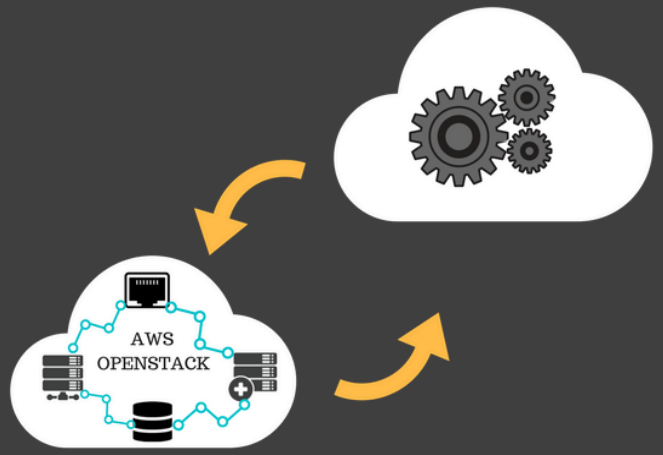
Course and Labs

AWS Design and Automation



Module 4: Design & Automate Compute in AWS
Topic 1: Amazon EC2

Mohanraj Shanmugam

Amazon EC2

AWS Compute services

Compute

Amazon EC2 Instances

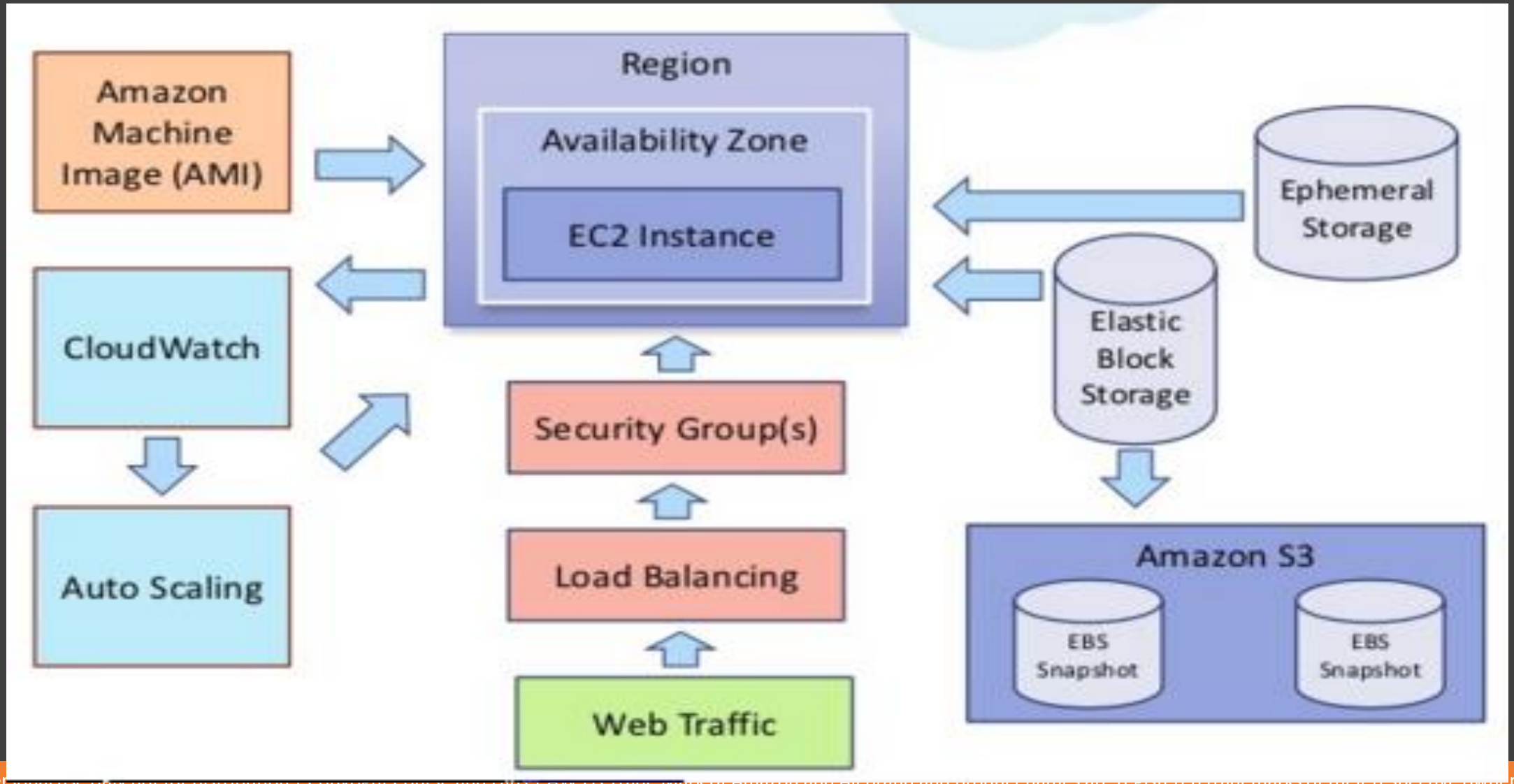
Amazon Elastic Compute Cloud (Amazon EC2) provides scalable computing capacity in the Amazon Web Services (AWS) cloud. Using Amazon EC2 eliminates your need to invest in hardware up front, so you can develop and deploy applications faster.

