Note sulla Virtualizzazione

Luca Battistin

febbraio 2024

Abstract

In queste note viene prima presentata una brevissima introduzione alla virtualizzazione in generale, per poi approfondire le macchine virtuali implementate su PC mediante hypervisor di tipo 2 e quelle implementate nei data-center mediante hypervisor di tipo 1. Si riassumono i principali vantaggi della virtualizzazione e si elencano i diversi modelli di servizi cloud (SaaS, PaaS, IaaS).

Contents

1 Introduzione

Il termine *Virtuale* compare in molte tecnologie informatiche e noi l'abbiamo già incontrato nei termini VLAN, VPN, memoria virtuale, JVM oltre che nelle macchine virtuali create mediante VirtualBox (che saranno oggetto di questo approfondimento). Rivediamo brevemente queste tecnologie, a cui aggiungiamo anche le *router subinterfaces*, per mettere in evidenza gli aspetti comuni relativi alla virtualizzazione.

Virtual LAN : è *come se* lo switch venisse sezionato in diverse parti; ovvero si crea una separazione logica delle interfacce in domini di broadcast differenti.

Virtual Private Network : è *come se* stendessimo un cavo privato tra due punti della rete mentre, di fatto, si usa una connessione pubblica promiscua e la si rende privata (o riservata) a livello logico, mediante la crittografia.

memoria virtuale : è *come se* la RAM diventasse più grande (per accogliere nuovi processi), ma di fatto l'estensione è solo logica, grazie ad un software del sistema operativo che, parcheggiando temporaneamente in memoria di massa le pagine meno usate, libera spazio per altri processi.

Java Virtual Machine è *come se* il bytecode fosse eseguito da un processore universale, indipendente dalla architettura fisica: è proprio la JVM a tradurlo poi per l'hardware specifico su cui è installata.

router subinterfaces è *come se* l'interfaccia del router venisse divisa in più interfacce (logiche) indipendenti a cui viene indirizzato uno specifico traffico identificato dal "vlan id".

In tutte le precedenti descrizioni è stato messo in evidenza il comportamento **virtuale** reso possibile da uno strato software che *astrae* le risorse hardware permettendone un uso più versatile. Il prezzo da pagare è l'**overhead** dovuto all'esecuzione del software di controllo.

2 Macchine Virtuali

una VM (Virtual Machine) è una istanza virtualizzata delle risorse hardware di un computer che è in grado di svolgere (quasi) tutte le funzioni dell'hardware fisico tra cui l'esecuzione dei sistemi operativi e quindi delle applicazioni.
L' **Hypervisor**, detto anche *virtual machine monitor* è quel software (quindi un processo) che crea e gestisce le VM. Esso permette alla stessa macchina fisica di supportare più macchine virtuali.
Come si vede in figura 1 ci sono due tipi di hypervisor:

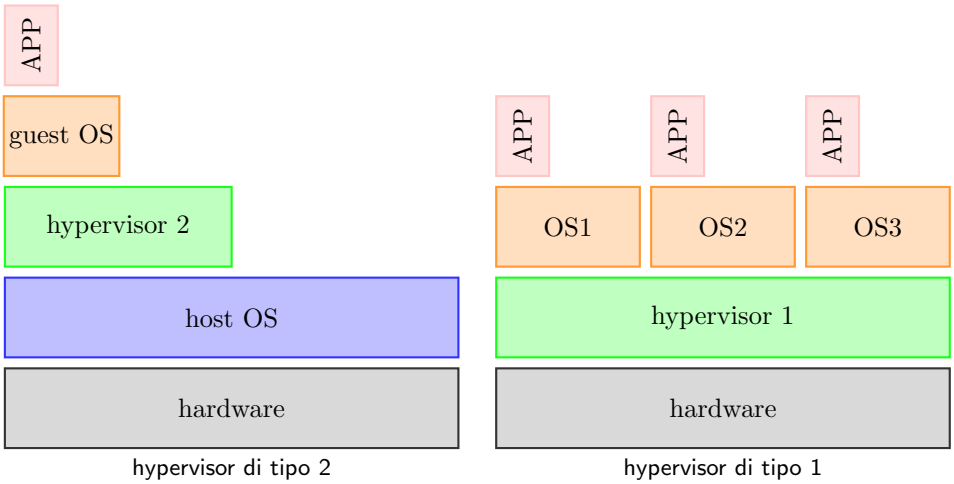

Figure 1: Hypervisor di tipo 1 e di tipo 2

hypervisor di tipo 2 detto anche *hosted* perché si appoggia ad un sistema operativo *HOST*[1] al quale richiede le risorse per poter creare le VM. Questa architettura è tipica nei sistemi PC dove l'utente può creare facilmente ambienti di test. Esempi di questo tipo sono VirtualBox, VMware player, Parallels Desktop for Mac, linux KVM[2]

hypervisor di tipo 1 detto anche *bare metal* perché si trova direttamente sopra l'hardware ed è tipico delle architetture server, soprattutto nei datacenter o nelle server-farm. vedi figura 2. Esempi di questo tipo sono VMware ESXi, Xen, Oracle VM Server, Microsoft Hyper-V,

