computer “reale” di ospitare uno o più computer “virtuali” – chiamati **macchine virtuali**

È una tecnologia che consente ad un computer fisico, reale, di ospitare uno o più computer virtuali. Questi computer virtuali offrono tutte le funzionalità dei computer reali pur non essendolo. Su una macchina virtuale, come su una reale, possiamo installare un SO ed eseguire delle operazioni. I termini macchina REALE e VIRTUALE si riferiscono quindi all'HARDWARE.



un computer “reale” – con il suo OS e le sue applicazioni



un computer “virtuale” – con il suo OS e le sue applicazioni



# Virtualizzazione (in generale)

- ❑ In generale, la **virtualizzazione** ha lo scopo di fornire l'accesso a un insieme di risorse computazionali **virtuali** a partire da un insieme di risorse computazionali **reali**
  - ad es., si pensi a un file system oppure a una Virtual Private Network
  - la virtualizzazione delle risorse avviene sulla base di uno strato **software di virtualizzazione** – tra le risorse reali e i consumatori delle risorse virtuali

Il termine virtualizzazione è usato in informatica con diversi significati. In generale vuol dire “io ho delle risorse reali, fornisco un accesso ad un livello di astrazione maggiore a queste risorse come se fossero risorse virtuali”. L'idea è quindi quella di definire risorse computazionali virtuali a partire da risorse computazionali reali, che hanno caratteristiche più desiderabili e che sono più semplici da utilizzare.

Un classico esempio è quello del file system che fa la virtualizzazione dello storage. Lo storage fisico è fatto da dischi cilindri blocchi lettori ecc quindi ciò che possiamo fare con l'hardware fisico è solo lettura e scrittura di un settore e al livello di realizzazione di applicazione questo è un po' scomodo. Allora l'astrazione offerta dal file system è quella in cui leggo i file di lunghezza non definita, organizzati in cartelle in modo gerarchico, posso leggere e scrivere file, appendere cose al file ecc ecc, e quindi per le applicazioni questo tipo di virtualizzazione è molto più semplice da utilizzare rispetto all'accesso ad una posizione. Però rimane il fatto che il disco deve esserci, una risorsa fisica deve esserci.

La virtualizzazione effettua una astrazione, mostra delle cose che non ci sono, come se in realtà ci fossero. In particolare avviene sulla base di un software di virtualizzazione posto tra le risorse reali e i consumatori delle risorse virtuali



## Virtualizzazione di sistema

Ci sono varie forme di virtualizzazione. Con quella “di sistema” si intende quella dell'HARDWARE di un COMPUTER FISICO. Abbiamo quindi la parte fisica che è la parte fisica di hardware di una macchina e la parte virtuale

- ❑ La **virtualizzazione di sistema** (**system virtualization** o **hardware virtualization**) virtualizza l'hardware di un intero computer fisico reale (“sistema”) per fornire una o più **macchine virtuali**
  - il software di virtualizzazione è chiamato **hypervisor** oppure **virtual machine monitor (VMM)**
  - viene chiamata spesso semplicemente “virtualizzazione”
- ❑ La virtualizzazione di sistema è una tecnologia importante soprattutto nei sistemi distribuiti e nel cloud
  - è una tecnologia abilitante per la gestione flessibile di ambienti di esecuzione (virtuali) – per eseguire in modo flessibile un insieme di applicazioni e servizi
  - è una tecnologia abilitante fondamentale del cloud computing
  - può sostenere qualità come disponibilità e scalabilità



# Macchine virtuali

- Una **macchina virtuale** (**virtual machine** o **VM**) è l'emulazione di una macchina reale
  - per “macchina” si intende l'hardware di un computer
  - una macchina virtuale espone la stessa interfaccia di un computer reale – ovvero, un insieme di risorse hardware (virtuali), come uno o più processori, una memoria, dei dispositivi di storage e di rete, ...
  - una macchina virtuale fornisce dunque l'**hardware virtuale di un computer completo** – in cui è poi possibile installare ed eseguire un OS e un insieme di servizi e applicazioni

7

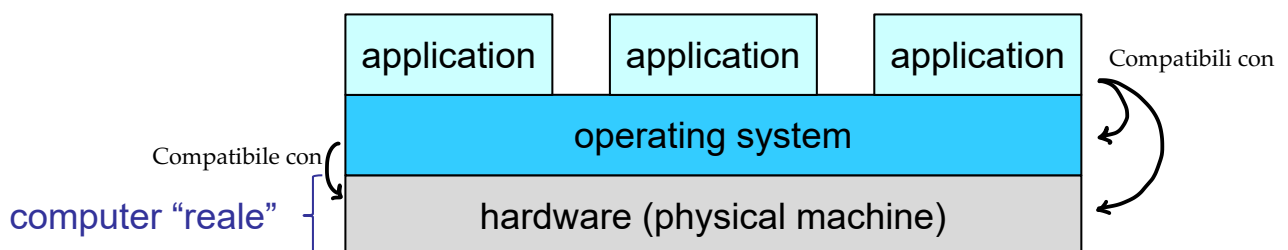
Macchine virtuali e virtualizzazione di sistema

Luca Cabibbo ASW



## Virtualizzazione e macchine virtuali

- Un esempio di computer non virtualizzato



8

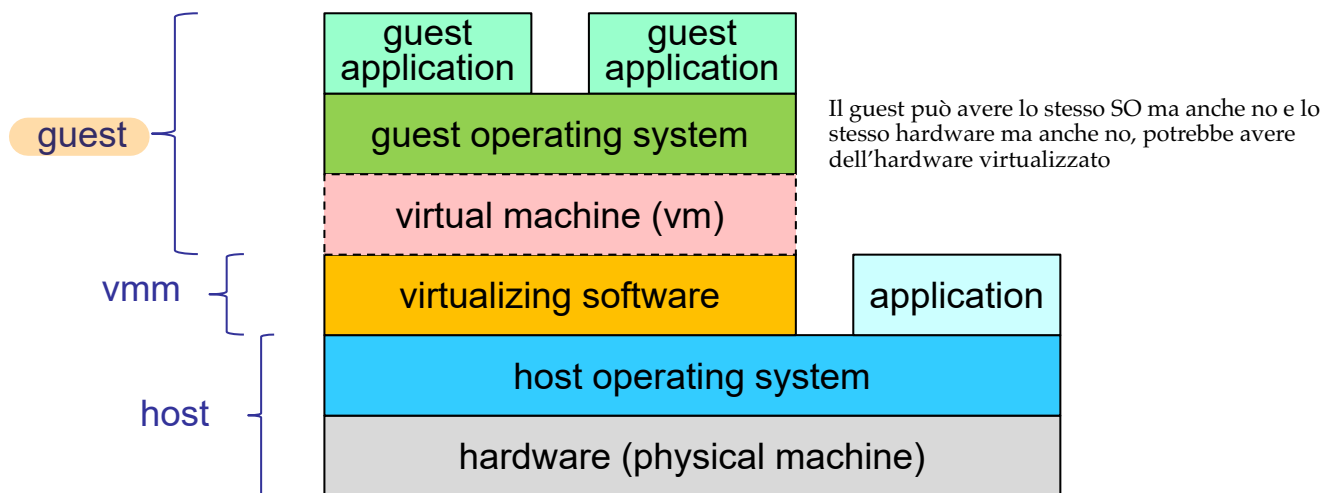
Macchine virtuali e virtualizzazione di sistema

Luca Cabibbo ASW



# Virtualizzazione e macchine virtuali

- Un esempio di computer virtualizzato
  - il computer fisico è l'**host**
  - il software di virtualizzazione è un *hypervisor* o *virtual machine monitor* (*VMM*)
  - la macchina virtuale è il **guest**