Business Applications

Docker Containers

Dedicated Host

Amazon EC2 Architecture



EC2 Components

- Virtual computing environments, known as *instances*
- Preconfigured templates for your instances, known as *Amazon Machine Images (AMIs)*
- Various configurations of CPU, memory, storage, and networking capacity for your instances, known as *instance types*
- Secure login information for your instances using *key pairs* (AWS stores the public key, and you store the private key in a secure place)
- Storage volumes for temporary data that's deleted when you stop or terminate your instance, known as *instance store volumes*
- Persistent storage volumes for your data using Amazon Elastic Block Store (Amazon EBS), known as *Amazon EBS volumes*

EC2 Components

- Persistent storage volumes for your data using Amazon Elastic Block Store (Amazon EBS), known as *Amazon EBS volumes*
- A firewall that enables you to specify the protocols, ports, and source IP ranges that can reach your instances using *security groups*
- Static IP addresses for dynamic cloud computing, known as *Elastic IP addresses*
- Metadata, known as *tags*, that you can create and assign to your Amazon EC2 resources
- Virtual networks you can create that are logically isolated from the rest of the AWS cloud, and that you can optionally connect to your own network, known as *virtual private clouds* (VPCs)

Availability Zone

Amazon EC2

volume

Availability Zone

Amazon EC2

volume

KEYPAIR

AMI

snapshot

Elastic IP

Elastic Load Balancing

Amazon CloudWatch

Security Group

region

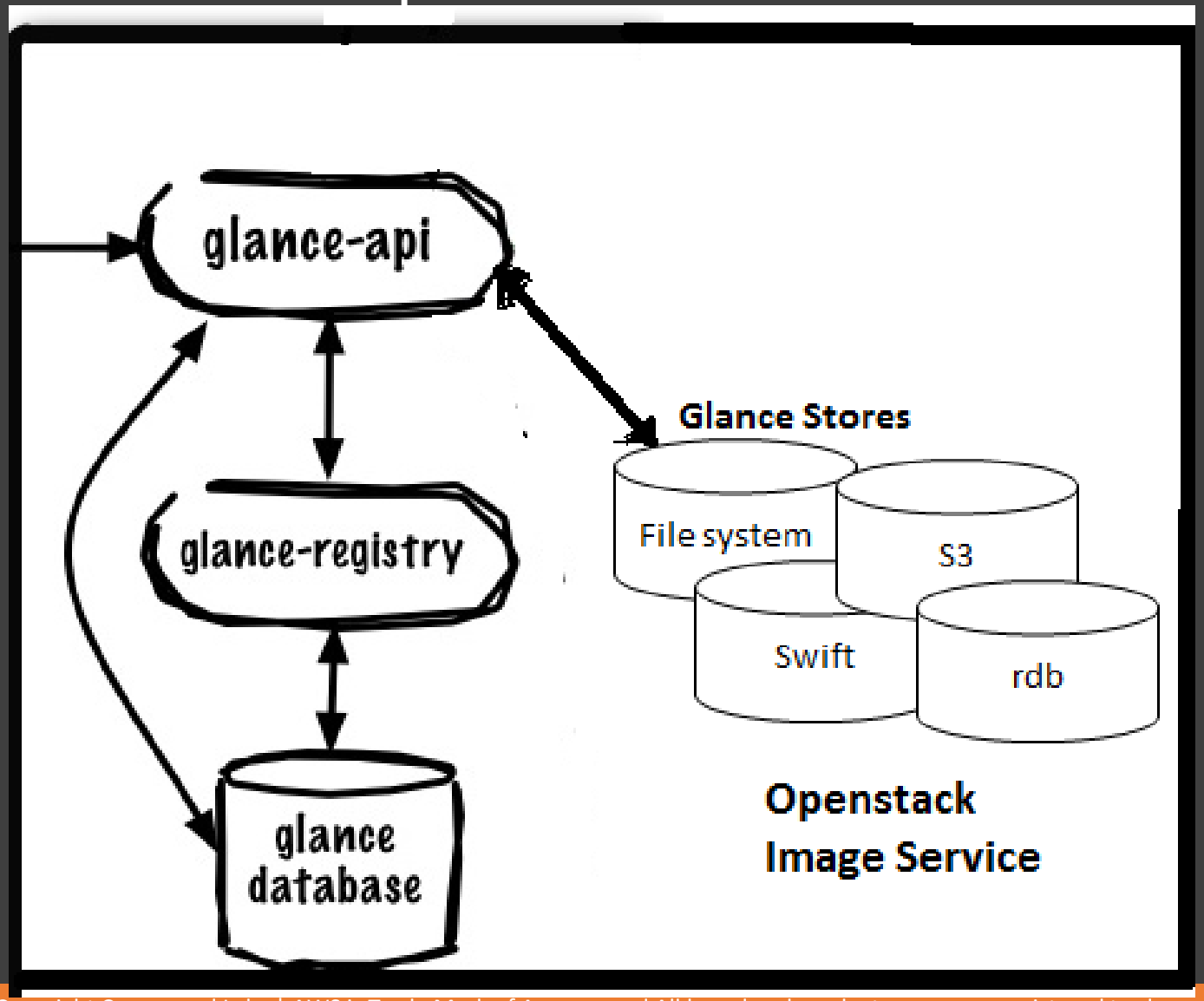
Resource Locations and Scope

Resource	Type	Description
AWS Account	Global	You can use the same AWS account in all regions
