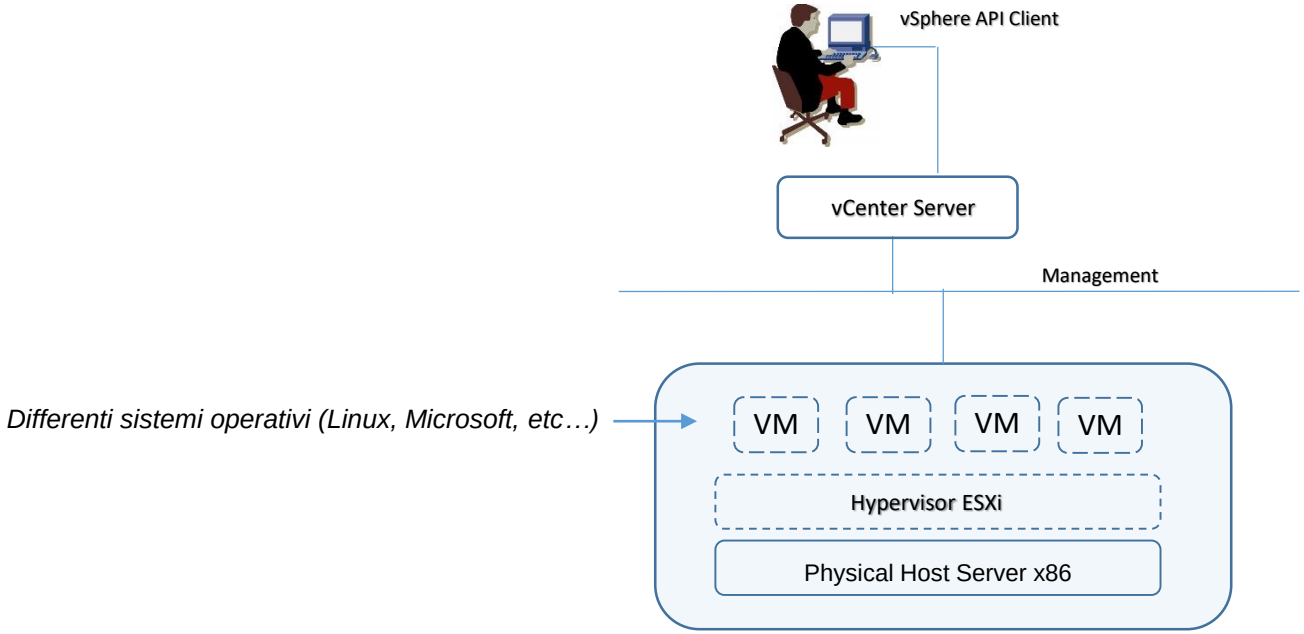
Few notes about network data center technologies virtualizations

Massimiliano Sbaraglia

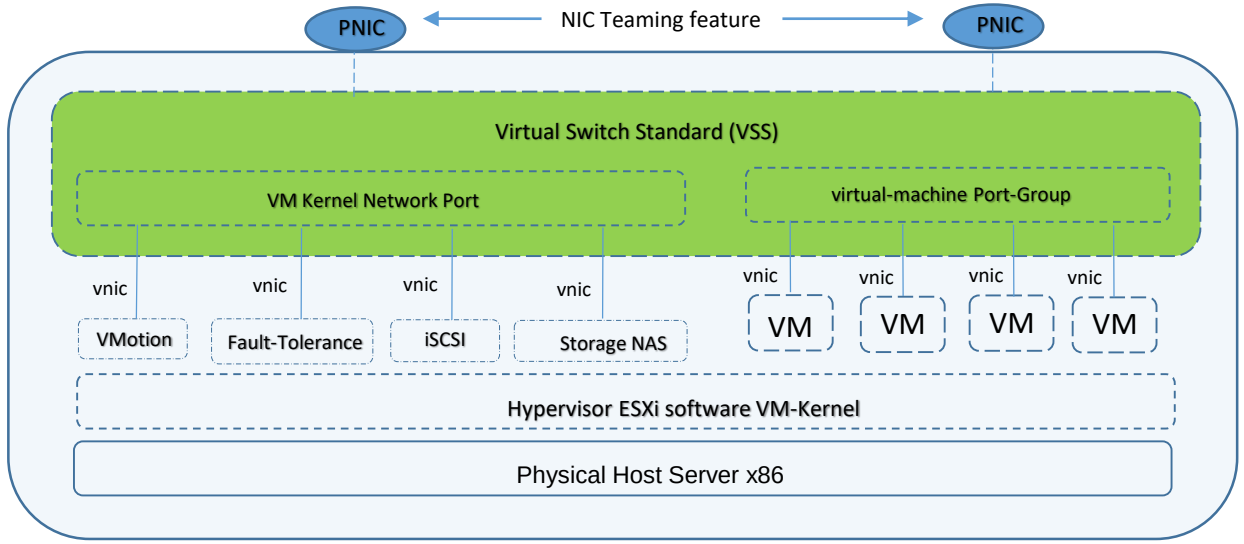
Cosa è ESX ed ESXi

- ESX è una piattaforma hypervisor di gestione dei server virtuali (VM) attraverso una consolle di management del sistema operativo (vm-kernel); ESX è stato sostituito da ESXi
- ESXi (Elastic Sky X integrated) ha le stesse funzionalità di un ESX ma la gestione dei server virtuali è demandata non più ad una consolle di management interna ma ad un vCenter Server VMware con vSphere licence e le sue API (Application Programming Interface)



