Cloud computing - ch - 3

Virtualization and Abstraction

topics

- What is Virtualization
- How abstraction is provided in cloud
- Advantages and Disadvantages
- Types of Hypervisors
- Load balancing

What is virtualization

- Virtualization is technology that allows you to create multiple simulated environments or dedicated resources from a single, physical hardware system.
- Software called a hypervisor connects directly to that hardware and allows you to split 1 system into separate, distinct, and secure environments known as virtual machines (VMs).
- These VMs rely on the hypervisor’s ability to separate the machine’s resources from the hardware and distribute them appropriately

Virtualization in Cloud Computing

- Cloud computing takes virtualization one step further:
- You don’t need to own the hardware
- Resources are rented as needed from a cloud
- Various providers allow creating virtual servers:
  - Choose the OS and software each instance will have
  - The chosen OS will run on a large server farm
  - Can instantiate more virtual servers or shut down existing ones within minutes
- You get billed only for what you used

Virtualization Security Requirements

- Scenario: A client uses the service of a cloud computing company to build a remote VM
  - A secure network interface
  - A secure secondary storage
  - A secure run-time environment
    - Build, save, restore, destroy

Virtualization Security Requirements

- A secure run-time environment is the most fundamental
  - The first two problems already have solutions:
    - Network interface: Transport layer security (TLS)
    - Secondary storage: Network file system (NFS)
  - The security mechanism in the first two rely on a secure run-time environment
    - All the cryptographic algorithms and security protocols reside in the run-time environment

how abstraction is provided in cloud

Abstraction in cloud computing refers to the process of hiding complex underlying infrastructure details and presenting users with simplified and higher-level services.

This abstraction helps users focus on their core tasks without needing to worry about the intricacies of hardware, networking, and other low-level components.

Cloud providers offer various levels of abstraction to cater to different user needs.

Based on service model

Infrastructure as a Service (IaaS): This level of abstraction provides virtualized computing resources like virtual machines, storage, and networking. Users have control over the operating system, applications, and configurations, but the underlying infrastructure management is handled by the cloud provider.

Platform as a Service (PaaS): PaaS abstracts even more of the infrastructure, offering a platform and environment for developers to build, deploy, and manage applications. Users focus on coding and application development, while the provider takes care of the underlying infrastructure, runtime, and middleware.

Software as a Service (SaaS): SaaS provides fully abstracted applications that are accessed over the internet. Users simply use the software without worrying about any underlying infrastructure, maintenance, or updates.

Based on virtualization

Virtualization is a foundational technology that enables abstraction in cloud computing.

It involves creating virtual instances of computing resources, such as virtual machines (VMs) or virtual networks.

Users interact with these virtual resources, while the cloud provider manages the physical infrastructure.

Based on resource scaling and managed service

Resource Scaling: Cloud providers offer scalable resources that can be easily adjusted to match user demands. Users can scale up or down in terms of computing power, storage, and network resources without needing to deal with the underlying hardware.

Managed Services: Cloud providers offer a wide range of managed services that abstract away complex tasks. These services include managed databases, load balancers, content delivery networks (CDNs), and more. Users leverage these services without needing to handle the operational aspects.

Based on apis and containers

APIs and Abstraction Layers: Cloud providers expose APIs (Application Programming Interfaces) that allow users to interact with and manage cloud resources programmatically. These APIs provide a level of abstraction, enabling users to control and automate cloud services without needing to know the underlying implementation details.

Containers and Container Orchestration: Containers abstract the application and its dependencies, making it portable and consistent across different environments. Container orchestration platforms like Kubernetes provide abstraction for managing and scaling containers, simplifying the deployment and management process.

Based on serverless platform and networking

Serverless Computing: In serverless computing, users focus solely on writing and deploying code, without managing the underlying servers. The cloud provider automatically handles resource allocation, scaling, and maintenance based on incoming requests.

