Virtualization and Containers

By Ahsan Farooqui

Presentation Roadmap

- ❑ Introduction
- ❑ Overview
- ❑ Shared Model of Virtualization Security
- ❑ Major Virtualization Categories in the Cloud
- ❑ Compute Virtualization
- ❑ Network Virtualization
- ❑ Storage Virtualization
- ❑ Containers Virtualization
- ❑ Containers Components
- ❑ Container Security
- ❑ Containers Isolation and Management
- ❑ AWS Services and Products
- ❑ Aws Hypervisors
- ❑ Aws Compute
- ❑ AWS Networking & Contents Delivery
- ❑ AWS Storage Services

Introduction

Virtualization isn't merely a tool for creating virtual machines—it's the core technology for enabling cloud computing. We use virtualization all throughout computing, from full operating virtual machines to virtual execution environments like the Java Virtual Machine, as well as in storage, networking, and beyond.

Cloud computing is fundamentally based on pooling resources and virtualization is the technology used to convert fixed infrastructure into these pooled resources. Virtualization provides the abstraction needed for resource pools, which are then managed using orchestration.

Introduction

Virtualization covers an extremely wide range of technologies; essentially any time we create an abstraction, we’re using virtualization. For cloud computing we tend to focus on those specific aspects of virtualization used to create our resource pools, especially:

- ❑ Compute
- ❑ Network
- ❑ Storage
- ❑ Containers

Cloud computing is fundamentally based on virtualization: It’s how we abstract resources to create pools. Without virtualization, there is no cloud.

Introduction

- Understanding the impacts of virtualization on security is fundamental to properly architecting and implementing cloud security.
- Virtual assets provisioned from a resource pool may look just like the physical assets they replace, but that look and feel is really just a tool to help us better understand and manage what we see.
- It’s also a useful way to leverage existing technologies, like operating systems, without having to completely rewrite them from scratch. Underneath, these virtual assets work completely differently from the resources they are abstracted from.

Overview

Many security processes are designed with the expectation of physical control over the underlying infrastructure. While this doesn’t go away with cloud computing, virtualization adds two new layers for security controls:

- ❑ Security of the virtualization technology itself, e.g., securing a hypervisor.
- ❑ Security controls for the virtual assets. In many cases, this must be implemented differently than it would be in the corresponding physical equivalent.
- ❑ For example, virtual firewalls are not the same as physical firewalls, and mere abstraction of a physical firewall into a virtual machine still may not meet deployment or security requirements.

Shared Model -Virtualization Security

Virtualization security in cloud computing still follows the shared responsibility model.

- ❑ **The cloud provider will always be responsible for securing the physical infrastructure and the virtualization platform itself.**
- ❑ **Meanwhile, the cloud customer is responsible for properly implementing the available virtualized security controls and understanding the underlying risks, based on what is implemented and managed by the cloud provider.**
- ❑ **For example, deciding when to encrypt virtualized storage, properly configuring the virtual network and firewalls, or deciding when to use *dedicated hosting vs. a shared host.***

Major Virtualization Categories in cloud

- Compute
- Networks
  - Monitoring and Filtering
  - Managing Infrastructure
  - Cloud Overlay Networks
- Storage
- Containers

Viewing in term of shared responsibility model

- Cloud Provider
- Cloud users

Compute Virtualization

- ❑ Compute virtualization abstracts the running of code (including operating systems) from the underlying hardware.
- ❑ Instead of running directly on the hardware, the code runs on top of an abstraction layer that enables more flexible usage, such as running multiple operating systems on the same hardware (virtual machines).
- ❑ Compute most commonly refers to virtual machines or Instances
- ❑ Containers and certain kinds of serverless infrastructure also abstract compute. These are different abstractions to create code execution environments, but they don’t abstract a full operating system as virtual machine does.

Compute Virtualization-Cloud Provider

- The primary security responsibilities of the cloud provider in compute virtualization are to enforce isolation and maintain a secure virtualization infrastructure.
- Isolation ensures that compute processes or memory in one virtual machine/container should not be visible to another. It is how we separate different tenants, even when they are running processes on the same physical hardware.
- The cloud provider is also responsible for securing the underlying infrastructure and the virtualization technology from external attack or internal misuse. This means using patched and up-to-date hypervisors that are properly configured and supported with processes to keep them up to date and secure over time. The inability to patch hypervisors across a cloud deployment could create a fundamentally insecure cloud when a new vulnerability in the technology is discovered.

Compute Virtualization-Cloud Provider

- Cloud providers should also support secure use of virtualization for cloud users. This means creating a secure chain of processes from the image (or other source) used to run the virtual machine all the way through a boot process with security and integrity. This ensures that tenants cannot launch machines based on images that they shouldn’t have access to, such as those belonging to another tenant, and that a running virtual machine (or other process) is the one the customer expects to be running.
- In addition, cloud providers should assure customers that volatile memory is safe from unapproved monitoring, since important data could be exposed if another tenant, a malicious employee, or even an attacker is able to access running memory.