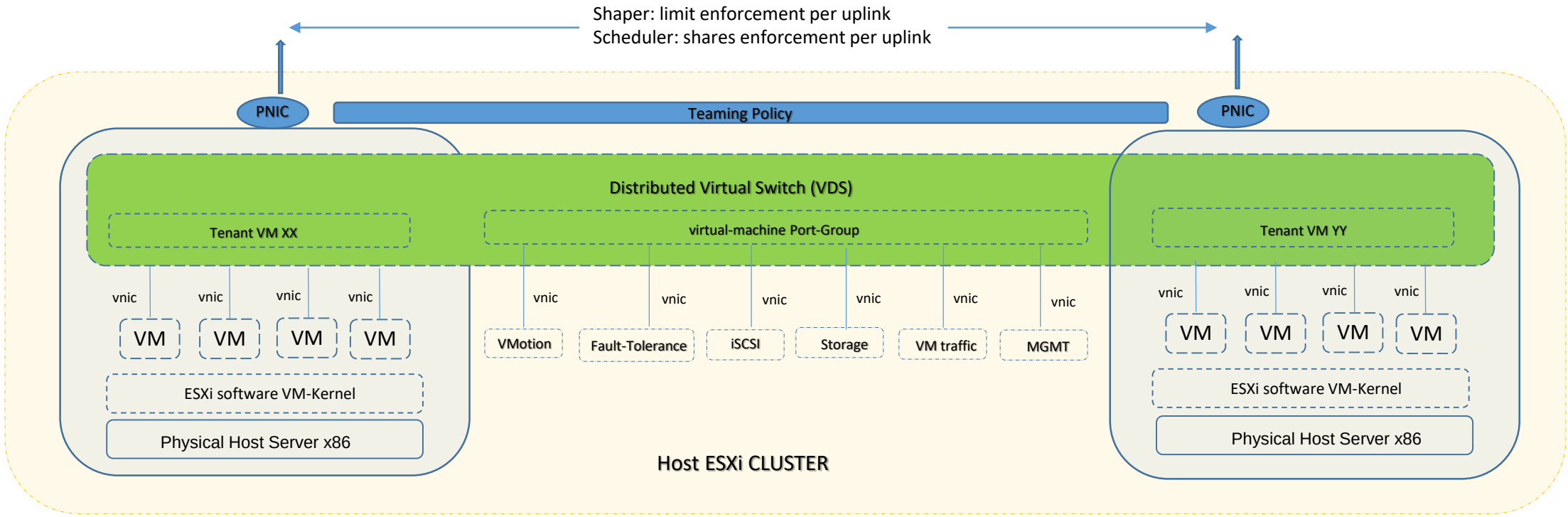
Cosa è un Virtual Switch

- Un Vswitch è una applicazione software che permette la configurazione di trasmissione dati (forwarding packets) tra differenti Virtual Server (VM) e permette un collegamento verso l'esterno per mezzo di una physical port (pnic)
- Il port-group permette di differenziare tipologie di traffico passanti per il vswitch (setting di vlans)
- VM kernel network port provvede all'accesso allo stack TCP/IP e possiamo creare nuove vmkernel port per gestire funzionalità quali vmotion, FT, iSCSI e Storage

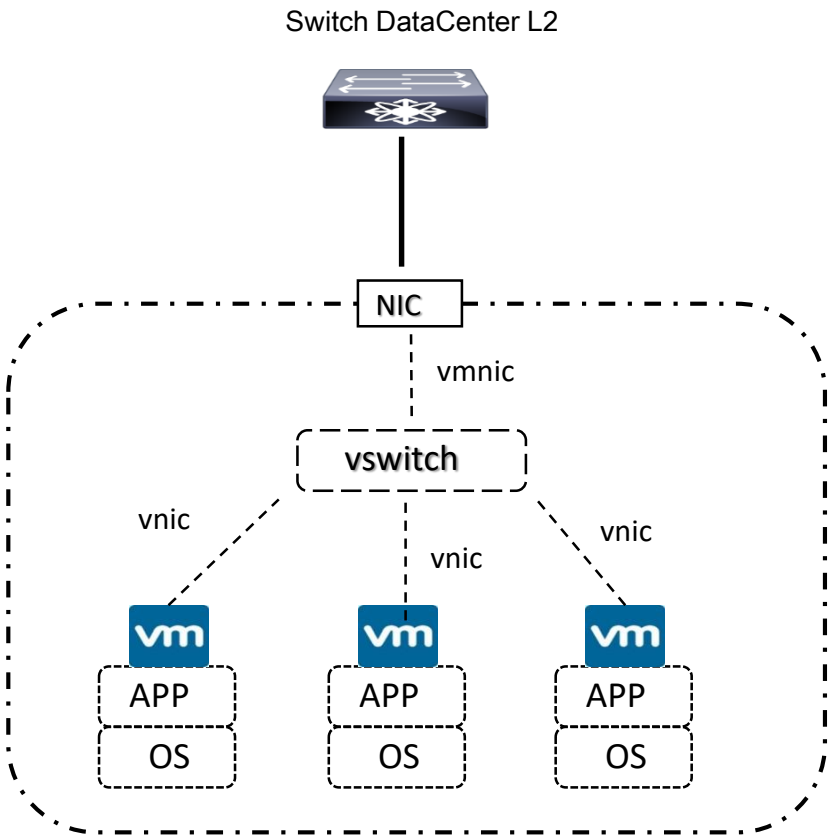


Cosa è un Distributed Virtual Switch

- Un Distributed Virtual Switch è una applicazione software che permette la configurazione di trasmissione dati (forwarding packets) tra differenti Virtual Server (VM) attraverso più Physical ESXi in cluster



Cosa è un Virtual Machine



Virtual Machine

- Una VM (Virtual Machine) emula un server fisico per sistema operativo, applicazioni, IP address e collegamento verso una rete (vnic)
- Vmware ha introdotto il concetto di vswitch (virtual switch) che altro non è che un Hypervisor che emula tutte le funzionalità di un vero layer 2 switch
- Questo vswitch provvede a collegamenti di tipo access ports verso le VM (vnic) e collegamenti uplinks verso physical NIC (collegamento definite vmnic) permettendo 802.1q tagging e MAC address table per trasmettere frame Ethernet basate sul loro valore di destination MAC
- Un vswitch offre configurazioni di tipo port-group; un port-group può contenere vlan-id, security feature, shaping definendo percentuali di banda utilizzabile e NIC teaming (vmnic load-balancing, network failover detection, switch notification, failure behavior)
- Cisco ha introdotto Nexus 1000V quale element virtuale che emula le funzionalità di un distribute vswitch vmware DVS attraverso proprie API (Application Programmable Interface) rilasciate attraverso NX-OS vCenter operations