9

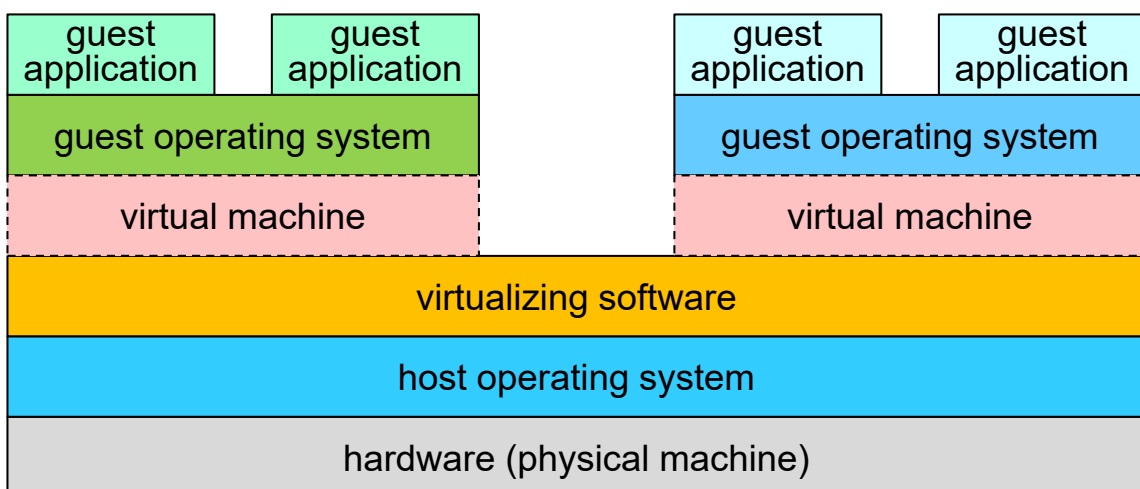
Macchine virtuali e virtualizzazione di sistema

Luca Cabibbo ASW



# Virtualizzazione e macchine virtuali

- Un altro esempio, in cui l'host ospita più VM



10

Macchine virtuali e virtualizzazione di sistema

Luca Cabibbo ASW

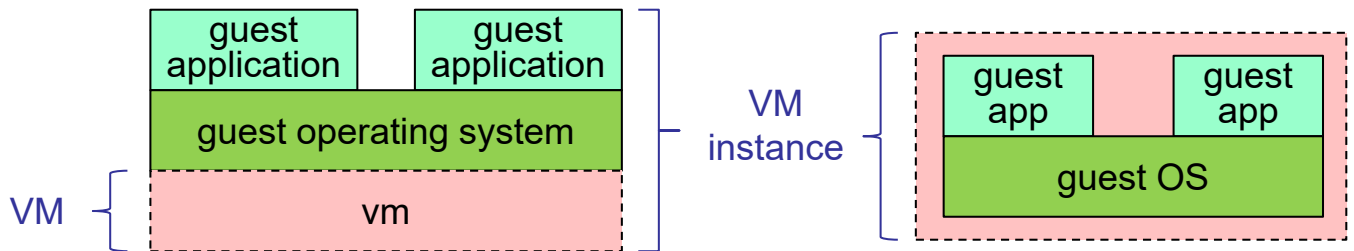


# VM e istanze di VM

Terminologia:

- Una precisazione sul termine “macchina virtuale”
  - una **macchina virtuale (VM)** è un’entità virtuale che emula l’**hardware** di un computer reale
  - un’**istanza di macchina virtuale (VM instance)** è una VM insieme al suo OS, alle sue applicazioni e al suo stato

Quindi una VM su cui sono installati e sono in esecuzione il SO e le applicazioni e in cui è presente uno stato attuale



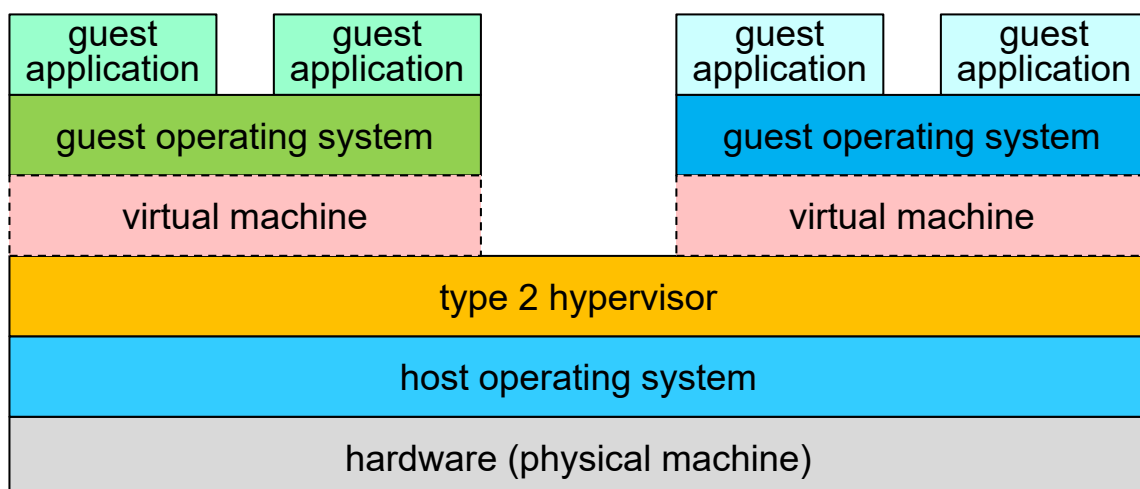
- il termine macchina virtuale viene però spesso utilizzato in pratica anche per indicare un’istanza di macchina virtuale



## Hypervisor di tipo 1 e 2

- Due tipi principali di hypervisor
  - **type 2 (hosted VMM o hosted hypervisor)**
    - VMware Workstation, Oracle VM Virtualbox, ...

Sono quelli comunemente usati per uso personale. Sono applicazioni che si installano sul sistema operativo del guest.



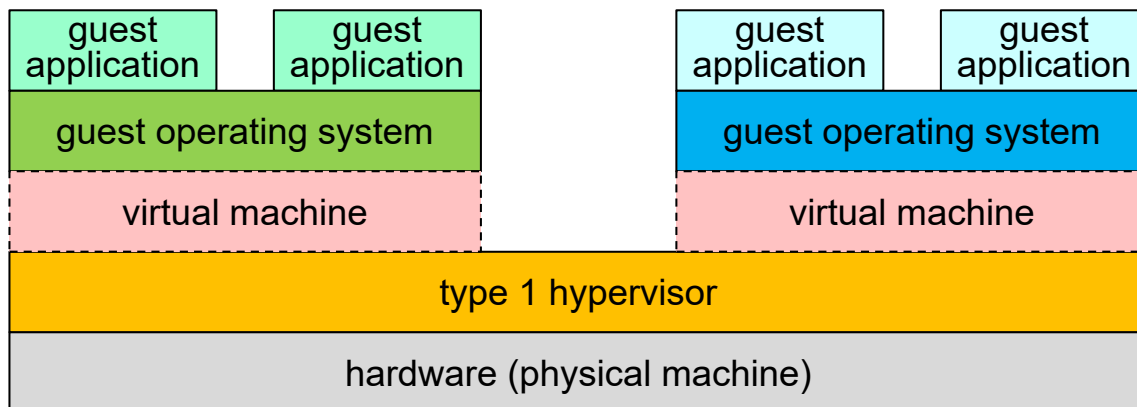


# Hypervisor di tipo 1 e 2

## ■ Due tipi principali di hypervisor

- **type 1** (*native VMM o bare-metal hypervisor*)
  - VMware vSphere, Xen, ...