Compute Virtualization-Cloud Users

- Meanwhile, the primary responsibility of the cloud user is to properly implement the security of whatever it deploys within the virtualized environment.
- Firstly, the cloud user should take advantage of the security controls
- for managing their virtual infrastructure, which will vary based on the cloud platform and often include:
    - Security settings, such as identity management, to the virtual resources. This is not the identity management within the resource, such as the operating system login credentials, but the identity management of who is allowed to access the cloud management of the resource—for example, stopping or changing the configuration of a virtual machine. (management plane security)

Compute Virtualization-Cloud Users

- ❑ Monitoring and logging monitoring and logging of workloads, including how to handle system logs from virtual machines of containers, but the cloud platform will likely offer additional logging and monitoring at the virtualization level. This can include the status of a virtual machine, management events, performance, etc.
- ❑ Image asset management. Cloud compute deployments are based on master images—be it a virtual machine, container, or other code—that are then run in the cloud. This is often highly automated and results in a larger number of images to base assets on, compared to traditional computing master images. Managing these—including which meet security requirements, where they can be deployed, and who has access to them—is an important security responsibility.
- ❑ • Use of dedicated hosting, if available, based on the security context of the resource.
- ❑ In some situations you can specify that your assets run on hardware dedicated only
- ❑ to you (at higher cost), even on a multitenant cloud. This may help meet compliance
- ❑ requirements or satisfy security needs in special cases where sharing hardware with
- ❑ another tenant is considered a risk.

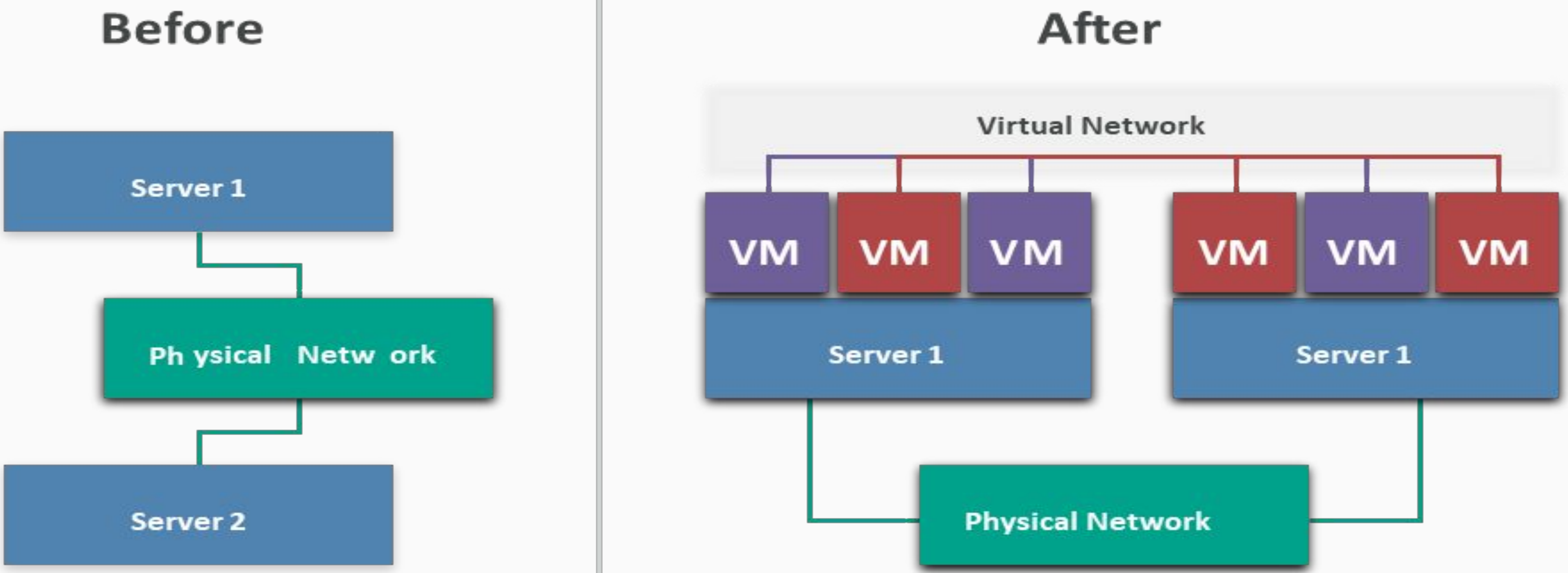
Compute Virtualization-Cloud Users

  - Use of dedicated hosting, if available, based on the security context of the resource.In some situations you can specify that your assets run on hardware dedicated only to you (at higher cost), even on a multitenant cloud. This may help meet or satisfy security needs in special cases where sharing hardware with another tenant is considered a risk.
- Secondly, the cloud user is also responsible for security controls within the virtualized resource:
  - This includes all the standard security for the workload, be it a virtual machine, container, or application code. These are well covered by standard security, best practices
  - Of particular concern is ensuring deployment of only secure configurations (e.g., a patched, updated virtual machine image). Due to the automation of cloud computing it is easy to deploy older configurations that may not be patched or properly secured.

Network Virtualization

- ❑ Cloud computing today uses Software-Defined Networks(SDN) for virtualizing networks.
- ❑ VLANs are often not suitable for cloud deployments since they lack important isolation capabilities for multitenancy
- ❑ SDN abstracts the network management plane from the underlying physical infrastructure, removing many typical networking constraints.
  - ❑ For example, you can overlay multiple virtual networks, even ones that completely overlap their address ranges, over the same physical hardware, with all traffic properly segregated and isolated. SDNs are also defined using software settings and API calls, which supports orchestration and agility.
- ❑ Virtual networks are quite different than physical networks. They run on physical networks, but abstraction allows for deep modification on networking behavior in ways that impact many security processes and technologies.