Cosa è un NSX VMware

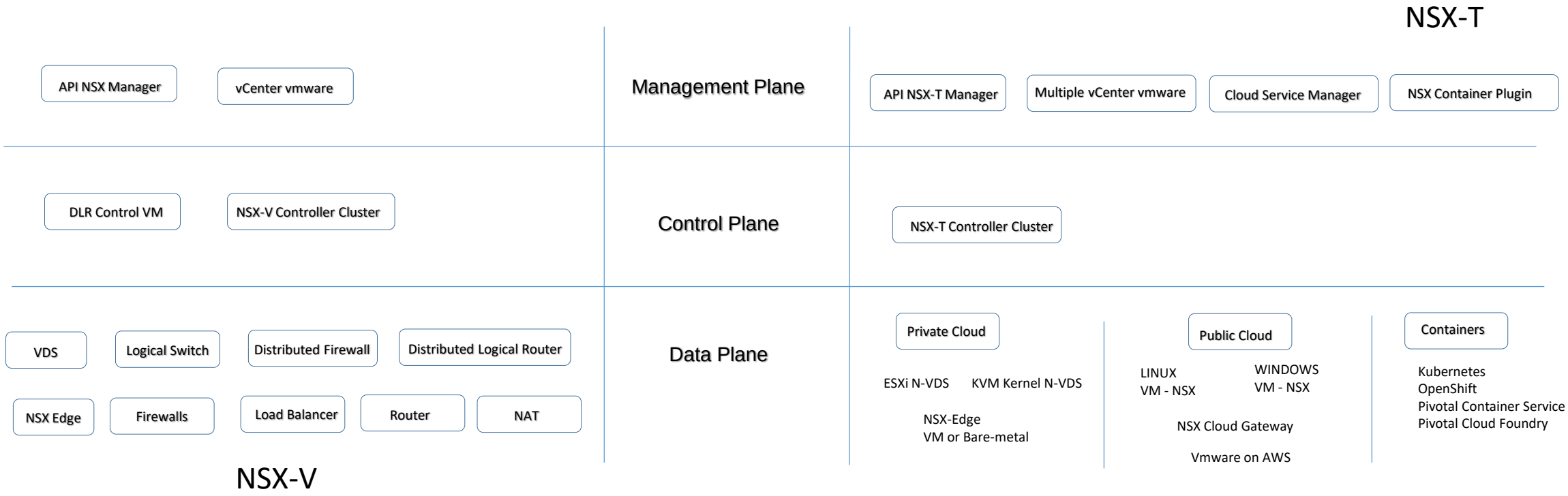
- NSX è una piattaforma Vmware virtuale per la configurazione di ambienti di networking e security attraverso famiglie di prodotti quali vCNS (virtual Cloud Networking Security) i quali virtualizzano servizi layer 4-7 ed NVP (Network Virtualization Platform) che virtualizzano servizi layer 2-3
- NSX Software-Defined è parte del cloud Vmware datacenter SDDC micro-segmentation, il quale offre computing VM attraverso tecnologie virtuali
- NSX offre una serie di porte logiche per firewalls, switches, routers, balancers in modo da abilitare networking devices attraverso dedicati hypervisor
- Logical switches utilizzano domini VXLAN per creare un overlay di livello 2 al quale collegare applicazioni e tenants di VM
- Distributed routers sono impiegati per la funzionalità di routing tra virtual network layer 3 via hypervisor kernel
- Distributed stetefull firewall sono impiegati la creazione di custom policies applicate a virtual interface card (vnic), garantendo logiche di sicurezza
- Logical balancer offrono servizi layer 4-7 per la gestione di traffico di rete a livello applicativo; sono inclusi servizi quali SSL (Secure Sockets Layer) offload e controllo di salute dei servers (health check)
- NSX offre la configurazione di VPN site-to-site, Remote-Access oltre che VPN per cloud gateway services
- NSX Edge Gateway è una VM che si comporta come un appliance per funzionalità di L3 routing, firewalling, VPN site-to-site, load balancing, etc; questa funzionalità supporta VXLAN to VLAN bridging
- API (Application Programming Interface) utilizza REST per semplificare la configurazione di terze-parti devices con relativi servizi di rete e per integrare NSX con un cloud management per maggiori capacità di automazione
- NSX operation prevede CLI centralizzato, SPAN (switch port analyzer), IPFIX (IP flow information export), ARM (application rule management), Vrealize Suite per monitoraggio proattivo, analisi e troubleshooting

Cosa è un NSX VMware

- NSX Dynamic Security Policy permette di assegnare regole di network e sicurezza alle applicazioni di rete attraverso un Service Composer, inoltre permette di creare dinamicamente gruppi ai quali associare dedicati filtri, oggetti, tag e Active Directory role
- NSX nativamente integra cloud management attraverso vRealize Automation e OpenStack per cloud management
- Cross-VC NSX permette di indirizzare piani di migrazione datacenters, performare long-distance vMotion, performare disaster recovery (DR) attraverso Vcenter – Vsphere (orchestration tools) Site Recovery Manager (SRM)
- NSX integra via vRealize Log Insight la possibilità di ricevere log dal nodo ESXi, utilizza i contenuti dei pacchetti per processare le informazioni ed analizza eventuali problematiche durante i deployment
- NSX Manager è un componente centrale per la gestione della rete; può essere rilasciato come VM in uno ESXi server gestito da un vCenter (OVA template)
- NSX Manager per vSphere si basa su Photon OS (simile a vCenter server appliance), oppure può lavorare su Ubuntu
- NSX Controller gestisce tutta la piattaforma virtuale di network e gestisce informazioni circa VMs, hosts, switches e vxlan; configurarlo in cluster garantisce ridondanza in caso di guasto di un singolo controller
- NSX Edge è il punto di uscita che provvede al collegamento di una rete esterna fisica; può essere installato come un distributed virtual router oppure come un service gateway. Possono essere previsti servizi quali dynamic routing, firewalls, NAT, DHCP, VPN, Load Balancing, High Availability

Cosa è un NSX-V ed NSX-T

- NSX-V è dedicato per lavorare con vSphere e progettato in modo tale che ogni singolo NSX-V manager platform sia legato ad un solo Vcenter vmware server instance; è ideale per la connettività di rete delle VM ed offre delle capacità di carico di lavoro difficili da ottenere con una piattaforma hardware di tipo fisico.
- NSX-T è un multi-hypervisor aware SDN e provvede a fornire servizi di networking, security, automation per nuove framework applicative ed architetture con eterogenei endpoints:
- NSX-T è idoneo per lavorare con cloud-native application, bare-metal workload, cloud-public e private ed ambienti multi-cloud

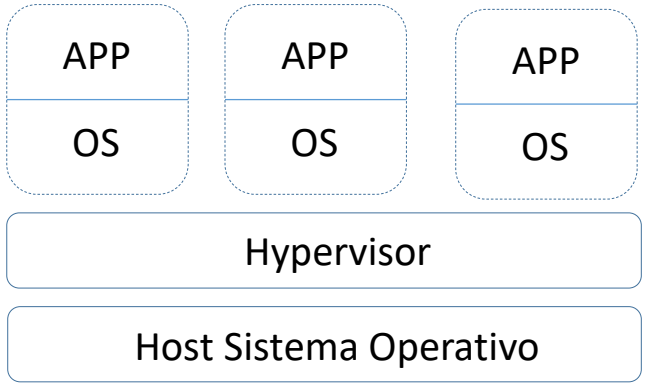


Cosa è un Container

- Un Container è un insieme di immagini applicative distinte, isolate dal resto del sistema operativo pur condividendo il kernel ossia la parte che gestisce le risorse software con l'hardware del client
- Il Container Linux che contiene una applicazione dove sono presenti le librerie, le dipendenze ed i file necessari
- Il Container quindi nasce per separare e virtualizzare dei processi in un ambiente modificato (tipo chroot) in modo tale che ogni tipo di accesso (filesystem, user, etc…) non potesse compromettere l'intero sistema
- Il Container presente tecnologie quali i gruppi di controllo (cgroups) i quali sono una feature del kernel per controllare e limitare l'uso di risorse da parte di un determinato processo; i cgroups utilizzano un sistema (systemd) di inizializzazione che configura lo spazio utente e ne gestisce i processi
- Il Container utilizza tecniche di virtualizzazione come lo spazio dei nomi dei kernel (ID di processo o nomi di rete), lo spazio dei nomi utente (ID user ed ID groups a livello di spazio dei nomi)
- Il Container Linux è chiamato anche LXC
- Altri Container come Docker consente maggiori capability come quella di invio delle immagini e di versioning, agevola la suddivisione delle applicazioni nei vari processi e mette a disposizione strumenti per farlo
- Kubernetes (K8s) è una piattaforma opensource che consente di gestire cluster di host su cui vengono eseguiti Container Linux su cloud pubblici o privati o ibridi.
- Kubernetes si integra con reti, storage, security per mettere a disposizione una infrastruttura di Container completa ed utilizza un sistema di Orchestration