Si installano direttamente sull'hardware, senza necessità di un SO del guest, quindi virtualizzazione l'intero hardware e a volte hanno qualche funzione da SO. Sono usati in ambienti enterprise

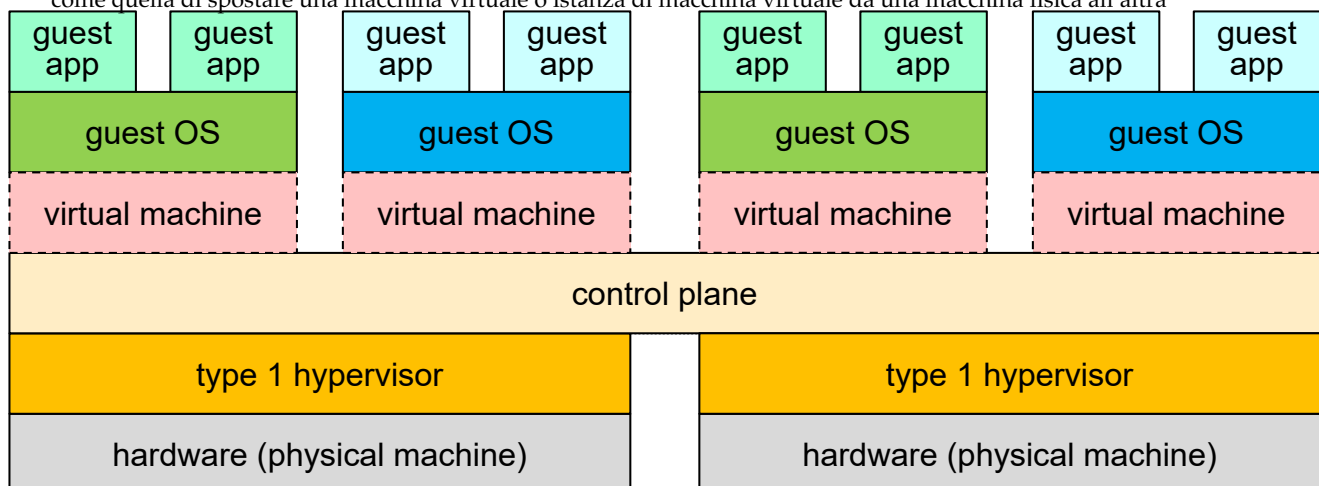


# Hypervisor di tipo 1 e 2

## ■ Due tipi principali di hypervisor

- **gli hypervisor di tipo 1 possono supportare la virtualizzazione di un cluster di host fisici – mediante uno strato software distribuito (*control plane*)**

Possono essere usati in data center per virtualizzare non un singolo computer ma tanti, anche se questo viene fatto con un ulteriore strato software in ciascuna macchina reale. Questo avviene grazie al control plane, distribuito su tutte le macchine che permette di gestire tutte le macchine virtualizzate. Il control plane ha anche funzionalità aggiuntive, come quella di spostare una macchina virtuale o istanza di macchina virtuale da una macchina fisica all'altra





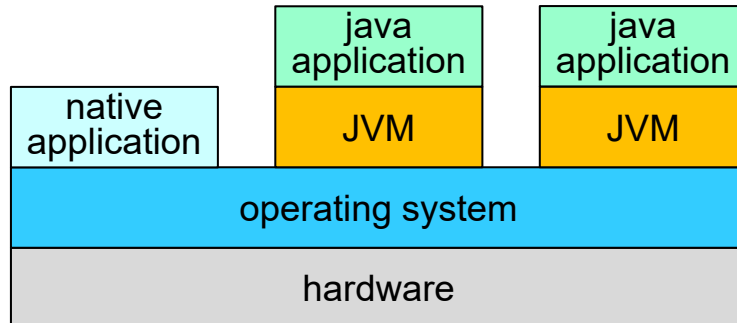


# Virtualizzazione di processo



- Un'altra forma di virtualizzazione è la **virtualizzazione di processo** (**process virtualization**)
  - ad es., la Java Virtual Machine (JVM)

Una virtualizzazione di sistema non è l'unica forma di virtualizzazione. Un'altra è la virtualizzazione di processo (es macchina virtuale Java, che consente di eseguire, su una qualunque piattaforma hardware/software, delle applicazioni Java)

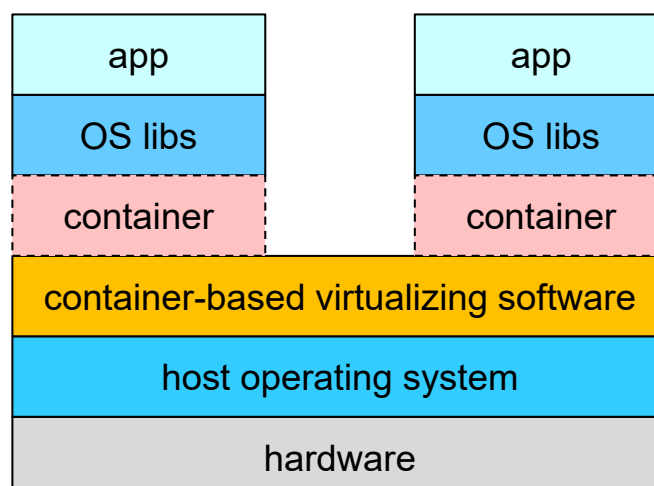


# Virtualizzazione basata su container



- Un'altra forma di virtualizzazione è la **virtualizzazione basata su container** (**container-based virtualization** o **OS-level virtualization**)
  - ogni **container** è un computer dotato di un kernel di OS virtuale (il kernel dell'OS host)

Altra forma di virtualizzazione è quella basata su container. È un tipo di virtualizzazione che prevede del software per virtualizzazione installato e supportato dal so host che permette di eseguire delle cose che si chiamano container, che in prima approssimazione sono assimilate a VM leggere, in seconda approssimazione sono assimilate a insiemi di processi. Ne parleremo più avanti





## \* Tecniche per la virtualizzazione di sistema

Che differenza c'è se eseguo un'applicazione software su una macchina fisica o su una virtuale? Devo comprendere la virtualizzazione di sistema



- ❑ L'hardware di un computer (reale o virtuale) è composto da un insieme di risorse (reali o virtuali) – CPU, memoria, I/O, reti, storage, ...
  - l'hypervisor deve fornire e gestire le risorse virtuali delle VM in termini delle risorse fisiche sottostanti
  - ci sono più tecniche di virtualizzazione per ciascun tipo di risorsa
  - descriviamo ora alcune tecniche e opzioni di virtualizzazione usate nella virtualizzazione di sistema



## - Requisiti generali per la virtualizzazione

### ❑ Requisiti per la virtualizzazione

- 4) ▪ l'hypervisor deve fornire l'illusione che ogni VM agisca come un computer reale  
Vero ma con delle eccezioni, ad esempio la virtualizzazione non può essere annidata, quindi su una macchina virtuale non posso eseguire un hypervisor
- 2) ▪ l'hypervisor dovrebbe fornire questa illusione in modo efficace ed efficiente, con queste caratteristiche
  - **fedeltà** – il comportamento di un programma in una VM dovrebbe corrispondere a quello in un computer reale
  - **sicurezza** – l'hypervisor dovrebbe avere controllo completo delle risorse virtualizzate
  - **efficienza** – la maggior parte del codice della VM dovrebbe essere eseguito direttamente dal computer host, senza intervento dell'hypervisor



## - Virtualizzazione del processore

Composta da istruzioni del processore e stato del processore

- ❑ Un processore è caratterizzato dalla sua ISA (Instruction Set Architecture) – l'ISA definisce le istruzioni del processore e il suo stato (registri e memoria) Quindi quando virtualizzo un processore devo virtualizzare sia istruzioni che stato
  - due approcci principali per la virtualizzazione dei processori
    - ① ▪ emulazione del processore
    - ② ▪ virtualizzazione del processore



## ① Emulazione del processore



- ❑ L'**emulazione del processore** – utile soprattutto quando il processore reale e quello virtuale sono di tipi differenti – avviene mediante la **virtualizzazione dell'ISA** (emulazione della CPU)
  - intuitivamente, si basa sulla **traduzione binaria** delle istruzioni
  - oggi è una tecnica di minore importanza, grazie all'ampia diffusione dei processori x86

Quello che succede è che l'hypervisor (la parte di emulazione del processore) svolge una di interpretazione delle istruzioni del linguaggio macchina del guest quindi l'idea è quella di fare una traduzione binaria delle istruzioni che devono essere eseguite. L'hypervisor prende il controllo e prende un blocco di istruzioni, lo traduce, lo esegue e passa al blocco successivo.



②

## Virtualizzazione del processore

- ❑ Se il processore reale e quello virtuale sono dello stesso tipo, allora molte istruzioni del software in esecuzione in una VM possono essere eseguite direttamente dal processore dell'host
  - in particolare, questo è vero per tutte le istruzioni che il guest esegue in “user mode”
  - tuttavia, ci sono alcune istruzioni che il guest esegue in “kernel mode” che sono “problematiche” – e non vanno eseguite direttamente dal processore host
    - ad es., le istruzioni del kernel dell'OS guest per abilitare e disabilitare le interruzioni e le istruzioni per la gestione della MMU (Memory Management Unit)

Il processore può funzionare in kernel mode (riservato al so) o user mode (utilizzato dalle operazioni). Le operazioni user mode possono essere eseguite direttamente dal processore host.  
Tra le operazioni in kernel mode ce ne sono alcune problematiche (es abilitare / disabilitare le interruzioni, organizzazione della memoria) che non possono essere eseguite automaticamente dal processore host, e vanno invece gestite come chiamate all'hypervisor.