Network Virtualization-Monitoring &Filtering



Network Virtualization-Monitoring & Filtering

- Monitoring and filtering (including firewalls) change extensively due to the differences in how packets move around the virtual network.
- Resources may communicate on a physical server without traffic crossing the physical network. For example, if two virtual machines are located on the same physical machine there is no reason to route network traffic off the box and onto the network. Thus, they can communicate directly, and monitoring and filtering tools inline on the network (to the routing/switching hardware) will never see the traffic.
- To compensate, you can route traffic to a virtual network monitoring or filtering tool on the (including a virtual machine version of a network security product). You can also bridge all network traffic back out to the network, or route it to a virtual appliance on the same virtual network.
- The cloud platform/provider may not support access for direct network monitoring. Public cloud providers rarely allow full packet network monitoring to customers, due to the complexity (and cost).

Network Virtualization-Monitoring & Filtering

❑ **All modern cloud platforms offer built-in firewalls, which may offer advantages over corresponding physical firewalls.**

These are software firewalls that may operate within the SDN or the hypervisor. They typically offer fewer features than a modern, dedicated next-generation firewall, but these capabilities may not always be needed due to other inherent security provided by the cloud provider.

Network Virtualization-Mgmt Infrastructure

Virtual networks for cloud computing always support remote management and, as such, securing the management plane/metastructure is critical. At times it is possible to create and destroy entire complex networks with a handful of API calls or a few clicks on a web console.

Network Virtualization-Mgmt Infrastructure

- Cloud Provider Responsibilities
  - The cloud provider is primarily responsible for building a secure network infrastructure and configuring it properly. The absolute top security priority is segregation and isolation of network traffic to prevent tenants from viewing another's traffic. This is the most foundational security control for any multitenant network.
  - The provider should disable packet sniffing or other metadata "leaks" that could expose data
  - or configurations between tenants. Packet sniffing, even within a tenant's own virtual networks,should also be disabled to reduce the ability of an attacker to compromise a single node and use it to monitor the network, as is common on non-virtualized networks. Tagging or other SDN-level metadata should also not be exposed outside the management plane or a compromised host could be used to span into the SDN itself.
  - All virtual networks should enable built-in firewall capabilities for cloud users without the need for host firewalls or external products. The provider is also responsible for detecting and preventing attacks on the underlying physical network and virtualization platform. This includes perimeter security of the cloud itself.

Network Virtualization-Mgmt Infrastructure

- Cloud User Responsibilities
  - Cloud users are primarily responsible for properly configuring their deployment of the virtual network, especially any virtual firewalls.
  - Network architecture can play a larger role in virtual network security since we aren’t constrained by physical connections and routing. Since virtual networks are software constructs, the use of multiple, separate virtual networks may offer extensive compartmentalization advantages not possible on a traditional physical network. You can run every application stack in its own virtual network, which dramatically reduces the attack surface if a malicious actor gains a foothold. An equivalent architecture on a physical network is cost prohibitive.

Network Virtualization-Mgmt Infrastructure

- Cloud User Responsibilities
  - Immutable networks can be defined on some cloud platforms using software templates, which can help enforce known-good configurations. The entire known-good state of the network can be defined in a template, instead of having to manually configure all the settings. Aside from the ability to create multiple networks with a secure baseline, these can also be used to detect, and in some cases revert, deviations from known-good states.
  - The cloud user is, again, responsible for proper rights management and configuration of exposed controls in the management plane. When virtual firewalls and/or monitoring don’t meet security needs, the consumer may need to compensate with a virtual security appliance or host security agent.

Network Virtualization-Cloud overlay Network

Cloud overlay networks are a special kind of WAN virtualization technology for created networks that span multiple “base” networks. For example, an overlay network could span physical and cloud locations or multiple cloud networks, perhaps even on different providers.

Storage Virtualization

- ❑ **Storage virtualization is already common in most organizations—Storage Area Network (SAN) and Network-Attached Storage (NAS) are both common forms of storage virtualization—and storage**

- ❑ **Most virtualized storage is durable and keeps multiple copies of data in different locations so that drive failures are less likely to result in data loss.**
- ❑ **Encrypting those drives reduces the concern that swapping out a drive, which is a very frequent activity, could result in data exposure.**
- ❑ **However, this encryption doesn't protect data in any virtualized layers; it only protects the data at physical storage. Depending on the type of storage the cloud provider may also (or instead) encrypt it at the virtualization layer, but this may not protect customer data from exposure to the cloud provider.**

Containers Virtualization

- ❑ Containers are highly portable code execution environments. To simplify, a virtual machine is a complete operating system, all the way down to the kernel. A container, meanwhile, is a virtual execution environment that features an isolated user space, but uses a shared kernel.
- ❑ Such containers can be built directly on top of physical servers or run on virtual machines. Current implementations rely on an existing kernel/operating system, which is why they can run inside a virtual machine even if nested virtualization is not supported by the hypervisor. (Software containers rely on a completely different technology for hypervisors.)
- ❑

Containers Components

- Software container systems always include three key components:
    - The execution environment (the container).
    - An orchestration and scheduling controller (which can be a collection of multiple tools).
    - A repository for the container images or code to execute.
    - Together, these are the place to run things, the things to run, and the management system to tie them together.
-