Abstraction in Networking: Cloud providers offer abstracted networking components such as virtual networks, subnets, firewalls, and load balancers. Users configure and manage these components through user-friendly interfaces without dealing with complex networking configurations.

Pros of Virtualization in Cloud Computing

Utilization of Hardware Efficiently –

With the help of Virtualization Hardware is Efficiently used by user as well as Cloud Service Provider which decreases hardware resource cost.In Service Provider point of View, they will vitalize the Hardware using Hardware Virtualization which decrease the Hardware requirement from Vendor side which are provided to User is decreased. Before Virtualization, Companies and organizations have to set up their own Server which require extra space for placing them, engineer's to check its performance and require extra hardware cost but with the help of Virtualization the all these limitations are removed by Cloud vendors who provide Physical Services without setting up any Physical Hardware system.

Availability increases with Virtualization –

One of the main benefit of Virtualization is that it provides advance features which allow virtual instances to be available all the times. It also has capability to move virtual instance from one virtual Server another Server which is very tedious and risky task in Server Based System. During migration of Data from one server to another it ensures its safety. Also, we can access information from any location and any time from any device.

Disaster Recovery is efficient and easy –

With the help of virtualization Data Recovery, Backup, Duplication becomes very easy. In traditional method , if somehow due to some disaster if Server system Damaged then the surety of Data Recovery is very less. But with the tools of Virtualization real time data backup recovery and mirroring become easy task and provide surety of zero percent data loss.

Pros of Virtualization in Cloud Computing

Virtualization saves Energy –

Virtualization will help to save Energy because while moving from physical Servers to Virtual Server's, the number of Server's decreases due to this monthly power and cooling cost decreases which will Save Money as well. As cooling cost reduces it means carbon production by devices also decreases which results in Fresh and pollution free environment.

Quick and Easy Set up –

In traditional methods Setting up physical system and servers are very time-consuming. Firstly Purchase them in bulk after that wait for shipment. When Shipment is done then wait for Setting up and after that again spend time in installing required software etc. Which will consume very time. But with the help of virtualization the entire process is done in very less time which results in productive setup.

Cloud Migration becomes easy –

Most of the companies those who already have spent a lot in the server have a doubt of Shifting to Cloud. But it is more cost-effective to shift to cloud services because all the data that is present in their server's can be easily migrated into the cloud server and save something from maintenance charge, power consumption, cooling cost, cost to Server Maintenance Engineer etc.

Cons of Virtualization

Data can be at Risk –

Working on virtual instances on shared resources means that our data is hosted on third party resource which put's our data in vulnerable condition. Any hacker can attack on our data or try to perform unauthorized access. Without Security solution our data is in threaten situation.

Learning New Infrastructure –

As Organization shifted from Servers to Cloud. They required skilled staff who can work with cloud easily. Either they hire new IT staff with relevant skill or provide training on that skill which increase the cost of company.

High Initial Investment –

It is true that Virtualization will reduce the cost of companies but also it is truth that Cloud have high initial investment. It provides numerous services which are not required and when unskilled organization will try to set up in cloud they purchase unnecessary services which are not even required to them

Virtual Machine Monitor (VMM)

- A virtual machine monitor (VMM), also known as a hypervisor, is a software, hardware, or firmware-based process that manages the creation and operation of virtualized environments from the host system.
- Virtual machine monitors provide IT operations managers visibility into the usage and performance of associated VMs.
- In supporting the management of a virtual environment, virtual machine monitoring supports efficient performance and maximal uptime of virtual machines; collects data about the performance of virtual machines necessary for troubleshooting and event resolution

VMM

- VMM is the primary software behind virtualization environments and implementations. When installed over a host machine, VMM facilitates the creation of VMs, each with separate operating systems (OS) and applications.
- VMM manages the backend operation of these VMs by allocating the necessary computing, memory, storage and other input/output (I/O) resources.
- VMM also provides a centralized interface for managing the entire operation, status and availability of VMs that are installed over a single host or spread across different and interconnected hosts.