## Virtualizzazione assistita dall'hardware

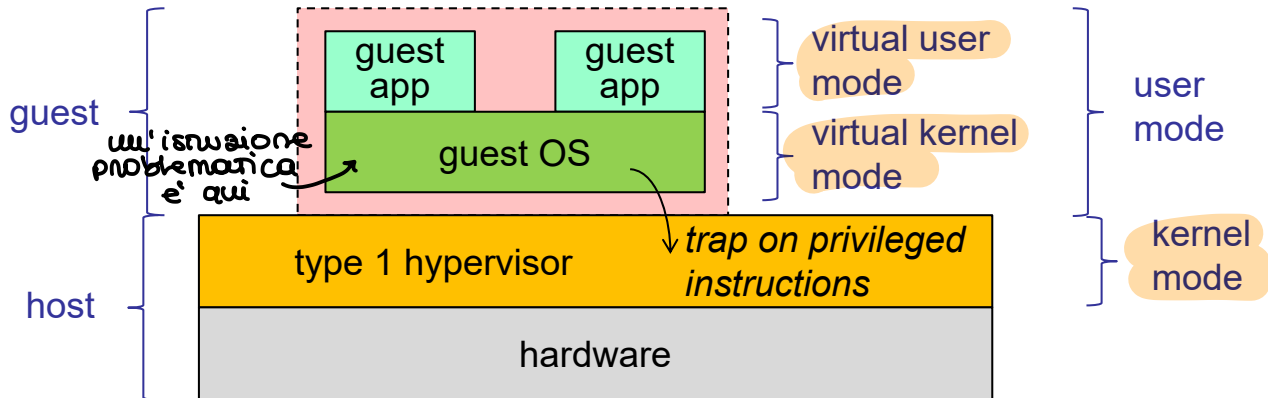
- ❑ La tecnica principale per la virtualizzazione del processore è la **virtualizzazione assistita dall'hardware** (chiamata anche **trap-and-emulate**)
  - le istruzioni della VM vengono eseguite dal processore reale dell'host – che normalmente le esegue direttamente – ma che cattura le istruzioni non virtualizzabili della VM (“trap”) e le gestisce come chiamate all'hypervisor (“emulate”)
    - si basa sull'uso di tecnologie hardware di virtualizzazione – ad es., Intel VT-x e AMD SVM nei processori x86 (dal 2005)

Le istruzioni problematiche vanno tradotte. Normalmente le istruzioni del guest vengono gestite dal processore dell'host. Questo processore dell'host però è anche in grado di catturare le istruzioni problematiche, che NON può eseguire, e che rimanda all'hypervisor



# Virtualizzazione assistita dall'hardware

I livelli per le astrazioni sono tre. Come fa il processore a gestire questi tre livelli? Mediante una cosa chiamata RING (in realtà nei processori ci sono 4 ring), che fanno in modo che le istruzioni nel ring per il virtual kernel mode siano filtrate ed eseguite in una modalità o un'altra in base al fatto che siano sicure da eseguire direttamente o meno



Io dico abilità le interruzioni. A seconda di chi lo dice vanno, nel processore fisico, abilitate le interruzioni oppure no. Quindi se io sto eseguendo un hypervisor e non c'è il sistema operativo, il computer sa che io sto usando un hypervisor. Come fa a saperlo? So che sto nel ring zero. Ogni volta che c'è uno switch tra il sistema operativo e le applicazioni o tra il sistema operativo e l'hypervisor o tra l'hypervisor e le applicazioni c'è un cambiamento di questo ring, e quello che fa il processore quando deve eseguire un'istruzione dipende dal ring in cui si trova.



## Virtualizzazione del processore



### □ Ulteriori tecniche di virtualizzazione dei processori

#### ▪ virtualizzazione full

- combina l'esecuzione diretta (della maggior parte delle istruzioni) con la traduzione binaria (delle istruzioni "problematiche")

#### ▪ paravirtualizzazione

- l'OS guest viene modificato per eliminare tutte le istruzioni "problematiche" del suo kernel, sostituendole con chiamate all'hypervisor

Solo nel contesto linux. Non compatibile con Windows perché non si può riscrivere il SO a meno che non decida di farlo Windows stesso

- sono tecniche utilizzate soprattutto prima delle tecnologie hardware di virtualizzazione dei processori – la virtualizzazione dei processori x86 è iniziata alla fine degli anni '90



## Virtualizzazione di più processori

- ❑ La virtualizzazione dei processori è particolarmente efficace quando applicata a processori multi-core oppure a computer multi-processore Quello che posso fare è partizione il mio hardware fisico, limitando/gestendo le risorse assegnate alle macchine virtuali

- i processori fisici (con i loro core) dell'host vengono virtualizzati in CPU virtuali (*virtual CPU* o *vCPU*) e assegnati alle VM
  - ciascuna vCPU ha un solo core
  - ad ogni VM possono essere assegnate una o più vCPU
  - è anche possibile specificare delle quote
- in questo modo, un sistema multi-processore viene virtualizzato in un sistema multi-computer

Nel multiprocessore questi possono per esempio condividere memoria/dischi, mentre nel sistema multi computer ogni computer ha la propria memoria, il proprio disco. Quindi passiamo dall'esecuzione parallela al mondo distribuito



## - Virtualizzazione della memoria

A ciascuna macchina virtuale assegno delle zone di memoria della macchina fisica reale

- ❑ Nella virtualizzazione di sistema, la virtualizzazione della memoria centrale riguarda l'assegnazione e la gestione di aree di memoria alle VM

Quello delle zone di memoria assegnate da hypervisor e quello del sistema operativo

- è necessario gestire un doppio livello di virtualizzazione della memoria fisica – perché ogni VM ha una propria memoria virtuale (fornita dall'OS)
  - oggi i processori forniscono un supporto hardware alla virtualizzazione annidata della memoria – ad es., le tecnologie Intel EPT e AMD NPT (dal 2008)
- l'hypervisor deve anche garantire l'isolamento tra le aree di memoria assegnate alle diverse VM

- ❑ Gli hypervisor offrono anche delle tecniche specializzate per una gestione efficiente della memoria

- ad es., deduplicazione delle pagine e ballooning

Tecnica che serve a fare in modo che una macchina virtuale liberi un'area di memoria che possa essere usata da un'altra macchina virtuale, che non è banale. Normalmente nel sistema operativo la gestione della memoria di un singolo computer viene fatta così: ci sono tutte le pagine, si sa quando sono state accedute, quando c'è necessità di caricare in memoria una nuova pagina bisogna spostare in memoria secondaria quella utilizzata meno di recente. Supponiamo di voler allocare memoria per il lancio di una macchina virtuale in più rispetto ad alcune che già ho e voglio fare in modo che quelle già esistenti liberino memoria per la nuova. L'hypervisor quindi chiede delle cose a delle macchine virtuali in modo da liberare memoria



## - Virtualizzazione dell'I/O

Spesso nelle macchine virtuali di tipo server, tranne per l'accesso ai dischi e alla rete, non vengono usati dispositivi di IO in modo particolare, quindi non ci servirà particolarmente

- Di solito l'hypervisor non assegna alle VM i dispositivi hardware di I/O (come dischi e schede di rete) presenti fisicamente nell'host
  - l'hypervisor assegna a ciascuna VM dei dispositivi virtuali, che possono anche essere diversi da quelli presenti fisicamente sull'host e che sono configurabili separatamente per ciascuna VM Possono non corrispondere a dispositivi di IO fisici. L' hypervisor gestisce il mapping tramite un driver
  - l'hypervisor può anche assegnare alle VM dei dispositivi virtuali che non hanno una controparte fisica equivalente – ad es., uno switch virtuale
  - l'OS guest accede a questi dispositivi virtuali mediante i propri driver, come se fossero dispositivi reali
    - le operazioni di I/O per questi dispositivi virtuali vengono poi catturate dall'hypervisor, che le gestisce in modo opportuno – spesso è necessario utilizzare anche i driver dei dispositivi fisici