Differenza grafica tra concetto di virtualizzazione e Container

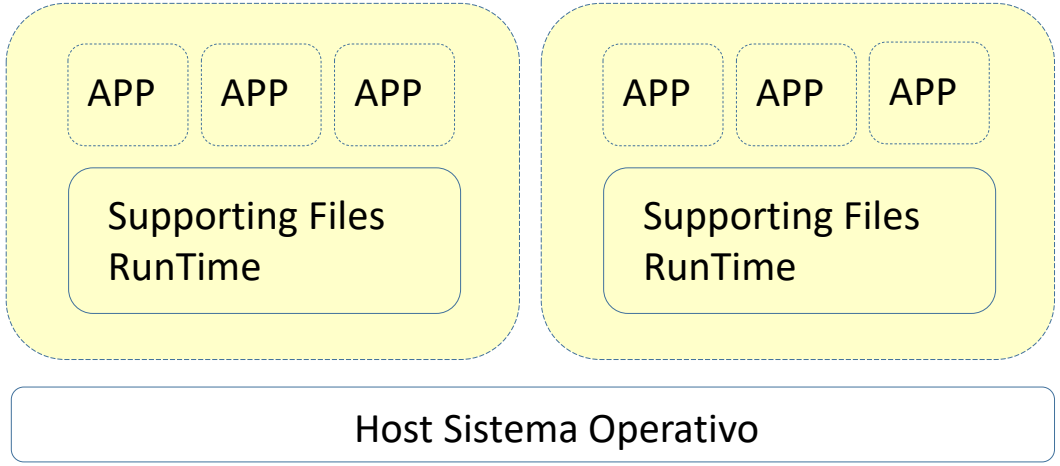
Concetto di Virtualizzazione VMware



Consente di eseguire più sistemi operativi contemporaneamente su un singolo sistema hardware
Viene utilizzato un hypervisor per emulare la parte hardware del sistema operativo