Supported Apps

VMWware ESX/ESXi	Microsoft Hyper-V	Citrix Hypervisor	Citrix Virtual Apps
VMware Horizon View	Docker	Kubernetes	Red Hat Virtualization
Kernel-based VM	Oracle VM	Openshift	

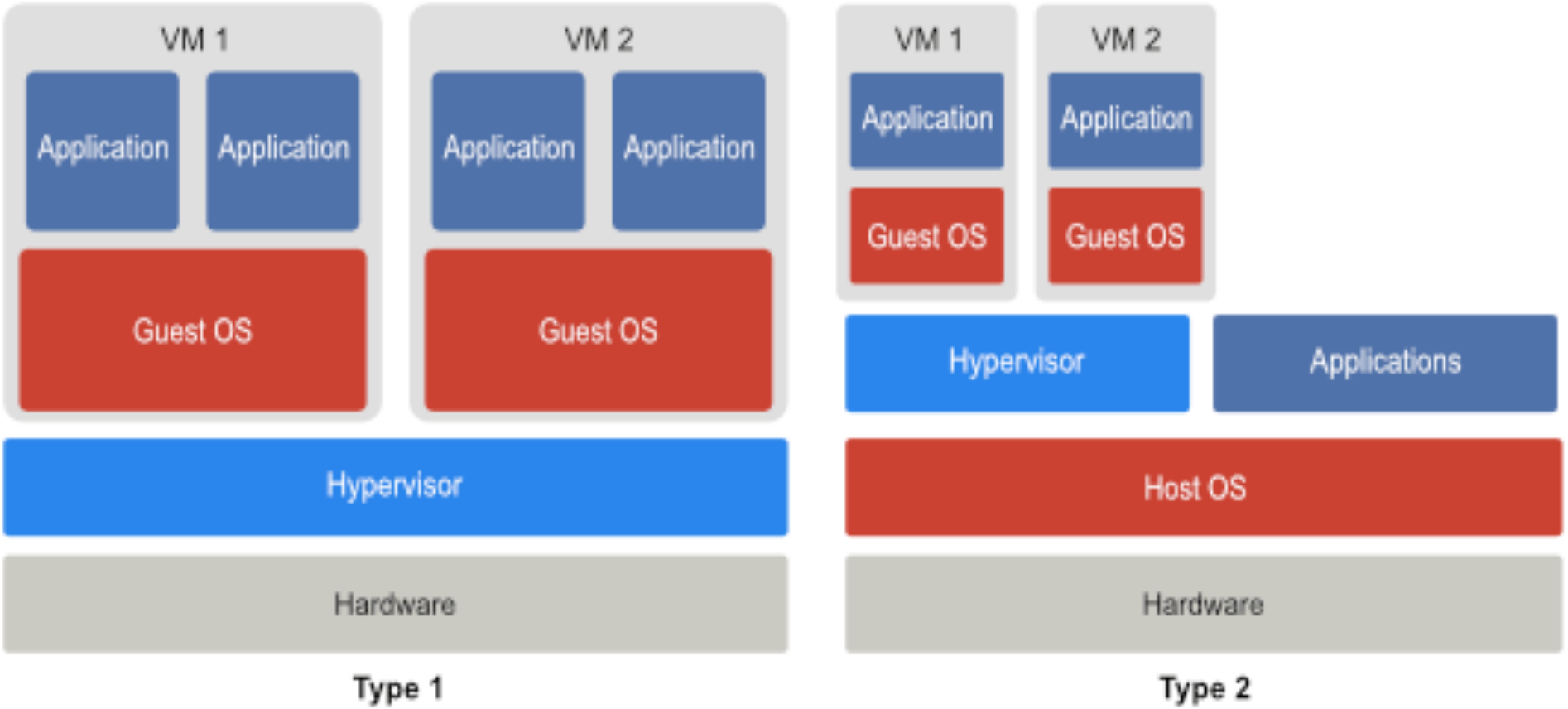
Types of Hypervisor

- A hypervisor, also known as a virtual machine monitor or VMM, is software that creates and runs virtual machines (VMs). A hypervisor allows one host computer to support multiple guest VMs by virtually sharing its resources, such as memory and processing.
- There are two main hypervisor types, referred to as “Type 1” (or “bare metal”) and “Type 2” (or “hosted”).