Instances	Availability Zone	An instance is tied to the Availability Zones in which you launched it. However, note that its instance ID is tied to the region
EBS Volumes	Availability Zone	An Amazon EBS volume is tied to its Availability Zone and can be attached only to instances in the same Availability Zone.
EBS Snapshots	Regional	An EBS snapshot is tied to its region and can only be used to create volumes in the same region. You can copy a snapshot from one region to another. For more information
Elastic IP Addresses	Regional	An Elastic IP address is tied to a region and can be associated only with an instance in the same region.
AMIs	Regional	An AMI is tied to the region where its files are located within Amazon S3.You can copy an AMI from one region to another.
Security Groups	Regional	A security group is tied to a region and can be assigned only to instances in the same region. You can't enable an instance to communicate with an instance outside its region using security group rules. Traffic from an instance in another region is seen as WAN bandwidth.
User-Supplied Resource Names	Regional	Each resource name, such as a security group name or key pair name, is tied to its region and can be used only in the region where you created the resource. Although you can create resources with the same name in multiple regions, they aren't related to each other
Amazon EC2 Resource Identifiers	Regional	Each resource identifier, such as an AMI ID, instance ID, EBS volume ID, or EBS snapshot ID, is tied to its region and can be used only in the region where you created the resource
Key Pairs	Global or Regional	You can use the key pairs that you create using Amazon EC2 only in the region where you created them. You can create and upload an RSA key pair that you can use in all regions.