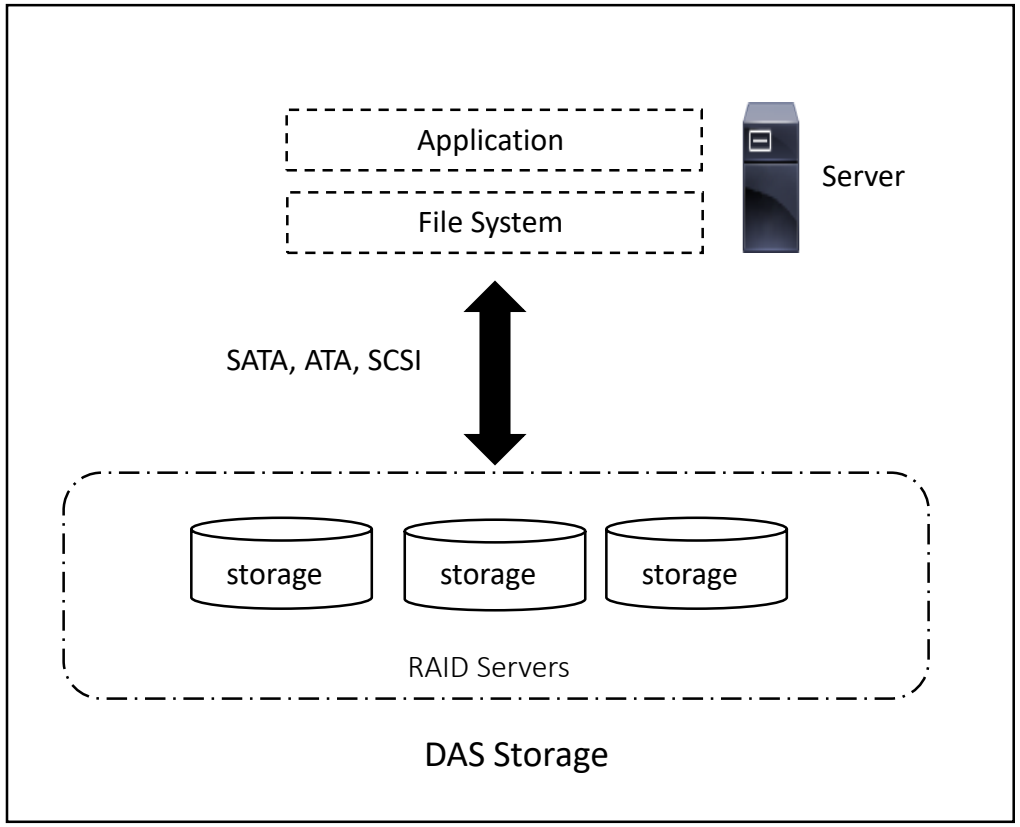
CONTAINER #1

CONTAINER #2



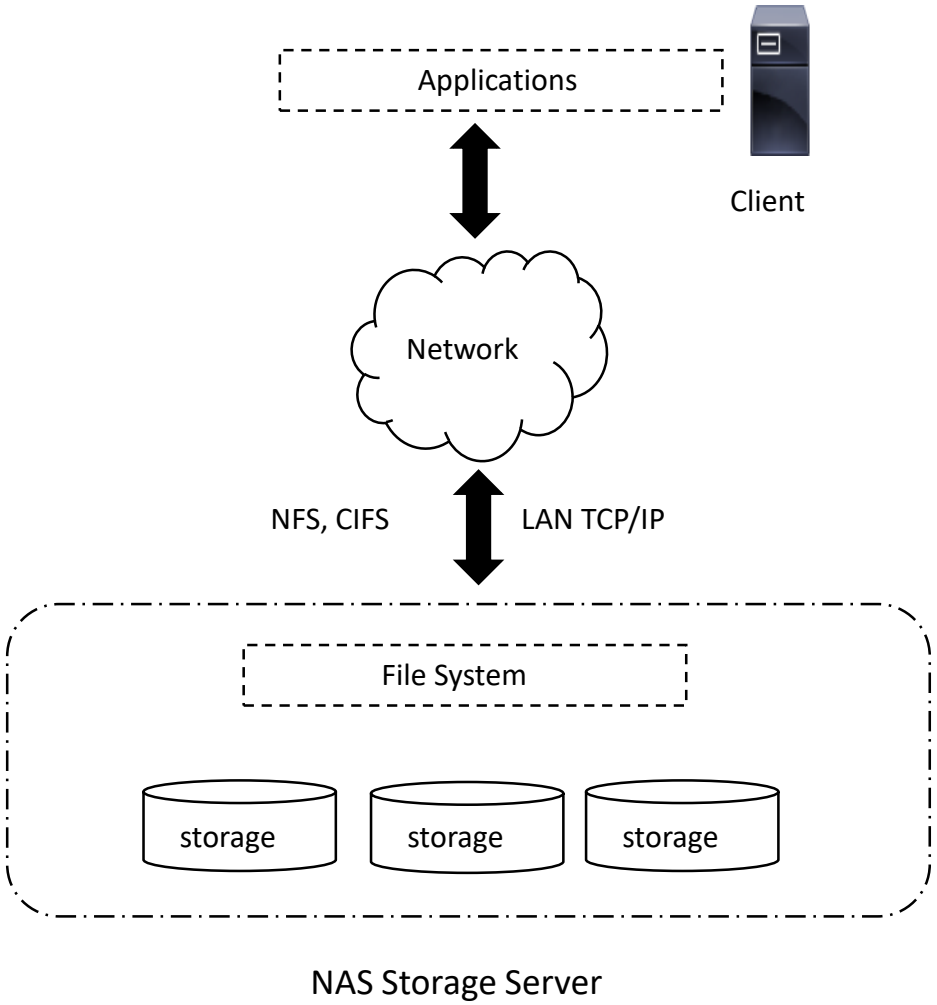
I Container condividono lo stesso kernel del sistema operativo ma isolano i processi applicativi dal resto del sistema
(esempio i sistemi Linux eseguono un container x.86 Linux, i sistemi windows eseguono un container x.86 windows, etc)

Cosa è un DAS



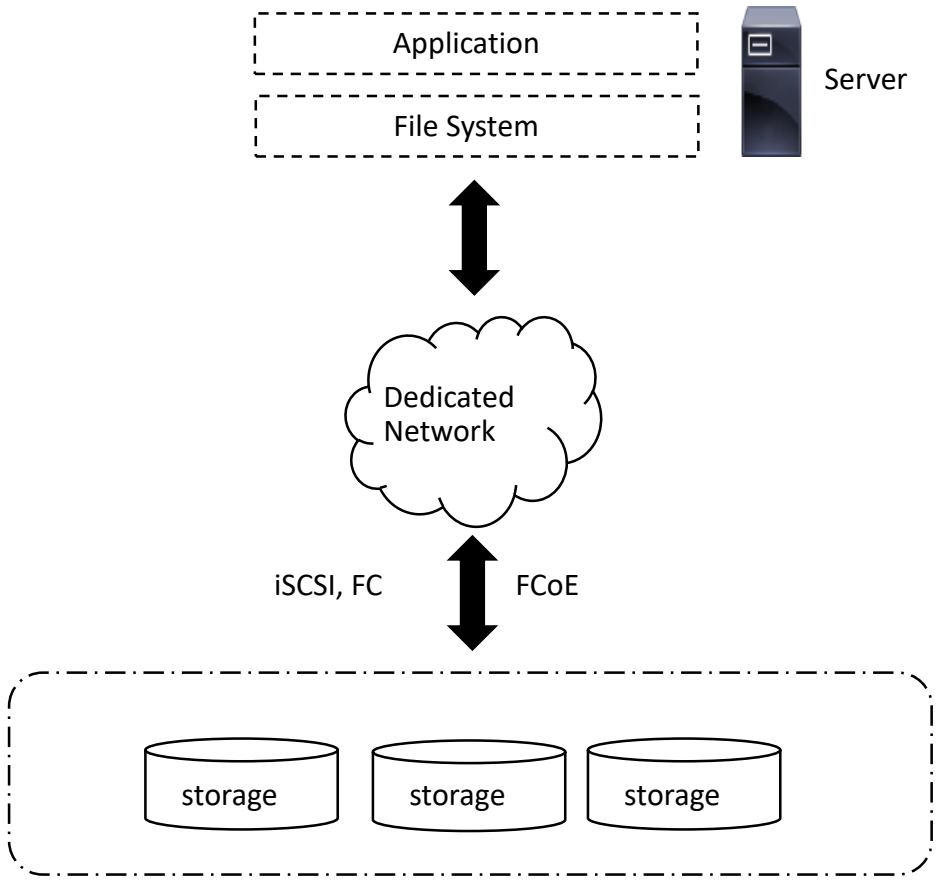
- Un DAS è uno storage sub-system direttamente collegato via cavo al server
- Hard Disk, Solid Drive, Optical Hard Drive, External Drives
- Può essere compost da un RAID (Redundant Array Indipendent Disk) combinando multipli hard drive all'interno di una unità logica di dischi
- Non esiste nessuna Network tra il collegamento di un sistema DAS ed un Server (nessuno switch, router, bridge, etc..)
- Protocolli quali ATA, SATA, SCSI, SAS, USB e FC permettono il collegamento di sistemi DAS

Cosa è un NAS



- Un NAS è un file-level storage server collegato attraverso una rete (network) e provvede all'accesso dei dati in modo etereogeneo
- L'accesso ai dati, consolidato per sistemi UNIX è il protocollo NFS (network File System) e per i sistemi Windows (Microsoft) è il protocollo CIFS (Common Internet File Sustem)
- I NAS sono gestibili via browser digitando un indirizzo IP della rete
- Un NAS ha una interfaccia di rete per il collegamento alla rete aziendale
- I NAS sono indicati per lo scambio di piccolo quantità di informazioni ed il protocollo TCP/IP si presta bene a questa funzionalità.