Type 1 hypervisor

- A type 1 hypervisor acts like a lightweight operating system and runs directly on the host's hardware
- In this type of hypervisor , virtualization software is installed directly on the hardware where the operating system is normally installed
- Because bare-metal hypervisors are isolated from the attack-prone operating system, they are extremely secure.
- In addition, they generally perform better and more efficiently than hosted hypervisors. For these reasons, most enterprise companies choose bare-metal hypervisors for data center computing needs.

Hypervisor Types



TYPE 1 hypervisor examples:

1. VMware ESX and ESXi

- These hypervisors offer advanced features and scalability, but require licensing, so the costs are higher.
- There are some lower-cost bundles that VMware offers and they can make hypervisor technology more affordable for small infrastructures.
- VMware is the leader in the Type-1 hypervisors. Their vSphere/ESXi product is available in a free edition and 5 commercial editions.

TYPE 1 hypervisor examples:

2. Microsoft Hyper-V

- The Microsoft hypervisor, Hyper-V doesn't offer many of the advanced features that VMware's products provide. However, with XenServer and vSphere, Hyper-V is one of the top 3 Type-1 hypervisors.
- It was first released with Windows Server, but now Hyper-V has been greatly enhanced with Windows Server 2012 Hyper-V.
- Hyper-V is available in both a free edition (with no GUI and no virtualization rights) and 4 commercial editions – Foundations (OEM only), Essentials, Standard, and Datacenter.

TYPE 1 hypervisor examples:

3. Citrix XenServer

It began as an open source project. The core hypervisor technology is free, but like VMware's free ESXi, it has almost no advanced features.

Xen is a type-1 bare-metal hypervisor. Just as Red Hat Enterprise Virtualization uses KVM, Citrix uses Xen in the commercial XenServer.

Today, the Xen open source projects and community are at Xen.org. Today, XenServer is a commercial type-1 hypervisor solution from Citrix, offered in 4 editions.

Confusingly, Citrix has also branded their other proprietary solutions like XenApp and XenDesktop with the Xen name.

TYPE 1 hypervisor examples:

4. Oracle VM

- The Oracle hypervisor is based on the open source Xen.
- However, if you need hypervisor support and product updates, it will cost you.
- Oracle VM lacks many of the advanced features found in other bare-metal virtualization hypervisors.

Type 2 hypervisor

Type 2 hypervisor runs as a software layer on an operating system, like other computer programs

TYPE 2 hypervisor examples:

1. VMware Workstation/Fusion/Player

- VMware Player is a free virtualization hypervisor. It is intended to run only one virtual machine (VM) and does not allow creating VMs.
- VMware Workstation is a more robust hypervisor with some advanced features, such as record-and-replay and VM snapshot support.
- VMware Workstation has three major use cases:
    - for running multiple different operating systems or versions of one OS
    - on one desktop,
    - for developers that need sandbox environments and snapshots, or
    - for labs and demonstration purposes.

TYPE 2 hypervisor examples:

2. VMware Server

- VMware Server is a free, hosted virtualization hypervisor that’s very similar to the VMware Workstation.
- VMware has halted development on Server since 2009

TYPE 2 hypervisor examples:

3. Microsoft Virtual PC

- This is the latest Microsoft's version of this hypervisor technology, Windows Virtual PC and runs only on Windows 7 and supports only Windows operating systems running on it.