Amazon Machine Images (AMI)

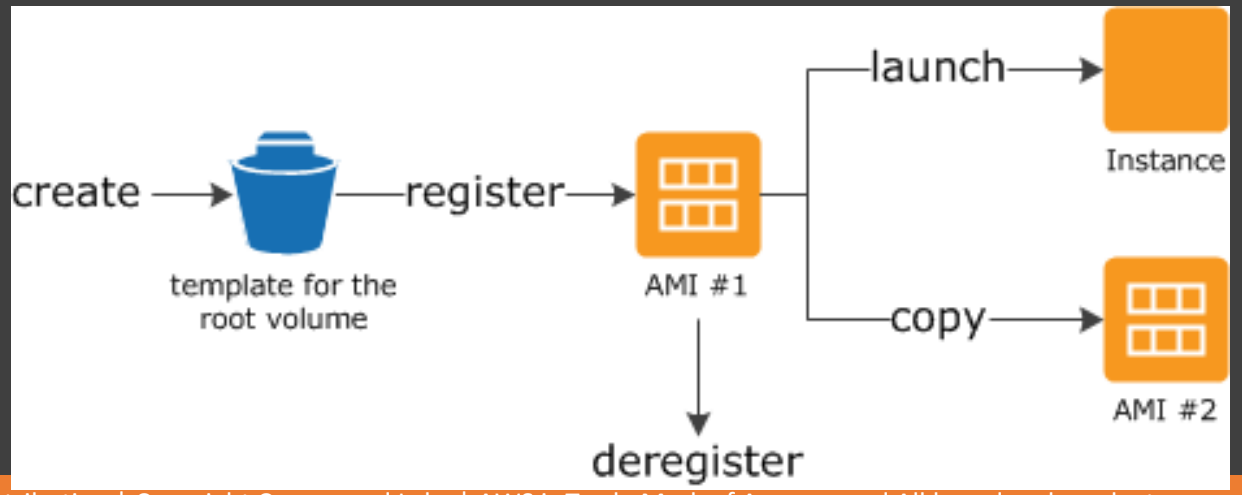
- An Amazon Machine Image (AMI) provides the information required to launch an instance, which is a virtual server in the cloud.
- You specify an AMI when you launch an instance, and you can launch as many instances from the AMI as you need.
- An AMI includes the following:
  - A template for the root volume for the instance (for example, an operating system, an application server, and applications)
  - Launch permissions that control which AWS accounts can use the AMI to launch instances
  - A block device mapping that specifies the volumes to attach to the instance when it's launched

Image Store Examples



AMI lifecycle

- Create a AMI
- Register a AMI
- launch new instances.
- copy an AMI to the same region or to different regions.
- Deregister the AMI Once finished launching the Instance



Selecting an AMI

- You can select an AMI to use based on the following characteristics:
  - Region Availability
  - Operating system
  - Architecture (32-bit or 64-bit)
  - Launch Permissions
  - Storage for the Root Device

AMI Launch Permission

- The owner of an AMI determines its availability by specifying launch permissions. Launch permissions fall into the following categories.

Launch Permission	Description
public	The owner grants launch permissions to all AWS accounts.
explicit	The owner grants launch permissions to specific AWS accounts.
implicit	The owner has implicit launch permissions for an AMI.

- Amazon and the Amazon EC2 community provide a large selection of public AMIs.