Containers Security

- ❑ Regardless of the technology platform, container security includes:
  - ❑ Assuring the security of the underlying physical infrastructure (compute, network, storage). This is no different than any other form of virtualization, but it now extends into the underlying operating system where the container's execution environment runs.
  - ❑ Assuring the security of the management plane, which in this case are the orchestrator and the scheduler.
  - ❑ Properly securing the image repository. The image repository should be in a secure location with appropriate access controls configured. This is both to prevent loss or unapproved modification of container images and definition files, as well as to forestall leaks of sensitive data through unapproved access to the files. Containers run so easily that it's also important that images are only able to deploy in the right security context.
  - ❑ Building security into the tasks/code running inside the container. It's still possible to run vulnerable software inside a container and, in some cases this could expose the shared operating system or data from other containers. For example, it is possible to configure some containers to allow not merely access to the container's data on the file system but also root file system access.Allowing too much network access is also a possibility. These are all specific to the particular container platform and thus require securely configuring both the container environment and the images/container configurations themselves.

Containers Isolation & Management

- ❑ Containers don’t necessarily provide full security isolation, but they do provide task segregation. That said, virtual machines typically do provide security isolation. Thus you can put tasks of equivalent security context on the same set of physical or virtual hosts in order to provide greater security segregation.
- ❑ Container management systems and image repositories also have different security capabilities, based on which products you use. Security should learn and understand the capabilities of the products they need to support. Products should, at a minimum, support role-based access controls and strong authentication. They should also support secure configurations, such as isolating file system, process, and network access.A deep understanding of container security relies on a deep understanding of operating system internals, such as namespaces, network port mapping, memory, and storage access.

- ❑ Different host operating systems and container technologies offer different security capabilities. This assessment should be included in any container platform selection process.

- ❑ One key area to secure is which images/tasks/code are allowed into a particular execution environment. A secure repository with proper container management and scheduling will enable this.

AWS Nitro Hypervisor

The AWS Nitro System is the underlying platform for our next generation of EC2 instances that enables AWS to innovate faster, further reduce cost for our customers, and deliver added benefits like increased security and new instance types.

AWS has completely re-imagined our virtualization infrastructure. Traditionally, hypervisors protect the physical hardware and bios, virtualize the CPU, storage, networking, and provide a rich set of management capabilities. With the Nitro System, we are able to break apart those functions, offload them to dedicated hardware and software, and reduce costs by delivering practically all of the resources of a server to your instances.

Nitro Hypervisor

The Nitro Hypervisor is a lightweight hypervisor that manages memory and CPU allocation and delivers performance that is indistinguishable from bare metal.

AWS Compute Services

Here are the compute services that AWS provides for different kind of use-cases, which we discuss these in details.

1. **Amazon Elastic Compute Cloud (EC2)**
2. **Amazon Elastic Container Registry (ECR)**
3. **Amazon Elastic Container Service (ECS)**
4. **Amazon Elastic Kubernetes Service (EKS)**
5. **AWS Elastic Beanstalk (EBS)**
6. **AWS Lambda**
7. **Amazon Lightsail**
8. **AWS Batch**

EC2 - Elastic Compute Cloud is one of the most popular and mostly used compute services that AWS provides for doing computations and processing. EC2 allows you to deploy virtual servers within your AWS environment. You can think of it as a virtual machine deployed on AWS physical data-centers irrespective of your local environment.

EC2 service can be broken down into following components.

Amazon Machine Images (AMI)

AMI's are Images or templates for preconfigured EC2 instances allow you to quickly launch Ec2 servers based on configuration

Instance Types

Once you select AMI's, you need to select what type of EC2 instance type you are required to use. AWS provides tons of options divided into Instance type families that offers distinct performance benefits. You can read further about these instances in details from here.

Instance Purchasing options

AWS also provides instance purchasing options for instances through a variety of different payment plans. They have been designed to help you save cost by selecting the most appropriate option for your deployment. You can read further about these instances in details from here.

User Data

During the launch of EC2 instance, there is an option available for which allows you to enter commands that will during the first boot cycle of the instance. This is a great way to automatically perform functions you want to to execute at your instance startup.

Storage

As a part of launching ec2 instance, you're asked to select configuration for storage. As storage is a crucial part for any server we have to provide some number in GB's for persisting the ec2 data.

Security

Security is fundamental part for any AWS deployment services. During launch of EC2, you're asked to create or attach a security group with your instance. A security group is essentially instance level firewall for managing inbound and outbound traffic for your EC2.

ECS - Elastic Container Service allows you to run container based application across a cluster of EC2 instances without requiring you to manage a complex and administratively heavy cluster management system. You can deploy, manage and scale containerized applications by using ECS.

You don't have to install softwares for managing and monitoring these clusters. AWS manage these itself as it is AWS managed service. AWS ECS provides 2 ways to launch an ECS cluster.

1. Fargate Launch
2. EC2 Launch

Fargate Launch

It requires you to specify CPU and memory required, define networking and IAM policies. And you need your application into containers.

EC2 Launch

It requires you to responsible for patching and scaling your instances, and you can specify which instance types you used, and how many containers should be in a cluster.

ECR - Elastic Container Registry links closely to the last discussed service i.e ECS. It provides secure location to store and manage your docker images that can be deployed across your applications. ECR is fully managed service by AWS means you don't have to create or manage any infrastructure to allow you to create this registry. You can think of it as a dockerhub for AWS.