TYPE 2 hypervisor examples:

4. Oracle VM VirtualBox

- VirtualBox hypervisor technology provides reasonable performance and features if you want to virtualize on a budget.
- Despite being a free, hosted product with a very small footprint, VirtualBox shares many features with VMware vSphere and Microsoft Hyper-V.

TYPE 2 hypervisor examples:

5. Red Hat Enterprise Virtualization

- Red Hat’s Kernel-based Virtual Machine (KVM) has qualities of both a hosted and a bare-metal virtualization hypervisor.
- It can turn the Linux kernel itself into a hypervisor so the VMs have direct access to the physical hardware.

Load balancing

What is load balancing

Load balancing is a crucial concept in computer networking and distributed systems, including cloud computing.

It refers to the process of distributing incoming network traffic or computational tasks across multiple servers, resources, or computing nodes to ensure optimal resource utilization, improved performance, and high availability.

Load balancing aims to prevent any single server or resource from becoming overloaded while ensuring that the workload is efficiently distributed.

Goals of load balancing

- **Optimal Resource Utilization**: Load balancing ensures that resources, such as servers, CPUs, memory, and network bandwidth, are utilized efficiently. By distributing workloads evenly, no single resource is overwhelmed while others remain underutilized.
- **Improved Performance**: Evenly distributing traffic or tasks across multiple resources reduces response times and latency. This results in faster processing of requests and a more responsive user experience.
- **Scalability**: Load balancing helps accommodate increased demand and growth by adding more resources as needed. This scalability ensures that applications can handle varying workloads without causing performance degradation.
- **High Availability**: By distributing traffic across multiple servers, load balancing helps minimize the impact of server failures. If one server goes down, the load balancer can redirect traffic to healthy servers, ensuring continuous availability of services.
- **Fault Tolerance**: Load balancers can detect and route traffic away from malfunctioning or unresponsive servers, preventing users from experiencing disruptions due to server failures.

Algorithms of load balancing

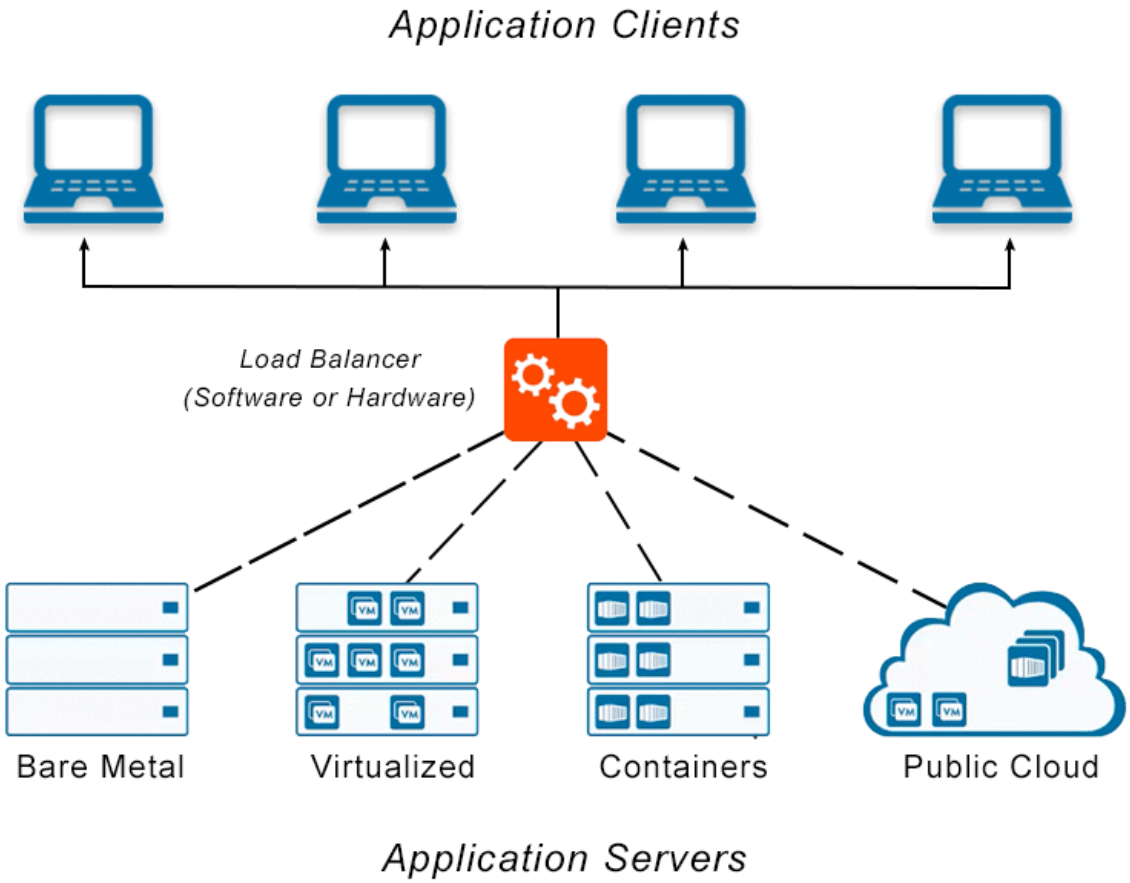
Round Robin: Incoming requests are distributed sequentially to each server in rotation. It's a simple method but doesn't consider server load or performance.