Qui c'è un problema di overhead a causa proprio della presenza di driver, ed è particolarmente problematico negli hypervisor di tipo 2

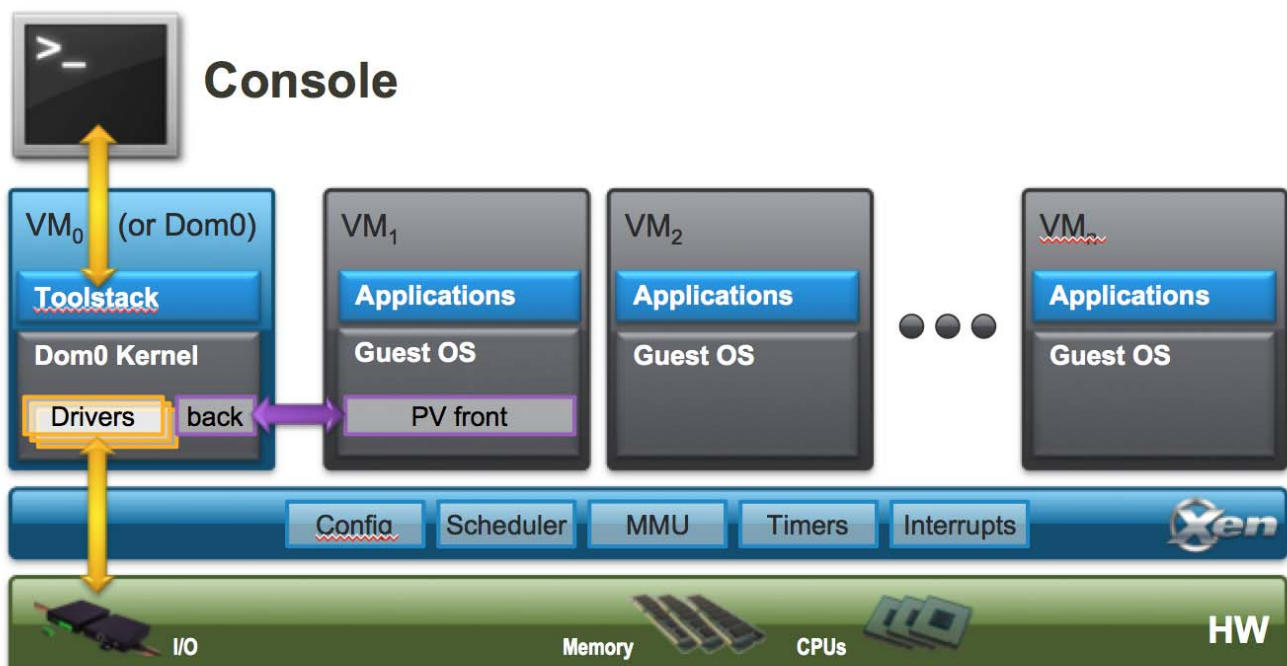
27

Macchine virtuali e virtualizzazione di sistema

Luca Cabibbo ASW



## Esempio – Xen e il “dominio 0”



28

Macchine virtuali e virtualizzazione di sistema

Luca Cabibbo ASW





## - Virtualizzazione dello storage

- ❑ La virtualizzazione dello storage ha l'obiettivo di astrarre lo strato fisico di memorizzazione persistente da quello delle VM
  - alcune possibili opzioni
    - un disco virtuale che corrisponde direttamente a un disco fisico oppure a una sua partizione
      - le prestazioni sono migliori
    - un disco virtuale implementato come un insieme di file dell'host – *file immagine (disk image files)*
      - la flessibilità è maggiore
  - in ogni caso, le VM vedono dei dischi virtuali

Ma è più macchinoso e quindi meno performante, c'è più overhead

Io definisco dei dischi utilizzati dalle macchine virtuali. Come si può fare? Alcune opzioni sono che il disco virtuale corrisponde direttamente al disco fisico o ad una sua partizione, e quindi accedere ad un disco vuol dire accedervi senza particolare mapping, quindi è alta la prestazione ma bassa la flessibilità perché se ho un disco e lo divido in dieci partizioni posso avere solo dieci macchine virtuali, o se c'è memoria che una macchina virtuale non usa ma è nella sua partizione rimane inutilizzata.

Oppure un'altra tecnica (molto flessibile ma le sue prestazioni sono peggiori): prevede che i dischi virtuali siano mappati su un insieme di file dell'host e quindi questo file cresce solo quando effettivamente il disco ha bisogno di accedere o di utilizzare più spazio. Se una macchina virtuale ha un disco da 100GB ma ne sta usando solo 10 nell'host vengono usati solo 10GB. Lo svantaggio qui sta nel fatto che quando faccio una lettura o una scrittura c'è una mappatura del file system ("scrivi in quel settore"), questa viene catturata da un driver che deve capire come mappare il settore sul file, poi va capito il settore fisico del disco... è molto macchinoso, c'è un overhead più significativo.



## Virtualizzazione dello storage

- ❑ La virtualizzazione dello storage può essere applicata
  - a unità direttamente collegate al computer host
    - unità DAS, Direct Attached Storage
  - a unità collegate in rete
    - unità SAN (Storage Area Network) – forniscono l'accesso a blocchi in unità remote
    - unità NAS (Network Attached Storage) – forniscono l'accesso a file in unità remote
  - la virtualizzazione basata su unità SAN/NAS aumenta la flessibilità

Il luogo dove sono memorizzati i dati potrebbe essere un'unità direttamente collegata all'host, ma questa è la soluzione meno utilizzata (se non per virtualizzazioni private), oppure delle unità collegate in rete utilizzabili da più host e da più guest, a cui si fa accesso mediante richieste in rete





# Virtualizzazione dello storage

Non sono COPIE, sono proprio spazi condivisi. I file risiedono sull'host e il guest vi può accedere

- ❑ Le **cartelle condivise (shared folder)** sono una funzionalità tipica degli hypervisor di tipo 2

- una o più cartelle condivise risiedono fisicamente nel file system dell'host – e vengono condivise tra l'OS host e una o più VM guest

Quando si parla di cartella condivisa si intende una cartella del file system dell'host che può essere acceduta sia in lettura che in scrittura da una o più macchine virtuali. Quindi posso agire sul contenuto del disco di una macchina virtuale agendo direttamente nell'host



## - Virtualizzazione della rete

- ❑ Una rete fisica

- un insieme di **host fisici** – ciascuno con una o più schede di rete fisiche (pNIC)
- uno o più **switch fisici (pSwitch)**, per connettere più segmenti di rete fisici

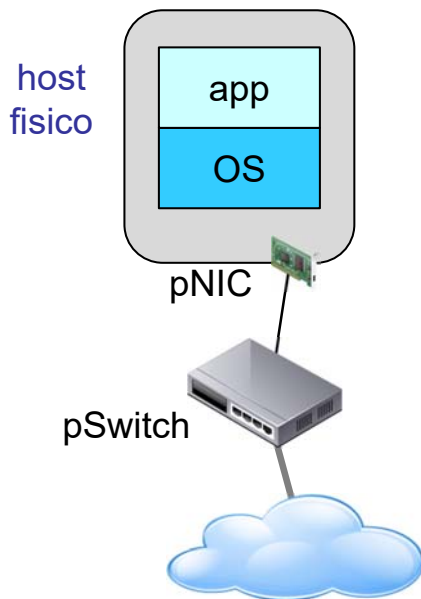
- ❑ Una **rete virtuale** (in prima approssimazione)

- un **insieme di VM** – ciascuna con una o più schede di rete virtuali (vNIC)
- uno o più **switch virtuali (vSwitch)**, per connettere le schede di **rete virtuali (vNIC) tra loro e con le schede di rete fisiche (pNIC)**
- per collegare le VM tra loro e con la rete a cui appartiene l'host, in modo opportuno