Amazon EKS

EKS - Elastic Kubernetes Service allows you to run and manage your infrastructure in kubernetes environment. Kubernetes is an open-source tool to manage or orchestrate your containers in form of worker nodes designed to automate, deploying, scaling, and operating containerized applications. It is designed to grow from tens, thousands, or even millions of containers. There are 2 main components kubernetes control plane and worker nodes manages the overall flow for EKS.

Kubernetes Control Plane

There are number of different components that make up the control plane and these include a number of different APIs. It has a job to manage and decide the clusters and responsible to communication for your nodes.

Worker Nodes

Kubernetes Clusters are composed of nodes. A node is a worker machine in Kubernetes and runs as an on-demand EC2 instance and includes software to run containers managed by the Kubernetes control plane.

AWS Elastic Beanstalk is a fully managed AWS service that allows you to upload your code of your web application and automatically deploys and provision the required resources required to make your application functional. It is a AWS managed service but it also provides you options for managing resources such as ec2 instances, auto-scaling groups, load-balancers, software support, databases etc for providing you to take complete control of it. For every application you need to create environment for it, which is responsible to manage those resources in form of Cloudformation stack. Yes, It uses Cloudformation for creating and provisioning your environment resources. Elastic-BeanStalk is brilliant service if you just want to upload your code and show it as a prototype of any software.

AWS Lambda

Amazon Lambda is a serverless compute service which has been designed to allow you to run your code (function) without having to manage and provision the EC2 servers. Serverless means that you do not have to manage your compute resources by yourself instead AWS will do the heavy work for your application. Obviously it uses servers under the hood for doing computing operations so its serverless for users perspective. If you don't have to spend time operating, managing, patching, and securing an EC2 instance, then you have more time to focus on the code of your application and its business logic, while at the same time, optimizing costs. With AWS Lambda, you only ever have to pay for the compute power when Lambda is in use via Lambda functions.

Amazon Lightsail is another compute service that resembles with EC2 service. Amazon Lightsail is essentially a virtual private server VPS backed by AWS infrastructure much like as EC2 but with less configuration options. Amazon Lightsail is designed for small scale business or for single users. With its simplicity and small-scale use, it's commonly used to host simple websites, small applications, and blogs. You can run multiple Lightsail instances together, allowing them to communicate. The applications can deployed quickly and cost effectively in just a few clicks.

Amazon Batch which is used to manage and run batch computing workloads within AWS. Batch computing is primarily used in specialist use cases, which require a vast amount of computer power across a cluster of compute resources to complete batch processing, executing a series of jobs or tasks.

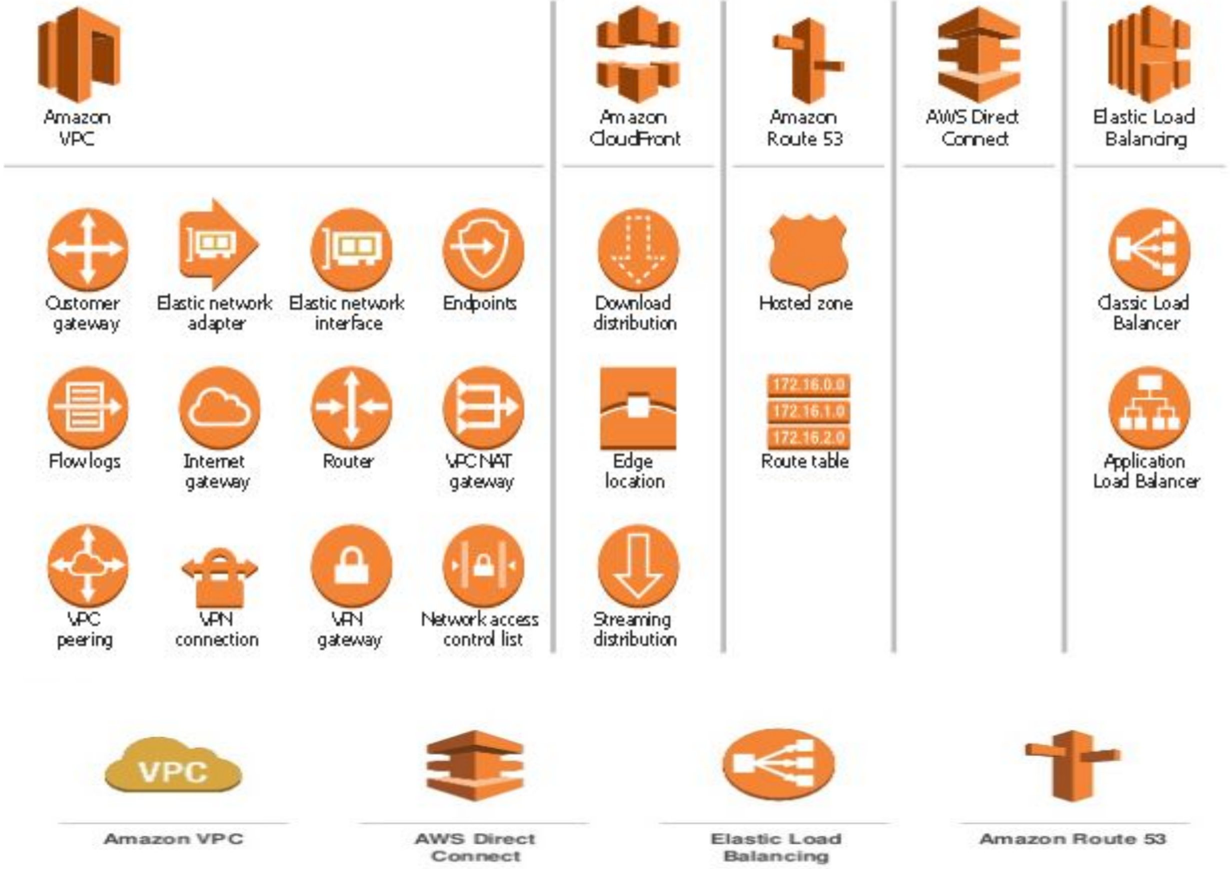
Jobs

A Job is classed as a unit of work that is to be run by AWS Batch. Job Definitions. These define specific parameters for the Jobs themselves.