Weighted Round Robin: Servers are assigned different weights, indicating their capacity or performance. Requests are then distributed based on these weights.

Least Connections: Traffic is directed to the server with the fewest active connections. This method can help balance workloads based on the current load of each server.

Weighted Least Connections: Similar to weighted round robin, this method assigns weights to servers based on their capacity, and requests are directed to the server with the lowest weighted connections.

Least Response Time: Traffic is directed to the server with the lowest response time. This method aims to minimize latency and improve user experience.


Application Clients
Load Balancer
(Software or Hardware)
Bare Metal
Virtualized
Containers
Public Cloud
Application Servers

Load balancers typically come in two flavours: hardware-based and software-based.

Vendors of hardware-based solutions load proprietary software onto the machine they provide, which often uses specialized processors.

To cope with increasing traffic on your website, you have to buy more or bigger machines from the vendor.

Software solutions generally run on commodity hardware, making them less expensive and more flexible.

The advantages of hardware load balancer

- **High Performance**

  The system performance is critical for any network application and load balancer is no exception. When it comes to system performance, you need properly designed software architecture running on dedicated hardware.The NIC driver should be tuned or even completely rewritten for best performance. Take Intel Gigabit and 10G ports as example. You just can’t install the software on random server or hardware and still hope the performance is good. Hardware load balancer has lower latency and more consistent performance.

- **Less prone for failure**

  The hardware load balancer is typically built on properly optimized and well-tested hardware platform. And underlying OS of load balancer is built against specific hardware for performance and stability.