Negli schemi della figura 1, per non appesantirli, non sono state indicate le macchine virtuali, ovvero le risorse hardware create e gestite dagli hypervisor. Nella figura 2, che mostra in maggior dettaglio l'architettura di un sistema con hypervisor 1, tipica di una server-farm, vengono riportate anche le VM (Virtual Machine)[3] oltre a mettere in evidenza una struttura **iper-convergente** dove

[1] il termine **host** ha una doppia valenza: può significare *ospitante* oppure *ospitato*, a seconda del contesto. Ciò avviene anche nel corrispondente termine italiano **ospite**, infatti essi condividono la radice etimologica *hŏstis*, straniero, e sia l'oste che l'ospite sono vicendevolmente stranieri. In questo caso il sistema operativo HOST è quello ospitante la virtual machine, mentre il sistema operativo ospitato è indicato come GUEST.

[2] Kernel-based Virtual Machine (KVM) di Linux e bhyve di FreeBSD sono moduli del kernel[5] che in pratica trasformano un sistema operativo host in un hypervisor di tipo-1 [wikipedia]. Pertanto KVM può essere usato sia come tipo 1 che come tipo 2.

[3] Il termine Virtual Machine viene in questo caso inteso come l'insieme delle risorse hardware virtualizzate dell'hypervisor. In altri contesti lo stesso termine sta ad indicare l'insieme delle risorse hardware (virtualizzate) e software: ovvero l'intero sistema di elaborazione il cui hardware è virtualizzato.

l'hardware gestito dall'hypervisor è dato da rack di server, storage e connessioni di rete.

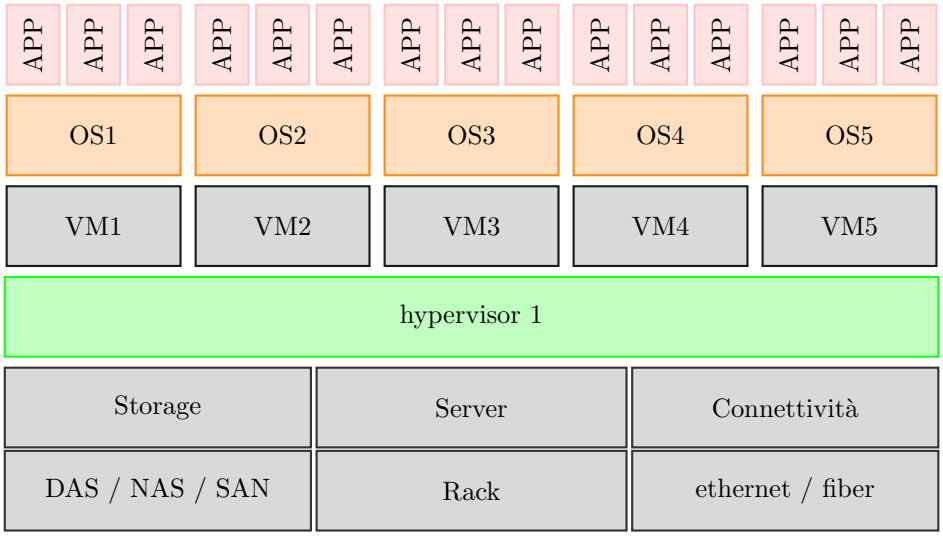

Figure 2: dettaglio hypervisor di tipo 1

3 Vantaggi della virtualizzazione

Come già accennato, il maggior svantaggio della virtualizzazione è l'overhead necessario per il processo hypervisor. I vantaggi sono però numerosi e, soprattutto nelle architetture server, spesso irrinunciabili. Sintetizziamo di seguito i principali:

ottimizzazione delle risorse. L'hypervisor bilancia le risorse disponibili tra le diverse macchine virtuali *on demand* permettendone un impiego più efficiente. Se le macchine fossero "fisiche" ognuna dovrebbe essere dimensionata in base al carico massimo e buona parte delle risorse rimarrebbe inutilizzata per la maggior parte del tempo. Di conseguenza, anche il costo totale dell'infrastruttura viene notevolmente ridotto.