Job Queues.

These are Jobs that are scheduled and placed into a Job Queue until they run. Job Scheduling. The Job Scheduler takes care of when a job should be run, and from which Compute Environment. And Compute Environments. These are the environments containing the compute resources to carry out the Job.

Networking & Content Delivery



AWS Networking and Content Delivery

Amazon CloudFront

Imagine if you can deliver data from a network to viewers at a high transfer speed and low latency, well that's what Amazon CloudFront does precisely. Amazon CloudFront is a popular Content Delivery Network (CDN) services that deliver data, be it videos, pictures, applications, and API securely over a cloud network.

Since CloudFront is integrated into AWS infrastructure, it becomes easy, fast and secure for data to be delivered across the global regions. You can get started in a few minutes once you set up your tools and they will be tools you are familiar with if you have done the initial set up your AWS account. These tools are APIs, AWS CloudFormation, CLIs, AWS Management Console and SDKs.

Amazon Virtual Private Cloud (VPC)

Are you looking for an isolated section of your AWS where you can be in complete control of the working environment? If yes, then Amazon VPC is right for the tasks. Amazon VPC lets the provision a section of the AWS cloud where the user is in total control over the environment. The user can change IPs, subnets, internet gateways, route tables, security groups, and networking configurations.

For instance, with a VPC, you can host a simple website or host multi-tier web applications. You can also connect and peer privately to other VPC's across a network.

AWS Direct Connect

This product allows for AWS users to set up an unwavering network connection for an on-premise data center. With AWS direct connect, you'd be connecting your AWS cloud to either a datacenter, office, or workstation, which invariably reduces the cost for an overall single connection.

AWS direct connect also permits access to other Amazon public and private resources such as Amazon S3 and Amazon EC2 respectively.