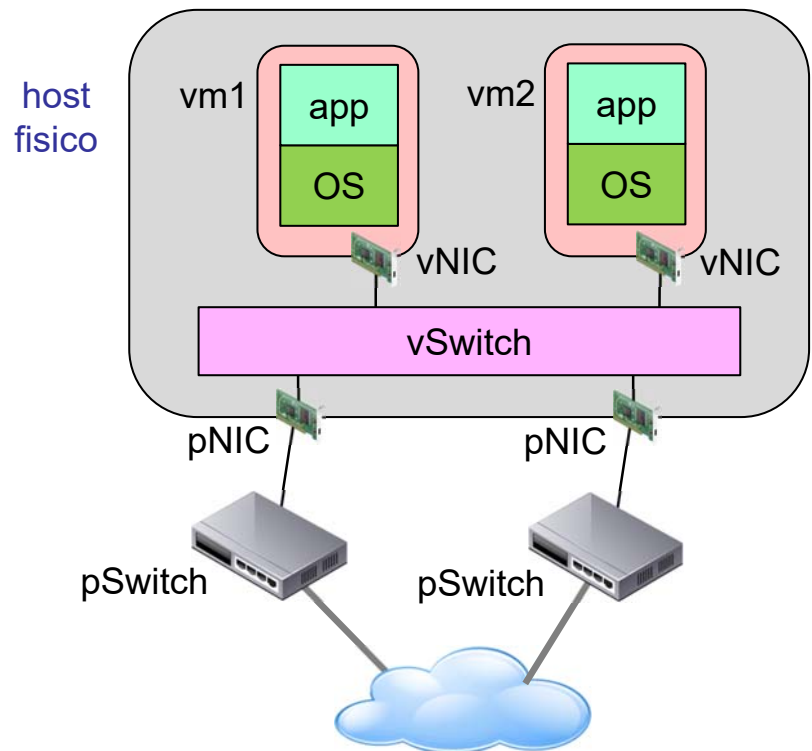


## Virtualizzazione della rete

### □ Una rete fisica



### □ Una rete virtuale (con un hypervisor di tipo 1)



33

Macchine virtuali e virtualizzazione di sistema

Luca Cabibbo ASW



## Virtualizzazione della rete

Valgono le seguenti affermazioni:

- Ogni VM può essere dotata di una o più schede di rete virtuali
  - ciascuna vNIC può emulare una certa scheda di rete reale comune – ma per favorire le prestazioni vengono spesso usate delle vNIC paravirtualizzate (ad es., virtio-net)
  - ciascuna vNIC può operare in una modalità di virtualizzazione differente (descritte dopo)
  - l'indirizzo IP di una vNIC può essere configurato in modo statico oppure in modo dinamico tramite DHCP (che potrebbe essere fornito dell'hypervisor)
  - è possibile creare delle configurazioni di rete complesse

34

Macchine virtuali e virtualizzazione di sistema

Luca Cabibbo ASW



- ❑ Le principali modalità in cui può operare una vNIC – ogni vNIC può operare in una modalità differente dalle altre
  - **NAT** (Network Address Translation)
    - la VM guest vede la rete esterna tramite la vNIC
  - **Bridged Networking**
    - la vNIC è collegata a una pNIC, e scambia pacchetti con rete esterna (ad es., Internet) direttamente tramite di essa
  - **Internal Networking**
    - per collegare un gruppo di VM guest tra di loro e creare una rete di VM
  - **Host-only Networking**
    - per definire una rete che contiene l'host e un insieme di VM guest



## Virtualizzazione della rete

- ❑ Il **port forwarding** mette in corrispondenza una porta di una VM guest con una porta dell'host
  - ad es., la porta 80 (HTTP) di un guest viene collegata con la porta 8080 dell'host – in modo che tramite la porta 8080 dell'host sia possibile accedere alla porta 80 di quel guest
  - è un modo comune per rendere accessibili i servizi in esecuzione in una VM guest all'host oppure alla rete esterna

Ha lo scopo di collegare una porta della vm con una porta dell'host, in modo che le richieste che l'host riceve su quella porta siano mappate sulla porta della vm. Nota che le due porte, seppur corrispondenti, non devono avere lo stesso numero, quindi una richiesta che arriva all' host sulla porta 8080 può essere mappata sulla porta di una vm che ha un altro numero



## - Immagini e istanze di macchine virtuali

- ❑ Un'**istanza** di macchina virtuale (**VM instance**) è un'entità **dinamica**, che ha un proprio stato, che può cambiare nel tempo
  - un'istanza di VM può essere effettivamente in esecuzione in un certo host Lo stato della istanza della vm è parte della definizione della istanza della vm stessa
  - lo stato di un'istanza di VM comprende lo stato di tutte le sue risorse, in un certo istante di tempo – ad es., lo stato dei suoi dischi, della memoria e dei registri delle sue vCPU
- ❑ Un'**immagine** di VM (**VM image**) è invece un'entità **statica**
  - un'immagine di VM è formata dai metadati della VM (ad es., numero di vCPU, quantità di memoria e MAC address delle schede di rete), insieme al contenuto dei volumi/dischi della VM
  - un'immagine di VM può essere rappresentata mediante uno o più file, in un formato opportuno
  - un'immagine di VM non può essere in esecuzione  
È presa di solito quando l'istanza della VM è spenta, se la volessi a VM accesa allora si chiamerebbe snapshot

37

Macchine virtuali e virtualizzazione di sistema

Luca Cabibbo ASW



## Immagini e istanze di macchine virtuali

- ❑ Che relazione c'è tra immagini di VM e istanze di VM?
  - un'istanza di VM può essere creata facilmente a partire da un'immagine di VM E posso anche avviarla perché ho il disco quindi posso passare da una immagine a una o più istanze (se voglio più istanza uguali posso partire dalla stessa immagine)
    - ad es., su Amazon EC2, si può creare una VM selezionando un tipo di istanza (ad es., A1.large) e un'immagine di VM (chiamata un'AMI, Amazon Machine Images, ad es., l'AMI Linux Ubuntu 24.04 per x64)
    - lo stato di un'istanza di VM può essere salvato come immagine di VM – con diverse finalità
    - ad es., per poter creare facilmente nuove VM a partire da quell'immagine

38

Macchine virtuali e virtualizzazione di sistema

Luca Cabibbo ASW



## - Clonazione di VM

Quello che creiamo non è quindi un vm identica, ma una vm con un indirizzo MAC diverso, alcuni parametri vengono ricalcolati o possono essere definiti separatamente

- ❑ La **clonazione** di una VM è la creazione di una nuova istanza di VM a partire da un'immagine di VM
  - per evitare di installare “da zero” l'OS e i servizi e le applicazioni di interesse di una VM
  - non è una semplice copia dell'immagine di una VM
  - da un'immagine di VM è possibile creare molte istanze di VM



## Virtual appliance

- ❑ Una **virtual appliance** è un'immagine di VM pre-configurata (in genere da terzi) da cui è possibile creare istanze di VM con quella configurazione
  - queste immagini vengono in genere rese accessibili in un repository pubblico o privato, in un formato opportuno (ad es., VMDK di VMware oppure VDI di VirtualBox)
  - la disponibilità di virtual appliance può ridurre in modo significativo i tempi di creazione delle VM
  - “installare un'applicazione, un server o una piattaforma complessa è semplice come scaricare un'app nel proprio smartphone”



## - Snapshot/checkpoint



- Una VM può essere avviata e arrestata – ma anche messa in pausa e riavviata
  - lo stato di una VM arrestata o in pausa può essere salvato come *snapshot* (o *checkpoint*) per un uso futuro
    - questo stato comprende lo stato del disco, lo stato della memoria e lo stato dei registri dei processori
  - è anche possibile avviare una VM a partire da uno snapshot – per ridurre i tempi di avviamento di una VM



## - Migrazione di VM



- La *migrazione* ha lo scopo di spostare un'istanza di VM in esecuzione da un host fisico a un altro
  - non sempre è accettabile spegnere la VM nel primo host e riavviarla nel secondo host
  - può essere meglio mettere in pausa la VM, prenderne uno snapshot, copiarlo sul secondo host e riavviare la VM sul secondo host a partire dallo snapshot
    - si può anche evitare la copia, se lo snapshot viene salvato su un'unità SAN/NAS condivisa dagli host
    - se lo storage della VM è gestito in un'unità SAN/NAS condivisa tra gli host, lo snapshot può limitarsi al solo stato della memoria – e la migrazione può essere estremamente veloce (*live migration*)