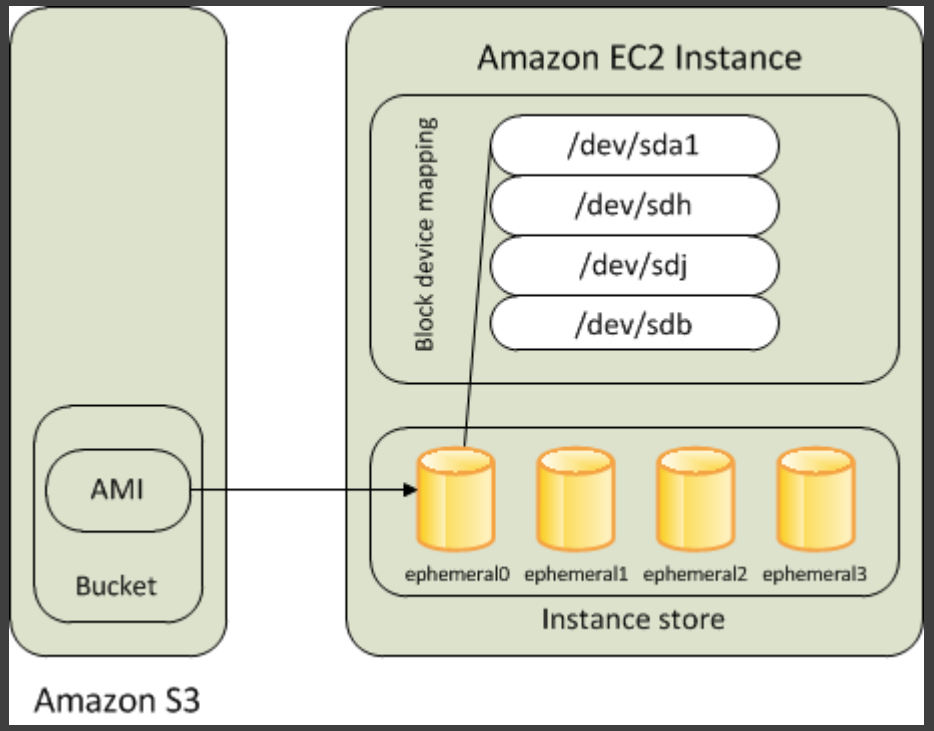
Shared and Paid AMI

- *A shared AMI* is an AMI that a developer created and made available for other developers to use. One of the easiest ways to get started with Amazon EC2 is to use a shared AMI that has the components you need and then add custom content. You can also create your own AMIs and share them with others.
- You use a shared AMI at your own risk. Amazon can't vouch for the integrity or security of AMIs shared by other Amazon EC2 users.
- A *paid AMI* is an AMI that you can purchase from a developer.
- Amazon EC2 integrates with AWS Marketplace, enabling developers to charge other Amazon EC2 users for the use of their AMIs or to provide support for instances.