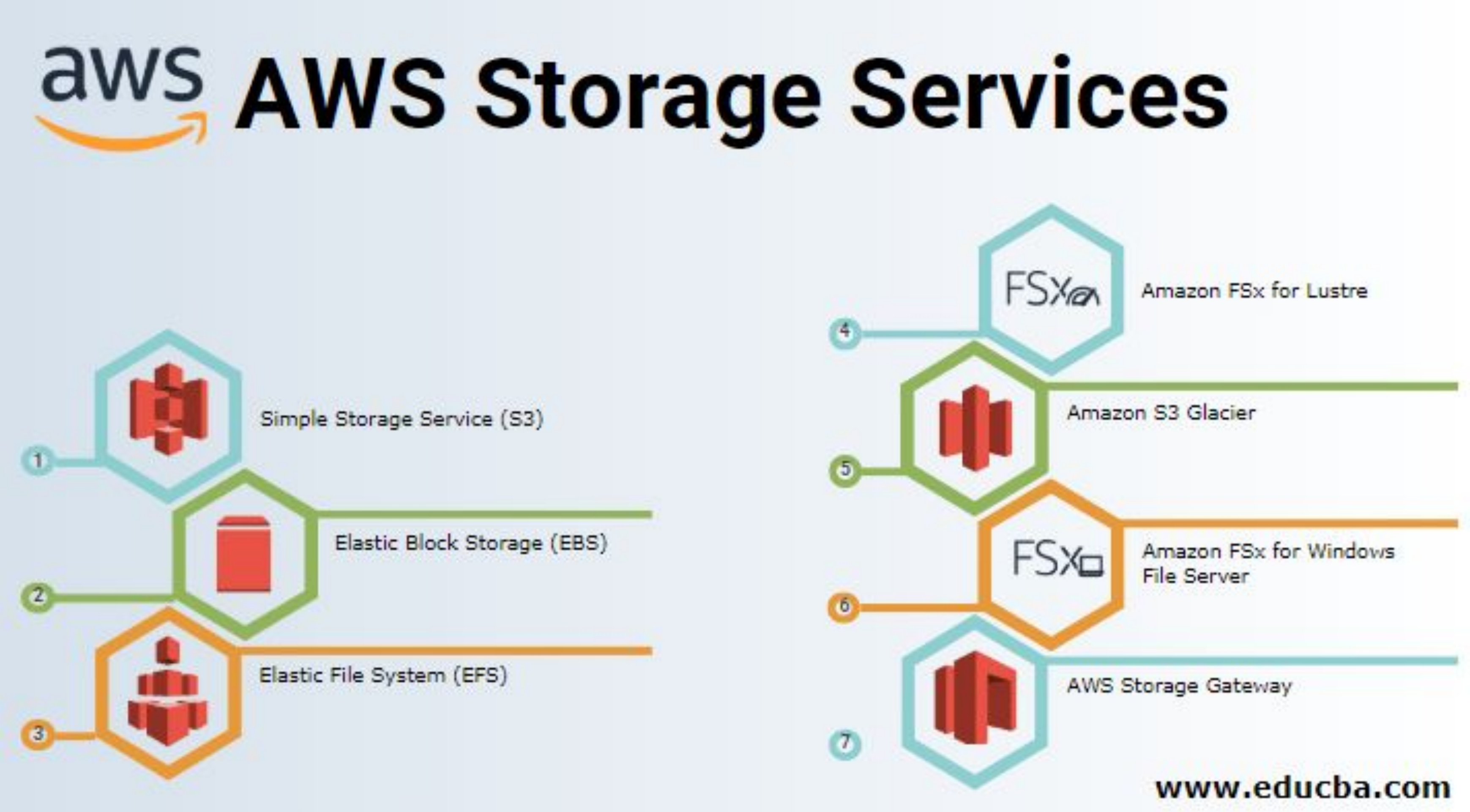
Elastic Load Balancing

As the name implies, it performs functions that balance the load of network traffic. Elastic load balancing distributes network traffic across multiple targets like EC2, to make applications less susceptible to network faults from heavy incoming traffic to your network.

It usually can perform load balancing in three ways: Application Load balancer, Network load balancer, and classic load balancer. The application load balancer works best when balancing traffic from HTTP and HTTPS request, depending on the content of delivery. The Network load balancer functions best when handling traffic from transmission control protocol (TCP) and the transport layer security (TLS) in complex requests. On the other hand, the classic load balancer tolerates traffic across the EC2 networks, and it's suited for applications built within this network.

Amazon Route 53

Amazon Route 53 offers a highly scalable, on-demand domain name system (DNS) web services. With this product, it becomes seamless for developers to translate DNS names to IP address using internet applications. Amazon Route 53 is cost-effective and extremely reliable for end users trying to route an internet application by translating the domain name to an IP address. Amazon Route 53 complies with the IPv4 guidelines in offering DNS services.



AWS Storage Services

1. Simple Storage Service (S3)
2. Elastic Block Storage (EBS)
3. Elastic File System (EFS)
4. Amazon FSx for Lustre
5. Amazon S3 Glacier
6. Amazon FSx for Windows File Server
7. AWS Storage Gateway

www.educba.com

1. Simple Storage Service (S3)

Amazon S3 is an object storage service that stores data of any type and size. It can store data for any business such as web applications, mobile applications, backup, archive, analytics. It also provides easy access control management for all your specific requirements and is almost 100% durable and by almost I mean 99.(11 nines)%. It can also be used to store all kinds of file formats as you would with a dropbox. S3 also allows a simple web-based file explorer to upload files, create folders or delete them.

2. Elastic Block Storage (EBS)

EBS provides block storage which is similar to hard drives to store any kind of data persistently. This can be attached to any EC2 instance and used as block storage, which even allows you to install any operating system. EBS volumes are placed in availability zones so that they are replicated to prevent loss of data due to single component failures. They provide absolute low-latency performance and you can also scale up or down your resources as and when required. EBS is available in both SSD and HDD formats depending on your requirement of speed and volume.

3. Elastic File System (EFS)

EFS is a managed network file system that is easy to set up right from the amazon console or CLI. When you have multiple EC2 instances needed to access the same file system EFS helps in providing just that. Unlike EBS, EFS is built using the NFS4.x protocol on SSDs and have a much faster throughput. This also means that EFS is much more expensive than EBS as it can be used on very large analytical workloads. EFS scales up or down based on the size of the files you store and is also accessible from multiple availability zones. The distributed nature of the file system can tempt you to use it as a CDN. But the costs of a CDN outweigh the benefits of using EFS. Hence it is better to use a CDN and use EFS in conjunction with files that can’t be stored on a CDN.

4. Amazon FSx for Lustre

Luster is a file system used for compute-intensive workloads. This mainly comes into the picture when you run machine learning operations on large data sets or when you need to run media encoding workloads. Running Lustre separately requires a lot of expertise in setting it up and configuring it for the right workloads. With the help of Amazon FSx, this can be avoided and a simple interface on the console helps you to quickly get started and start working on your data. The ability to connect it seamlessly to S3 and the option of running it in VPC provides a low cost yet a performant way to achieve your compute-intensive workloads leveraging luster without the administrative overhead of running it.

5. Amazon S3 Glacier

The glacier is used mainly for archival and long-term data storage. This means that there is a low retrieval rate on this storage system due to which it is offered at an extremely cheap rate. It does also come with compliant security features to encrypt your data. Glacier allows you to run queries and analytics on it directly and you will be charged only for the few minutes or hours when you read the data. In terms of durability, it offers 99.(11 nines)% durability which is one of the highest in the industry. Glacier hopes to replace the legacy on-premise tape-based backup service with a much more cost-effective and durable solution.