## - Interfacce per la gestione di VM

- ❑ Le operazioni per la gestione delle VM – come creazione, configurazione, avvio e arresto – possono essere gestite
  - tramite una GUI o una console web – in modo manuale
  - tramite un'interfaccia di tipo CLI o REST – anche mediante degli script
    - questo sostiene la gestione automatizzata delle VM

Quando uso un sistema di virtualizzazione normalmente c'è una console che mi consente di fare le varie cose (creare, avviare vm ecc). Questa non è l'unica interfaccia per le applicazioni di virtualizzazione, ci sono anche interfacce CLI o REST prive di interfacce grafiche



## - Discussione

*recap a 1h24min*

- ❑ Alcune conseguenze della virtualizzazione di sistema
  - è possibile eseguire in modo fedele un'applicazione o servizio in una VM
  - la virtualizzazione può sostenere alcune qualità
    - flessibilità – per il rilascio flessibile di sistemi software distribuiti in ambienti virtuali
    - sicurezza – le VM sono isolate tra loro e dall'host
    - disponibilità – ad es., la creazione e l'avvio rapido di VM
  - la virtualizzazione ha anche degli inconvenienti
    - c'è un overhead sulle prestazioni – ma può essere mantenuto basso



- ❑ Descriviamo brevemente alcuni sistemi di virtualizzazione per la piattaforma x86
  - Xen
  - KVM
  - la famiglia di prodotti VMware
  - Oracle VM VirtualBox



## - Xen



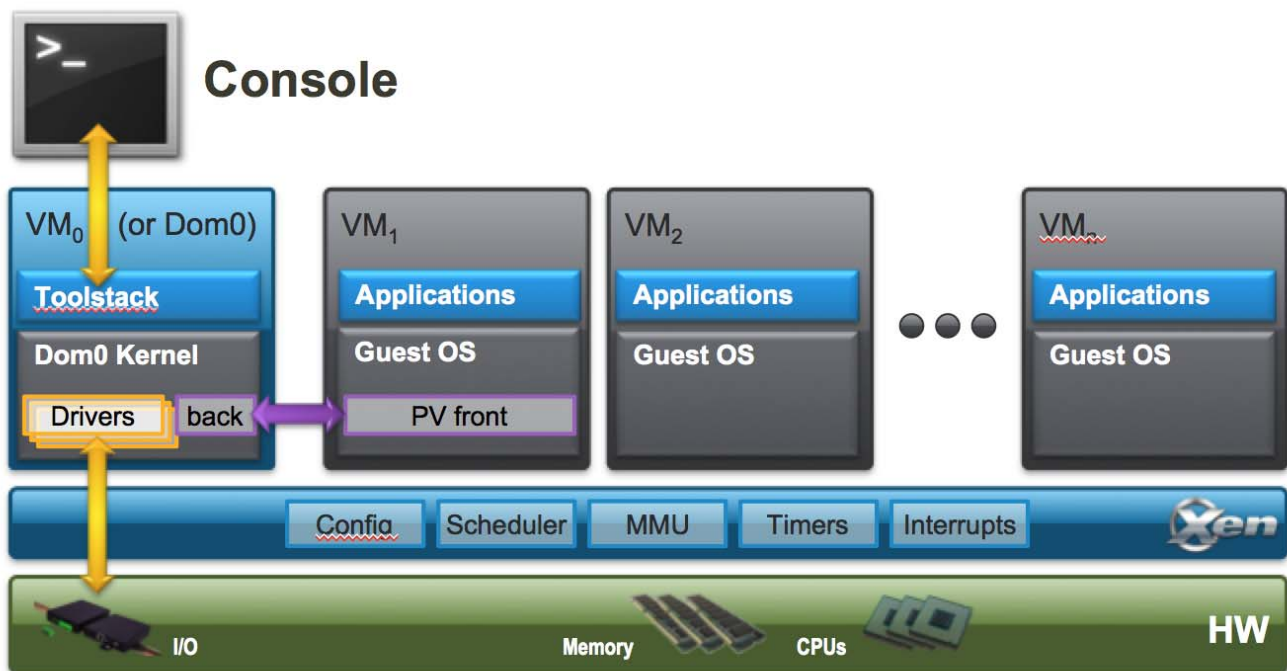
- ❑ Xen è un hypervisor di tipo 1 open source per sistemi x86
  - supporto per più OS guest, soprattutto Linux (e altri OS Unix) ma anche Windows
  - supporta sia la paravirtualizzazione (PV) che la virtualizzazione assistita dall'hardware (HVM)
  - un progetto di ricerca alla fine degli anni novanta, poi diventato un progetto open source nel 2002
  - dal 2013, un “collaborative project” della Linux Foundation – i membri comprendono Amazon, Google, Oracle, Intel e AMD
  - secondo Wikipedia, è usato come hypervisor primario in molti sistemi – tra cui Amazon EC2







## □ Architettura di Xen



47

Macchine virtuali e virtualizzazione di sistema

Luca Cabibbo ASW



## □ Architettura di Xen

- basata su un hypervisor sottile – questo sostiene robustezza e sicurezza
- ogni VM è chiamata un guest o dominio
- il dominio 0 (o dominio di controllo) è un dominio speciale (con privilegi speciali)
  - contiene i driver per l'hardware fisico, e supporta l'hypervisor nell'accesso all'hardware
  - contiene uno stack software di controllo (toolstack) per gestire la creazione, configurazione e distruzione delle altre VM – che può essere acceduto dalla linea di comando, da un'interfaccia grafica o da altri stack per l'orchestrazione di VM
- XenServer è una piattaforma di virtualizzazione per il cloud basata sull'hypervisor Xen

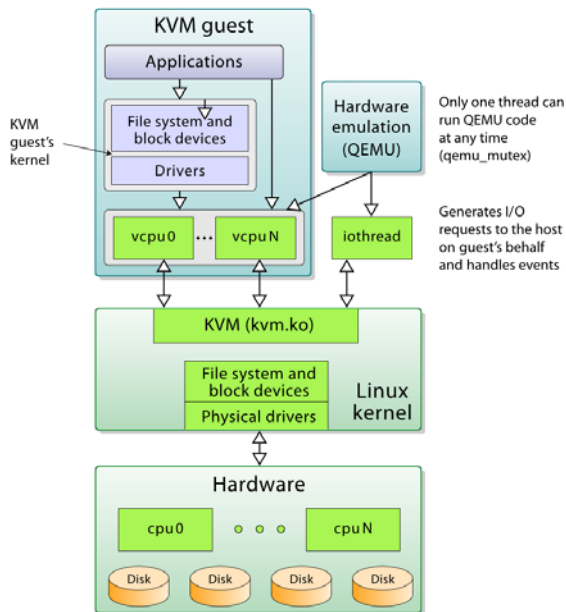
48

Macchine virtuali e virtualizzazione di sistema

Luca Cabibbo ASW



- ❑ KVM (Kernel Virtual Machine) è una soluzione di virtualizzazione open source per sistemi x86 (con estensioni per la virtualizzazione) integrata nei kernel Linux – può essere considerato un hypervisor di tipo 1
  - supporto per OS guest Linux e Windows non modificati



49

Macchine virtuali e virtualizzazione di sistema

Luca Cabibbo ASW



- ❑ Architettura di KVM
  - basata su un modulo del kernel Linux (kvm.ko) che fornisce il nucleo dell'infrastruttura di virtualizzazione
  - inoltre QEMU – che è un hosted hypervisor per la virtualizzazione dell'hardware (da non confondere con la virtualizzazione assistita dall'hardware) basato su traduzione binaria – viene usato come ambiente per l'esecuzione dei guest KVM
    - ove possibile, il codice guest viene eseguito direttamente dall'host
  - ogni vCPU delle VM guest è gestita come un thread dell'OS host
  - è possibile interagire con le capacità di virtualizzazione di KVM mediante libvirt – una API comune per Linux per gestire e controllare VM in modo sicuro e anche remoto

50

Macchine virtuali e virtualizzazione di sistema

Luca Cabibbo ASW



- VMware è una società (sussidiaria di EMC) con una ricca offerta di tecnologie per la virtualizzazione per piccole, medie e grandi aziende, che comprende