AMI Virtualization Types

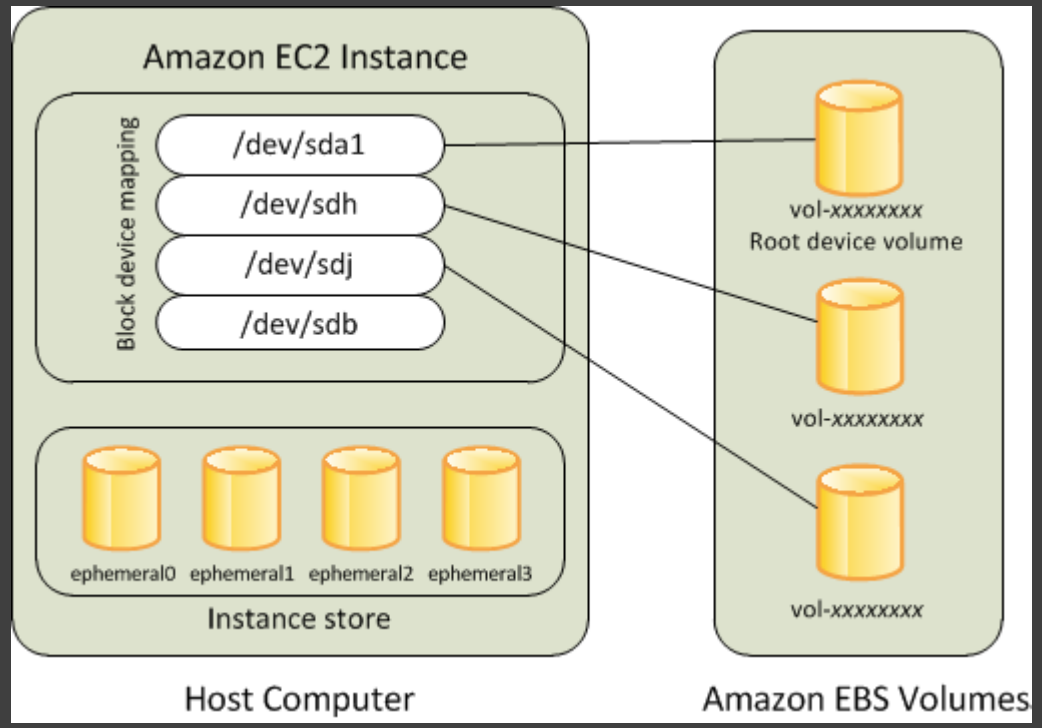
- Linux Amazon Machine Images use one of two types of virtualization: paravirtual (PV) or hardware virtual machine (HVM).
- For the best performance, we recommend that you use current generation instance types and HVM AMIs when you launch your instances.
- HVM AMIs are presented with a fully virtualized set of hardware and boot by executing the master boot record of the root block device of your image. This virtualization type provides the ability to run an operating system directly on top of a virtual machine without any modification, as if it were run on the bare-metal hardware.
- PV AMIs boot with a special boot loader called PV-GRUB, which starts the boot cycle and then chain loads the kernel specified in the menu.lst file on your image.

Storage for the Root Device



- All AMIs are *backed by*
  - *Amazon EBS*
  - *instance store*
- Instance Store
  - root device for an instance launched from the AMI is an instance store volume created from a template stored in Amazon S3.
  - Any data on the instance store volumes persists as long as the instance is running, but this data is deleted when the instance is terminated
  - After an instance store-backed instance fails or terminates, it cannot be restored.
  - If you plan to use Amazon EC2 instance store-backed instances, we highly recommend that you distribute the data on your instance stores across multiple Availability Zones.
  - You should also back up the data on your instance store volumes to persistent storage on a regular basis.

Storage for the Root Device



- *Amazon EBS* Backed AMI
  - root device for an instance launched from the AMI is an Amazon EBS volume created from an Amazon EBS snapshot.
  - Instances that use Amazon EBS for the root device automatically have an Amazon EBS volume attached.
  - When you launch an Amazon EBS-backed instance, we create an Amazon EBS volume for each Amazon EBS snapshot referenced by the AMI you use.
  - An Amazon EBS-backed instance can be stopped and later restarted without affecting data stored in the attached volumes.

Storage for the Root Device

- Amazon EBS-backed instance is in a stopped state you can:
  - modify the properties of the instance
  - change the size of your instance
  - update the kernel
  - attach your root volume to a different running instance
- By default, the root device volume and the other Amazon EBS volumes attached when you launch an Amazon EBS-backed instance are automatically deleted when the instance terminates.
- By default, any Amazon EBS volumes that you attach to a running instance are detached with their data intact when the instance terminates. You can attach a detached volume to any running instance.