The disadvantages of hardware load balancer

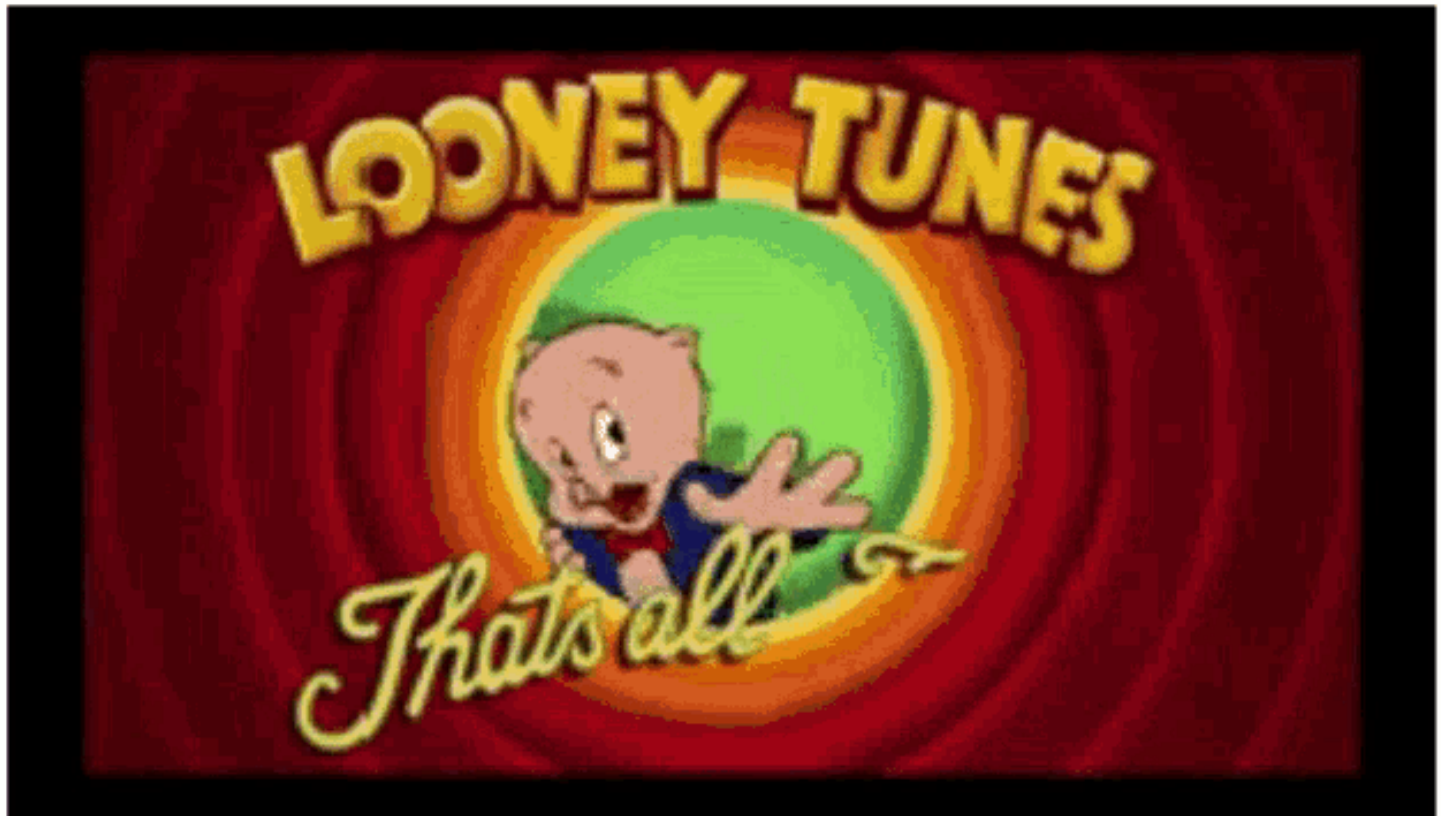
- **Overprovisioning**
  - You have to pay more for load balancing capability to meet peak demands.
- **Cost**
  - Hardware load balancer requires expensive maintenance and it definitely increase TCO for IT infrastructure.

The advantages of software load balancer

- **Cost effective**
  - Deploying software load balancer is much more cost effective than its hardware counterparts.
- **Easy scaling up**
  - The nature of software load balancer makes it easier to scale up or down.
- **Cloud and Virtualization**
  - This is where benefits of a software load balancer come into play. Because software load balancer can be running directly on VM. You just can use hardware load balancer in Cloud. With hardware virtualization, software load balancer can be running on a hypervisor.

The disadvantages of software load balancer

- Performance
  - Compared to hardware load balancer, the main downside to software load balancer is in its performance.



Thats all folks for this chapter !!!!