Cosa è una SAN



SAN Storage

- Un SAN prevede una rete di switch dedicata per l'accesso dei dati tra blocchi di Servers
- La connessione verso devices di rete SAN è possibile grazie ad una estensione definita in una HBA (Host Bus Adapter)
- I protocolli impiegati sono iSCSI, FC, FCoE
- Una SAN si adatta bene ad ambienti dove lo scambio di dati è di grandi dimensioni (Terabyte di dati)
- Le SAN sono dotate di sistemi di protezione dei dati e ridandanza di hardware per evitare interruzioni di servizio
- L'assenza di interruzioni di servizio è garantita dalla presenza di una rete di tipo lossless Ethernet, indispensabile per il trasporto di pacchetti SCSI incapsulato dentro pacchetti Fiber Channel over Ethernet
- In una SAN vi sono I concetti di VSAN, Zoning (WWN World Wide Name) e LUN (Logical Unit Number to Server)

Cosa è un IaaS, PaaS, SaaS

- Premessa i componenti su cui si poggia una piattaforma cloud sono:
    - Spazio anche conosciuto come Storage composto da un NAS (Network Attached Storage), da una SAN (Storage Area Network) oppure da una architettura dedicata
    - Nodi di gestione processi di elaborazione virtualizzata
    - Controller per la migrazione dei dati

- **IaaS** significa Infrastructure as a Service dove si mettono a disposizione risorse hardware virtualizzate con lo scopo di creare una infrastruttura via cloud da parte dell'utente finale, senza sapere dove sono collocate queste risorse
- Esempio di IaaS:
    - EC2 (Amazon Elastic Cloud Compute)
    - S3 (Amazon Simple Storage Service)
    - VPC (Amazon Virtual Private Cloud)
    - AWS (Amazon Web Service)
    - Google Cloud Engine
    - Google Cloud Storage
    - Oracle
    - Etc…

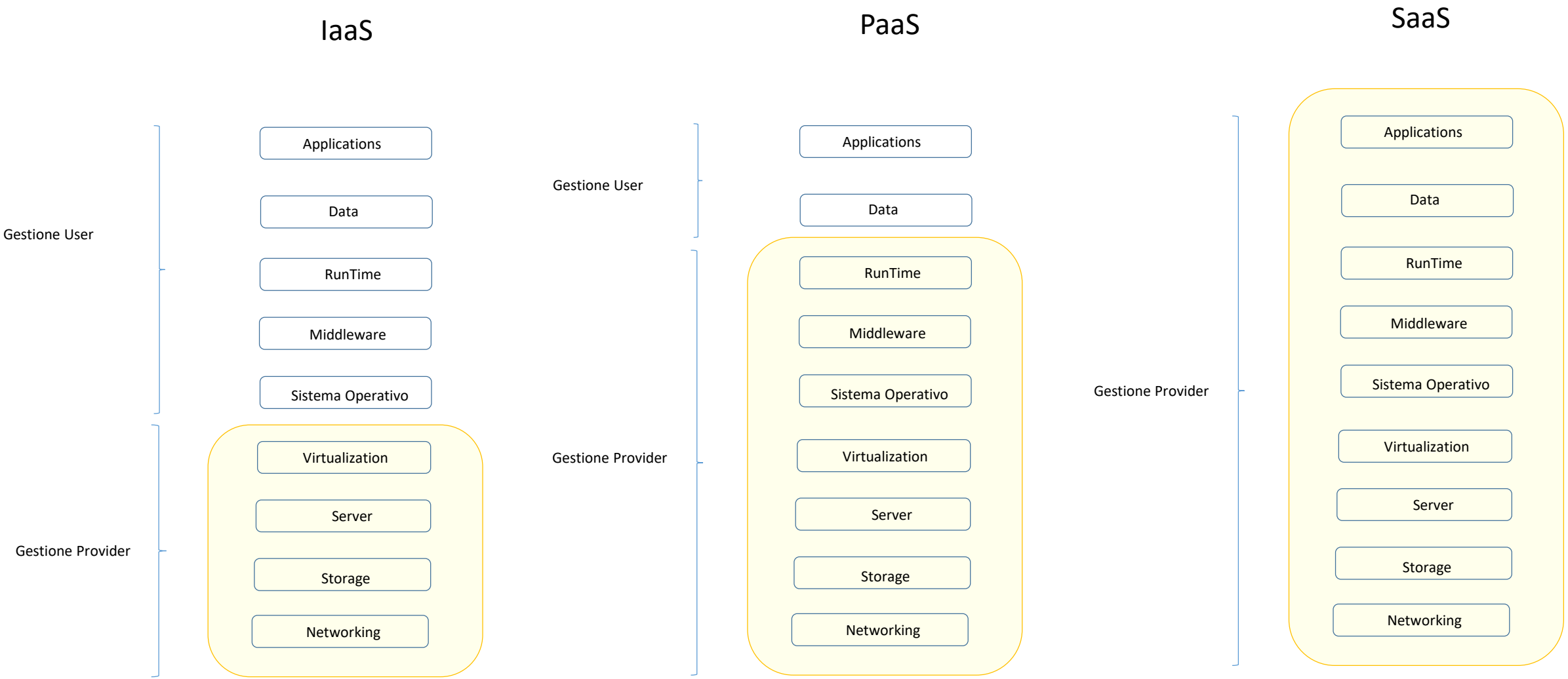
Cosa è un IaaS, PaaS, SaaS

- **SaaS** significa Software as a Service dove si mettono a disposizione sistemi ed applicazioni software accessibili da qualsiasi dispositivo fisso o mobile attraverso il semplice uso di una interfaccia client; l'infrastruttura viene gestita dal Provider
- Esempio di SaaS:
  - G Suite
  - Gmail
  - Dropbox

- **PaaS** significa Platform as a Service è un modello dove vengono situati i servizi si piattaforme online dove poter effettuare il rilascio (deployment) di applicazioni (DB, runtime, email, storage), software (ERP, CRM, E-commerce) oppure esigenze quali backup dei dati i DR da parte di un user che intende fornire a terzi; l'infrastruttura viene gestita dal Provider
- Esempio di PaaS:

  - RDS (Amazon Relational Database Service)
  - Amazon Dynamo DB
  - Amazon API Gateway
  - Google Cloud App Engine
  - Google Cloud SQL
  - Google Cloud Datastore
  - Microsoft Azure
  - Etc….