EC2 Networks

Amazon EC2 Instance IP Addressing

- **Private IP Addresses and Internal DNS Hostnames**
  - A private IP address is an IP address that's not reachable over the Internet.
  - You can use private IP addresses for communication between instances in the same network
  - When you launch an instance, we allocate a private IP address for the instance using DHCP.
  - Each instance is also given an internal DNS hostname that resolves to the private IP address of the instance
  - `ip-10-251-50-12.ec2.internal`. You can use the internal DNS hostname for communication between instances in the same network, but we can't resolve the DNS hostname outside the network that the instance is in.

Default VPC IP Addressing

- EC2 Classic and Default VPC
  - Any AWS account created after 12/04/2013 will have default VPC by default
  - The Account created before that have a option to create a EC2 classic and Default VPC
  - EC2-Classic will assign Private and Public IP by default to all instances
  - Default VPC will by default assign private address, Public Address needs to done optionally while creating or assign Elastic IP after creating
  - We will see detail of EC2 and Default VPC network in Networking sessions
  - EC2-Classic, we release the private IP address when the instance is stopped or terminated. If you restart your stopped instance, it receives a new private IP address.
  - For instances launched in a VPC, a private IP address remains associated with the network interface when the instance is stopped and restarted, and is released when the instance is terminated.
- Make sure you have ACLs and Security group access to access Amazon DNS server for Port 53 for lookups

Public IP Addresses and External DNS Hostnames

- A public IP address is reachable from the Internet.
- You can use public IP addresses for communication between your instances and the Internet.
- Each instance that receives a public IP address is also given an external DNS hostname
- `ec2-203-0-113-25.compute-1.amazonaws.com`. We resolve an external DNS hostname to the public IP address of the instance outside the network of the instance, and to the private IP address of the instance from within the network of the instance.
- **The public IP address is mapped to the primary private IP address through network address translation (NAT).**

Public IP Addresses and External DNS Hostnames

- When you launch an instance in EC2-Classic, we automatically assign a public IP address to the instance. You cannot modify this behavior.
- When you launch an instance into a VPC, your subnet has an attribute that determines whether instances launched into that subnet receive a public IP address.
- By default, EC2 don't automatically assign a public IP address to an instance that you launch in a non default subnet.
- You can control whether your instance in a VPC receives a public IP address by doing the following:
  - Modifying the public IP addressing attribute of your subnet.
  - Enabling or disabling the public IP addressing feature during launch,

Public IP Addresses and External DNS Hostnames

- A public IP address is assigned to your instance from Amazon's pool of public IP addresses, and is not associated with your AWS account. When a public IP address is disassociated from your instance, it is released back into the public IP address pool, and you cannot reuse it.
- You cannot manually associate or disassociate a public IP address from your instance.
- Instead, in certain cases, we release the public IP address from your instance, or assign it a new one:
  - We release the public IP address for your instance when it's stopped or terminated. Your stopped instance receives a new public IP address when it's restarted.
  - We release the public IP address for your instance when you associate an Elastic IP address with your instance, or when you associate an Elastic IP address with the primary network interface (eth0) of your instance in a VPC. When you disassociate the Elastic IP address from your instance, it receives a new public IP address.
  - If the public IP address of your instance in a VPC has been released, it will not receive a new one if there is more than one network interface attached to your instance.
- If you require a persistent public IP address that can be associated to and from instances as you require, use an Elastic IP address instead. You can allocate your own Elastic IP address, and associate it with your instance.

Elastic IP Addresses

- An *Elastic IP address* is a static IP address designed for dynamic cloud computing.
- With an Elastic IP address, you can mask the failure of an instance or software by rapidly remapping the address to another instance in your account.
- Your Elastic IP address is associated with your AWS account, not a particular instance, and it remains associated with your account until you choose to release it explicitly.
- By default, all AWS accounts are limited to 5 EIPs, because public (IPv4) Internet addresses are a scarce public resource. We strongly encourage you to use an Elastic IP address primarily for the ability to remap the address to another instance in the case of instance failure, and to use DNS hostnames for all other inter-node communication.