Backup/restore più facile e veloce. La macchina virtuale (VM), quando è spenta, è di fatto un file, quindi è facile farne degli *snapshot*[4] e archiviarli. Quando, per attacchi o mal configurazioni, la VM dovesse corrompersi, risulta relativamente facile rimettere in piedi uno degli snapshot salvati. Per lo stesso motivo risulta molto facile avere delle copie della stessa VM.

[4]Snapshot significa letteralmente *istantanea*. Quando si crea lo snapshot di una VM, viene copiata e archiviata un'immagine della macchina virtuale in un determinato stato.

isolamento Ogni macchina virtuale definisce un ambiente di esecuzione separato (sandbox) da quelli delle altre; ciò implica la possibilità di effettuare testing di applicazioni preservando l'integrità degli altri ambienti. Inoltre aumenta la **fault tollerance** perché eventuali attacchi da parte di malware o spyware sono confinati alla singola VM.

Disaster Recovery e Business Continuity decisamente migliori. Questo vantaggio è in buona parte conseguenza dei precedenti che, aggiunti alla possibilità di spostare le VM *a caldo* da un hardware all'altro, permettono la "sopravvivenza" almeno dei servizi vitali.

4 Storage

In relazione alla figura 2 è bene chiarire i termini relativi allo storage:

DAS (Directed Attached Storage). È la soluzione tipica nei server di piccole dimensioni (come, ad esempio il nostro v-learning): i dischi sono direttamente connesso al server tramite SATA[5] o altre interfacce ad alta velocità, come SCSI[6] o SAS[7].

NAS (Network Attached Storage). È un dispositivo di archiviazione, composto da uno o (più frequentemente) più dischi, collegato alla rete, anziché ad un singolo server. Ha pertanto un suo sistema operativo (spesso una distribuzione linux customizzata) che offre a tutti gli altri computer della rete risorse di archiviazione indipendentemente dal loro sistema operativo. Ideale per una realtà aziendale di piccole o medie dimensioni

SAN (Storage Area Network). È una rete (al alta velocità - es. Gigabit ethernet) di dispositivi di archiviazione. Rispetto al NAS offrono prestazioni più elevate in termini di velocità, di capacità, di fault tollerance (a fronte di un maggior costo). Sono la soluzione ideale per grosse realtà aziendali o server FARM

Le precedenti soluzioni di archiviazione sono quasi sempre organizzate in **RAID** (Redundant Arrays of Independent Disks)[8] schiere di dischi fisici indipendenti organizzati in modo più o meno ridondante. Le configurazioni in cui tali dischi si possono trovare sono molte; vediamo le principali:

[5] Serial ATA; bus tipico anche dei sistemi PC

[6] SCSI Small Computer System Interface. Interfaccia standard per il trasferimento di dati in modalità parallela. Si pronuncia "scasi"

[7] Serial Attached SCSI (SAS) è una tecnologia o interfaccia di trasferimento dati, evoluzione della SCSI, studiata per lavorare sia con dispositivi ad accesso diretto, come i dischi fissi, sia per quelli ad accesso sequenziale, come i nastri magnetici [Wikipedia]

[8] Originariamente nella sigla RAID la I stava per Inexpensive secondo l'articolo del 1988 di by David Patterson, Garth A. Gibson, and Randy Katz dell'università della California, Berkeley: "A Case for Redundant Arrays of Inexpensive Disks (RAID)", presented at the SIGMOD Conference

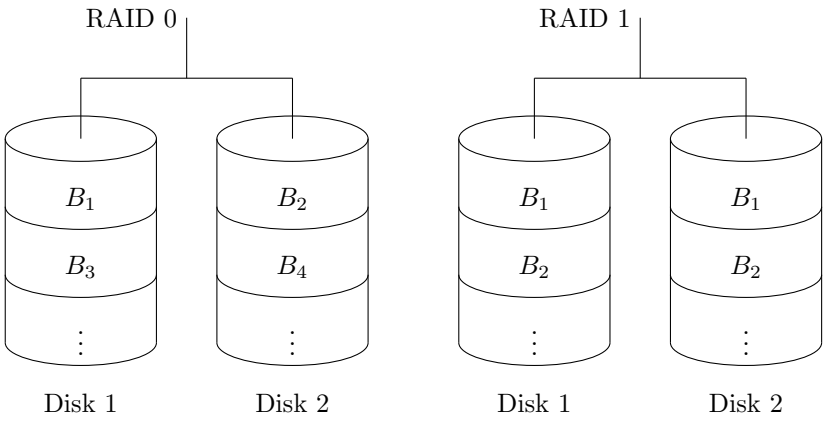

Figure 3: RAID 0: stripping and RAID 1: mirroring

RAID 0 (stripping): i dati sono scomposti in blocchi (o strisce) nei diversi dischi in modo da aumentare la velocità di accesso che avviene in modo parallelo. Vedi figura 3 di sinistra. Tanti più dischi ci sono tanto più aumenta la velocità, oltre alla capacità. In questo caso non c'è alcuna ridondanza.