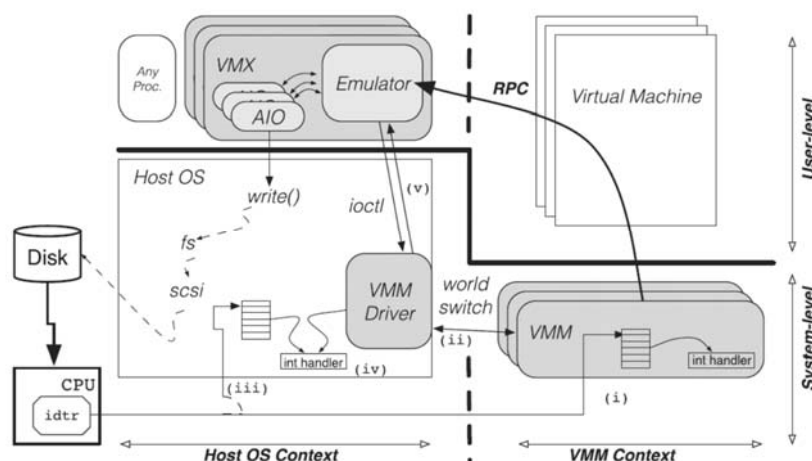
- prodotti per la virtualizzazione di singoli computer – come gli hypervisor di tipo 2 VMware Workstation e Fusion (Pro e Player)
- prodotti per la virtualizzazione dei data center e di gestione del cloud – come vSphere (una suite di prodotti, con l'hypervisor di tipo 1 ESXi e il control plane vCenter) e vCloud Suite (comprende funzioni per la disponibilità, l'automazione e la gestione di VM, per fornire un cloud privato)
- prodotti per la virtualizzazione del desktop – come Horizon
- la prima versione di VMware Workstation è stata rilasciata nel 1999, la prima versione di ESX server nel 2001



## VMware Workstation



- L'architettura di VMware Workstation è basata su tre componenti principali (la figura mostra a sinistra il contesto dell'OS host e a destra il contesto dell'hypervisor)
- VMM (virtual machine monitor) è l'hosted hypervisor
- VMX è l'interfaccia utente nel sistema host
- il VMM driver viene installato come driver nell'OS host – ma in realtà guida il VMM e lo nasconde all'OS host





- ❑ Oracle VM VirtualBox è un prodotto di virtualizzazione per sistemi x86 per uso enterprise oppure personale (dal 2007)
  - un hypervisor di tipo 2, per OS host Windows, Linux e MacOS, e per OS guest Windows e Linux
  - un progetto open source controllato dalla Oracle
  - supporta numerose tecniche e opzioni di virtualizzazione
  - le VM possono essere create mediante una GUI oppure mediante una interfaccia dalla linea di comando (VBoxManage)
  - le VM possono essere accedute localmente o remotamente
  - un uso comune è quello delle VM pre-costruite per sviluppatori
    - è possibile sperimentare stack software complessi installando solo VirtualBox e scaricando una singola virtual appliance pre-definita



## \* Applicazioni e benefici della virtualizzazione di sistema

- ❑ Discutiamo brevemente le applicazioni della virtualizzazione di sistema e i suoi benefici



## Applicazioni della virtualizzazione

### ❑ Server consolidation

- si consideri un sistema software distribuito composto da più servizi e server – ciascun server è in esecuzione su un computer (fisico) differente
  - ci sono buoni motivi per usare più computer separati
  - è però una soluzione costosa e difficile da gestire – ad es., è difficile il dimensionamento dei singoli computer
- nella **server consolidation** i diversi server vengono eseguiti in VM differenti – in uno o più computer fisici virtualizzati
  - la virtualizzazione di sistema realizza un'infrastruttura dinamica basata su un pool di risorse computazionali
  - l'hypervisor garantisce l'isolamento tra le diverse VM
  - questo porta a un utilizzo maggiore delle risorse e a una flessibilità maggiore – ed anche a risparmi significativi
  - l'affidabilità dell'hardware può peggiorare

55

Macchine virtuali e virtualizzazione di sistema

Luca Cabibbo ASW



## Applicazioni della virtualizzazione



### ❑ Altre applicazioni comuni della virtualizzazione

- fornire un ambiente di esecuzione a un'applicazione legacy (application consolidation) – ad es., a seguito della migrazione a una nuova piattaforma hardware/software
- creare ambienti di esecuzione multipli, ciascuno con il proprio OS e un proprio stack software
  - per supportare lo sviluppo di sistemi software distribuiti
  - per supportare il testing e la QA (quality assurance), in ambienti multipli e separati
- eseguire applicazioni non sicure (sandboxing)
- desktop (client) virtualization
  - consente agli utenti di accedere al proprio desktop virtuale da un computer (client) qualunque
- nell'hosting di servizi web
- nel contesto del cloud computing

56

Macchine virtuali e virtualizzazione di sistema


Luca Cabibbo ASW



- ❑ Ecco i principali benefici offerti dalla virtualizzazione
  - riduzione dei costi
  - miglioramento delle qualità delle applicazioni
    - disponibilità e tolleranza ai guasti
    - efficienza, agilità, produttività e flessibilità dell'IT
    - isolamento e sicurezza
    - estendere la vita delle applicazioni
  - semplificazione della gestione dei datacenter
    - provisioning di risorse e VM semplificato e velocizzato
    - supporto alla scalabilità e all'elasticità
    - gestione centralizzata
    - datacenter definito tramite software
  - supporto allo sviluppo, al testing e alla QA
  - ridurre il vendor lock-in e favorire la migrazione al cloud



## \* **Macchine virtuali e rilascio del software**

- ❑ Le VM sono un'opzione di rilascio per i sistemi software distribuiti
  - ogni VM incapsula uno o più servizi software, insieme allo stack software necessario per quei servizi
- ❑ Ma come gestire queste VM?
  - **approccio "tradizionale"**
    - creare ciascuna VM in modo manuale, installandoci il software e i servizi di interesse sempre in modo manuale
    - le VM vengono considerate semplicemente la versione virtuale di computer fisici
  - **un approccio moderno e migliore** Completamente automatizzato
    - costruire **automaticamente** le immagini di VM di interesse Mai a partire da zero
    - creare le VM a partire da queste immagini  è anche possibile creare più VM a partire da ciascuna immagine, per replicare i servizi corrispondenti



## Benefici

### ❑ Benefici nell'usare le VM per il rilascio del software

- il rilascio è semplice e affidabile – il rilascio di un servizio viene gestito come la creazione di una VM a partire dall'immagine relativa a quel servizio
- isolamento dei guasti e sicurezza – ogni VM (con i relativi servizi) viene eseguita in isolamento
- le VM possono essere rilasciate sia nel cloud che on premises, in un data center privato
- la creazione e l'avvio di una VM (a partire da un'immagine di VM) richiedono in genere da pochi secondi a pochi minuti (meno che un computer fisico)



## Inconvenienti

### ❑ Inconvenienti nell'usare le VM per il rilascio del software

- è possibile un uso poco efficiente delle risorse – ogni servizio o gruppo di servizi richiede un'intera VM
  - Se frammento troppo i servizi la moltitudine di VM che uso introduce un overhead che può diventare pesante
  - questa inefficienza aumenta se ogni VM viene usata per un singolo servizio leggero – ma rilasciare più servizi in una singola VM riduce l'isolamento dei guasti
- overhead nell'amministrazione di sistema delle VM – chi crea la VM (o la sua immagine) è responsabile di effettuare anche gli aggiornamenti del software che vi è installato
- la creazione e l'avvio di una VM (a partire da un'immagine di VM) richiedono in genere da pochi secondi a pochi minuti (più che un container)





## \* Discussione

- ❑ La virtualizzazione di sistema consente a un computer “reale” di ospitare più computer (macchine) “virtuali” – ciascuna VM può essere usata per eseguire un proprio OS e dei propri servizi e applicazioni
  - la virtualizzazione di sistema si basa su varie tecniche di virtualizzazione – per virtualizzare risorse computazionali diverse
  - la virtualizzazione di sistema ha numerose applicazioni, e consente diversi benefici
  - in particolare, favorisce la definizione e la gestione di ambienti di esecuzione virtuali – on premises e nel cloud – con l’obiettivo di ottimizzare l’utilizzazione delle risorse hardware, di fornire flessibilità operativa, nonché di isolare tra loro le applicazioni e gli ambienti