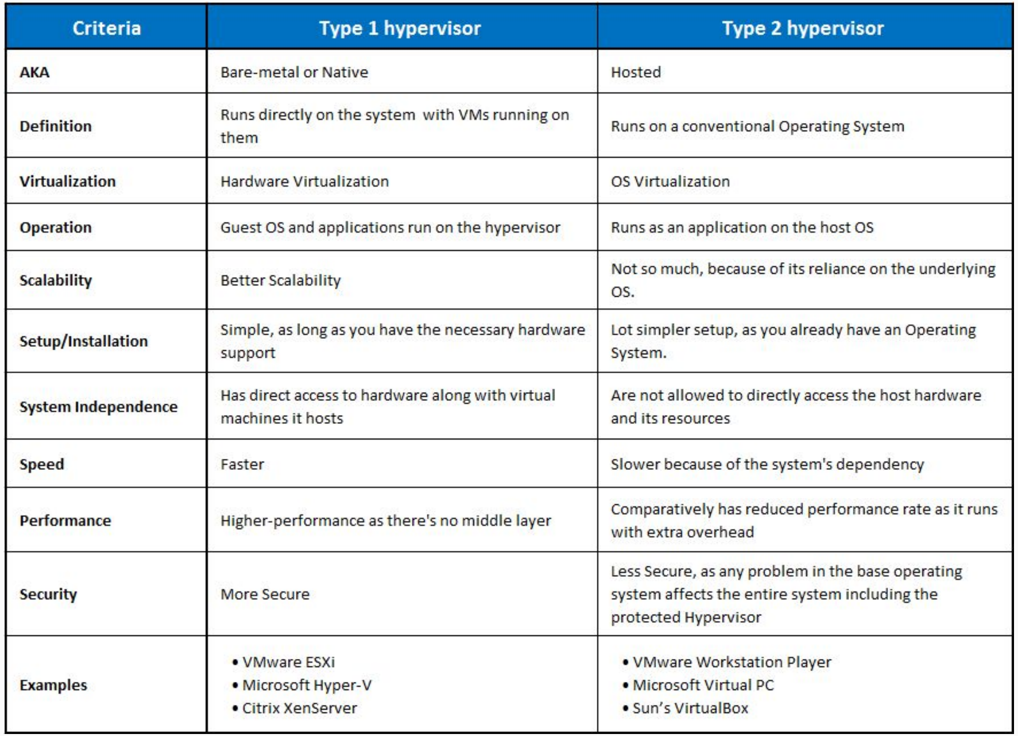
6. Amazon FSx for Windows File Server

Whenever you need to run your windows specific software that needs to access the proprietary windows file system on the cloud, AWS provides you with Amazon FSx to easily achieve that. Windows-based .Net applications, ERPs and CRMs require shared file storage to move workloads between them. Also, Amazon FSx provides support for all native windows based technologies such as NTFS, SMB protocol, Active Directory (AD) and Distributed File System (DFS). Similar to luster, Amazon FSx eliminates the administrative overhead for setting up and maintaining a windows file server and provides you with a simple cost-effective way to run your windows file server on AWS.

Storage Gateways

Storage Gateway is a simple way to let your on-premise applications store, access or archive the data into the AWS cloud. This is achieved by running on a hypervisor on one of the machines in your data center which contains the storage gateway and then is available on AWS to connect to S3, Glacier or EBS. It provides a highly optimized, network resilient and low-cost way to move your data from on-prem to the cloud. Local caching is also available on your on-prem to allow for accessing the more active data. Storage gateway also supports legacy backup stores such as tapes as virtual tapes backed up directly into AWS Glacier.

Hypervisors Type



Criteria	Type 1 hypervisor	Type 2 hypervisor
AKA	Bare-metal or Native	Hosted
Definition	Runs directly on the system with VMs running on them	Runs on a conventional Operating System
Virtualization	Hardware Virtualization	OS Virtualization
Operation	Guest OS and applications run on the hypervisor	Runs as an application on the host OS
Scalability	Better Scalability	Not so much, because of its reliance on the underlying OS.
Setup/Installation	Simple, as long as you have the necessary hardware support	Lot simpler setup, as you already have an Operating System.
System Independence	Has direct access to hardware along with virtual machines it hosts	Are not allowed to directly access the host hardware and its resources
Speed	Faster	Slower because of the system's dependency
Performance	Higher-performance as there's no middle layer	Comparatively has reduced performance rate as it runs with extra overhead
Security	More Secure	Less Secure, as any problem in the base operating system affects the entire system including the protected Hypervisor
Examples	• VMware ESXi • Microsoft Hyper-V • Citrix XenServer	• VMware Workstation Player • Microsoft Virtual PC • Sun's VirtualBox

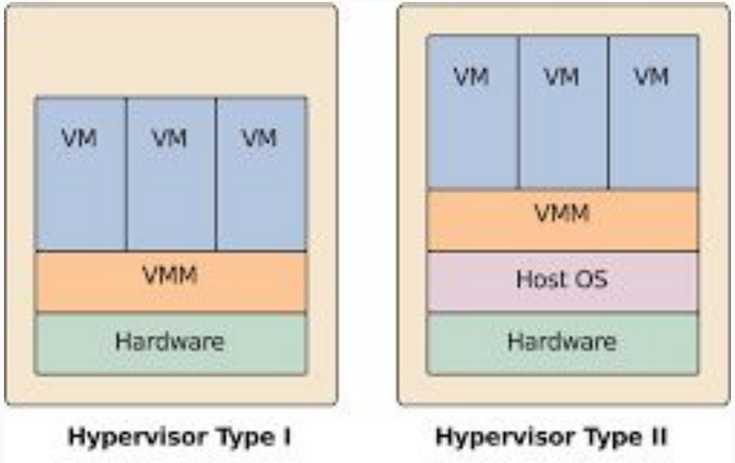


Fig. 2. System VMs.