RAID 1 (mirroring): i dati sono replicati completamente, ovvero, ogni disco ha una sua copia. Vedi figura 3 di destra. Questa soluzione è fortemente ridondante quindi, rispetto alla precedente ha capacità dimezzata e velocità notevolmente minore. È adatta per applicazioni critiche dove l'integrità dei dati è prioritaria

RAID 0 e RAID 1 sono due configurazioni contrapposte tra le quali si possono classificare tutte le altre. Le due vie di mezzo più utilizzate sono:

RAID 5 (necessita di almeno 3 dischi). Vedi fig 4. Implementa un compromesso da fault tollerance e prestazioni operando lo stripping su $n-1$ blocchi in parallelo e calcolando la parità (**parity**) sul blocco n-esimo. Nella maggior parte delle configurazioni RAID 5, la parità è calcolata con lo XOR dei dati delle altre strisce (stripes) ed è memorizzata du dischi diversi. Per la sua versatilità, il RAID 5 è una delle configurazioni più comunemente usate.

RAID 10 È la composizione di diversi RAID 1 che formano un sistema RAID 0. È costituito da almeno 4 dischi di cui due in stripping e due in mirroring. Più in generale è composto da 2n dischi, n dei quali in stripping. Combina i due vantaggi: stripping e mirroring al prezzo di dover impiegare il doppio della capacità hardware.

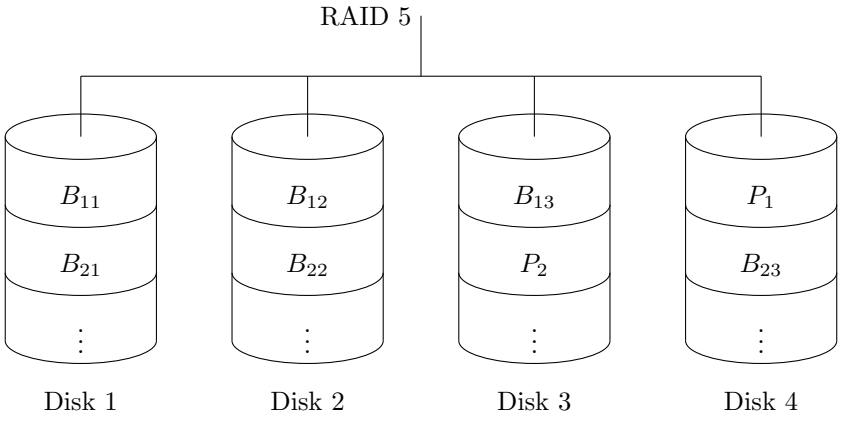

Figure 4: RAID 5: stripping and parity

5 Cloud computing

La virtualizzazione e la connettività hanno favorito il **cloud computing** ovvero lo spostamento in remoto delle risorse hardware e software con dei vantaggi notevoli quali l'accessibilità a dati e risorse di calcolo da qualsiasi dispositivo, la facilità di condivisione, l'abbattimento dei costi iniziali e di gestione (si pensi ad esempio al backup o al mantenimento e aggiornamento dell'hardware). Si classificano i servizi cloud secondo tre modelli:

SaaS (Software as a Service - detto anche Pay Per Use) : il servizio mette a disposizione un applicativo che, mediante una interfaccia web, offre le medesime funzionalità dei programmi per PC. Praticamente ogni applicazione Desktop ha la sua controparte SaaS ma, per portare un esempio classico, si pensi alle suite di office automation.

PaaS (Platform as a Service) : il servizio mette a disposizione una intera piattaforma sulla quale l'utente può installare le applicazioni che preferisce. Esempi tipici sono le macchine virtuali messe a disposizione da Azure o AWS.

IaaS (Infrastructure as a Service) : il servizio mette a disposizione risorse hardware on demand sulle quali l'azienda cliente può costruire la infrastruttura di cui necessita.

Lo svantaggio principale del cloud computing è il fatto di non avere completo controllo sui propri dati e apparati ovvero di dover riporre la fiducia nell'azienda che offre il servizio. Inoltre, il costo mensile potrebbe non essere vantaggioso sul lungo periodo.