Cosa è un IaaS, PaaS, SaaS



Cosa è un SDN ed un NFV

- **SDN** Software Defined Network
- **NFV** Network Function Virtualization

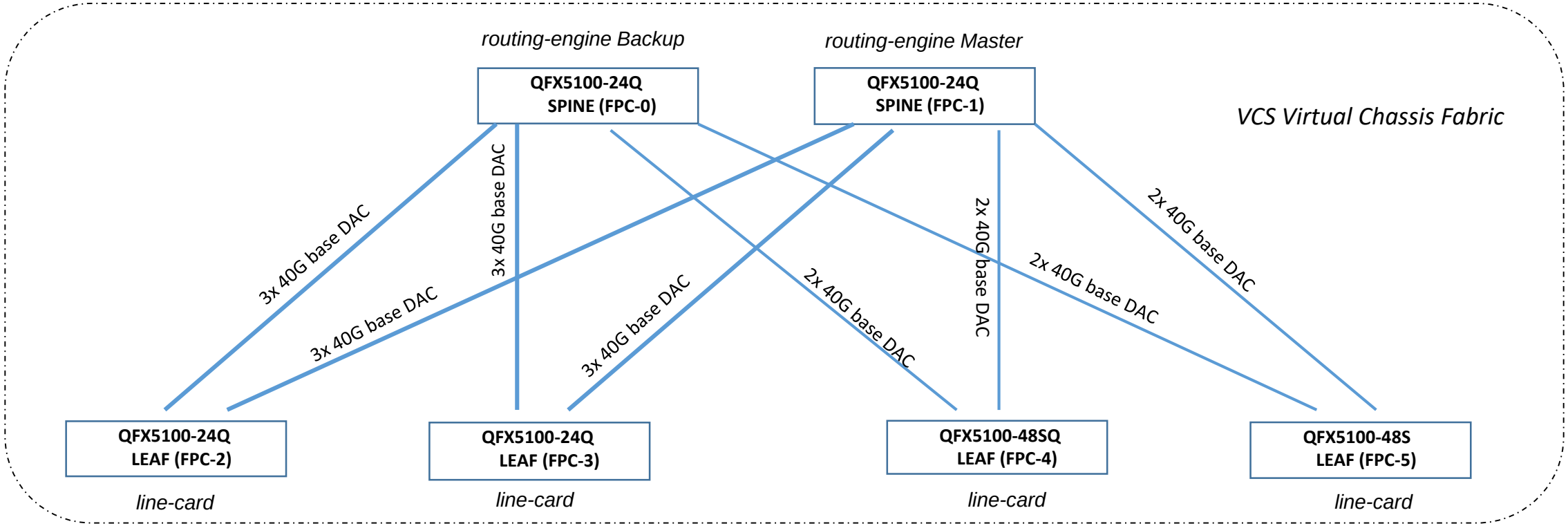
Entrambe condividono un sistema di trasporto network basato e gestito via software dove il perno tecnologico è la Fabric Ethernet con un nuovo concetto di switching.

Si basano su reti fisiche di tipo CLOS a due livelli chiamati rispettivamente Spine and Leaf con un unico dominio le cui principali caratteristiche sono:

- Alta scalabilità (possibilità di inserimento nuovi elementi) ed una grande capacità in numero di porte
- Riduzione OpEx (es: riduzione numero apparati rispetto ad una tradizionale rete a tre livelli)
- Riduzione CapEx (es: risparmio energetico)
- Spanning Tree Free
- L3 Ethernet equal-cost multipath (ECMP Load Balancing)
- avere funzionalità L2 (switching) attraverso L3 capability IPv4 e IPv6 (oltre MPLS, BGP, ISIS), inoltre supporta funzionalità quali FCoE, VXLAN, NVGRE, VMware integration

Cosa è una Fabric via QFX5100 Juniper

- La Fabric opera in modalità VCF (Virtual Chassis Fabric) in cui tutti gli switch della Fabric si aggregano a formare logicamente un unico switch L2/L3 nel contesto del quale i due apparati di Spine assolvono il ruolo di routing engine (active/standby) e i nodi Leaf operano concettualmente come linecard.
- La Fabric consente l'aggregazione di più porte fisiche, anche di switch differenti, in gruppi LACP. Ciò a scopo di distribuzione del traffico su più interfacce e di alta affidabilità ai guasti.



Cosa è una Fabric via QFX5100 Juniper

E’ un’architettura CLOS (Spine and Leaf) dove le principali features sono:

- Fabric multi-path: il piano di forwarding di un pacchetto tra i nodi è regolato dal protocollo SPF (Shortest Path First);
- Intelligent Bandwidth Allocaton: il nodo trasmittente considera la quantità di banda disponibile per ogni multi-path tra un nodo e l’altro, allocando le risorse di rete end-to-end;
- Bidirectional MDT (Multicast Distribution Tree): VFC calcola multipli alberi (tree) multicast in modo bidirezionale e performa load-balancing in questi percorsi;
- L2 and L3 capability: in base alla licenza adottata, possiamo avere funzionalità L2 attraverso L3 capability IPv4 e IPv6 (oltre MPLS, BGP, ISIS in tutte le porte VFC), inoltre supporta funzionalità quali FCoE, VXLAN, NVGRE, VMware integration;
- Resiliency and High Availability: include redundant routing engine in modalita active-backup, redundant data-plane con modalità active-active uplinks;
- NSSU (No Stop Software Upgrade): disponibile per VFC con doppio RE (Routing Engine) e consente aggiornamenti software senza distruzioni o interruzioni di funzionalità.

Cosa è una Fabric via ACI Cisco

Cisco ACI (Application Centric Infrastructure) è basato sul concetto di group-based policy SDN;

End-User ACI può definire una serie di regole senza la conoscenza e/o informazioni che derivano dalla struttura networking;

Cisco APIC (Application Policy Infrastructure Controller) è responsabile della gestione centralizzata delle policies configurate e distribuirle a tutti i nodi facenti parte della ACI Fabric;

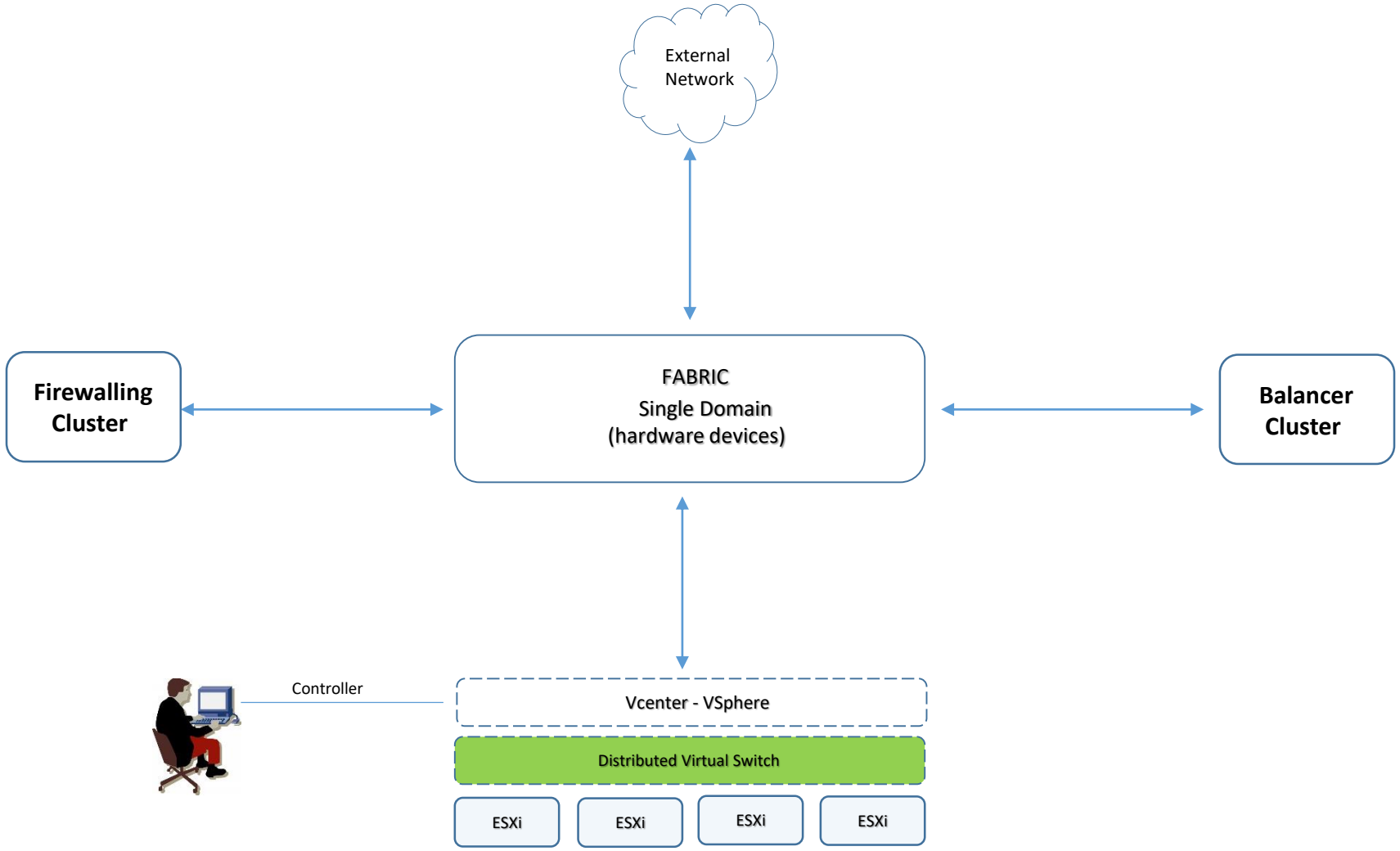
Cisco ACI è disegnato per scalare in modo trasparente nei confronti di cambiamenti di connettività, bandwidth, tenants e policies; la sua architettura è di tipo spine-leaf che si presta efficientemente a introdurre e/o cambiare requisiti di rete;

Cisco ACI include servizi layer 4 to layer 7, APIs (Application Programming Interface), virtual networking, computing, storage resources, wan routers, orchestration services.

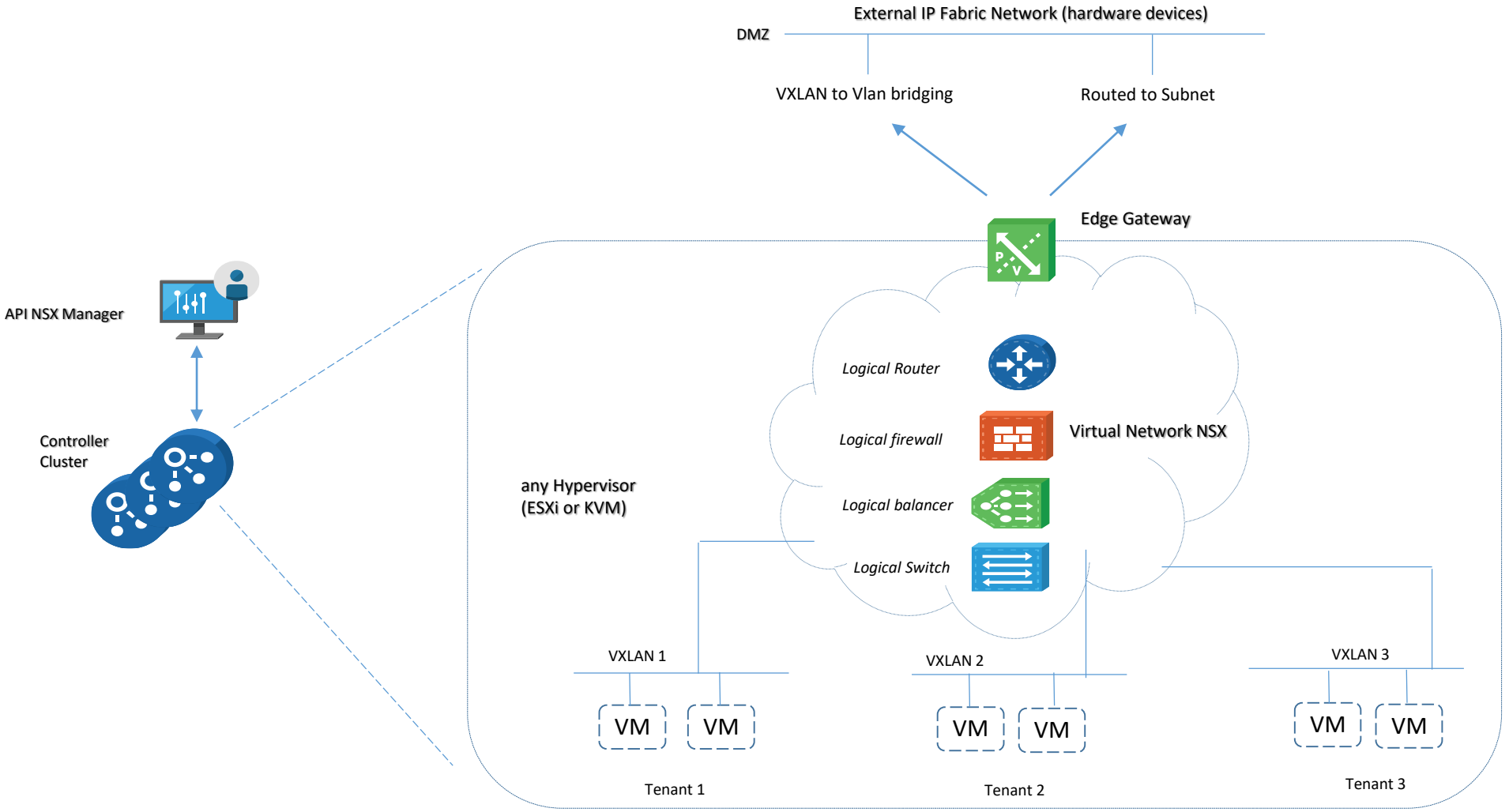
Cisco ACI consiste in:

- Un insieme di software e hardware devices che costituiscono una Fabric
- APIC per la gestione delle policies centralizzata
- AVS (Application Virtual Switch) per virtual network edge level
- Integrazione di fisiche e virtuali infrastrutture
- Un aperto ecosistema di network, storage, management e orchestration vendor

Esempio di una architettura DC bare-metal Vmware Computing



Esempio di una architettura DC con NSX



Esempio di una architettura DC con ACI Cisco Nexus N9K