Elastic IP Lifecycle

- Allocating an Elastic IP Address
  - It will allocate a Public IP address to your AWS account from the Pool
- Associate Elastic IP Address
  - Associating Elastic IP to Running Instances and NAT to the Private IP of the Instance
- Disassociate Elastic IP address
  - Remove association of the IP to the node and made it available in your VPC
- Release Elastic IP address
  - Release the IP address from your pool

Security Groups

Security Groups

- A *security group* acts as a virtual firewall that controls the traffic for one or more instances.
- When you launch an instance, you associate one or more security groups with the instance.
- You add rules to each security group that allow traffic to or from its associated instances.
- You can modify the rules for a security group at any time; the new rules are automatically applied to all instances that are associated with the security group.
- When we decide whether to allow traffic to reach an instance, we evaluate all the rules from all the security groups that are associated with the instance.

Security Group Rules

- The rules of a security group control the inbound traffic that's allowed to reach the instances that are associated with the security group and the outbound traffic that's allowed to leave them.
- The following are the characteristics of security group rules:
  - By default, security groups allow all outbound traffic.
  - Security group rules are always permissive; you can't create rules that deny access.
  - You can add and remove rules ,modify existing rules, and copy the rules from an existing security group to a new security group.
  - When you add or remove rules, your changes are automatically applied to the instances associated with the security group after a short period, depending on the connection tracking for the traffic.
  - Security groups are stateful — if you send a request from your instance, the response traffic for that request is allowed to flow in regardless of inbound security group rules. For VPC security groups, this also means that responses to allowed inbound traffic are allowed to flow out, regardless of outbound rules.

Security Group Rules

- **Connection Tracking**
  - Your security groups use connection tracking to track information about traffic to and from the instance.
  - Rules are applied based on the connection state of the traffic to determine if the traffic is allowed or denied.
  - This allows security groups to be stateful — responses to inbound traffic are allowed to flow out of the instance regardless of outbound security group rules, and vice versa.
  - For example, if you initiate an ICMP `ping` command to your instance from your home computer, and your inbound security group rules allow ICMP traffic, information about the connection (including the port information) is tracked. Response traffic from the instance for the `ping` command is not tracked as new request, but rather as an established connection and is allowed to flow out of the instance, even if your outbound security group rules restrict outbound ICMP traffic.

Default Security Groups

- When you create a VPC, we automatically create a default security group for the VPC.
- If you don't specify a different security group when you launch an instance, the instance is automatically associated with the appropriate default security group.
- A default security group is named `default`, and it has an ID assigned by AWS. The following are the initial settings for each default security group:
  - Allow inbound traffic only from other instances associated with the default security group
  - Allow all outbound traffic from the instance
- You can change the rules for a default security group. For example, you can add an inbound rule to allow SSH connections so that specific hosts can manage the instance.

Custom Security Groups

- If you don't want all your instances to use the default security group, you can create your own security groups and specify them when you launch your instances.
- If you don't want all your instances to use the default security group, you can create your own security groups and specify them when you launch your instances.

Security Group Lifecycle

- Creating a Security Group
- Copy a Security Group
- Add Rules to Security Group
- Assaign a Security Group to a instance
- Change Security Group to a Instance
- Delete Rules to Security Group
- Delete a Security Group

Key Pairs

Amazon EC2 Key Pairs

- Amazon EC2 uses public–key cryptography to encrypt and decrypt login information.
- Public–key cryptography uses a public key to encrypt a piece of data, such as a password, then the recipient uses the private key to decrypt the data.
- The public and private keys are known as a *key pair*.
- To log in to your instance, you must create a key pair, specify the name of the key pair when you launch the instance, and provide the private key when you connect to the instance.
- Linux instances have no password, and you use a key pair to log in using SSH. With Windows instances, you use a key pair to obtain the administrator password and then log in using RDP.

Creating a Key Pair

- You can use Amazon EC2 to create your key pair.
- Alternatively, you could use a third-party tool and then import the public key to Amazon EC2.
- Each key pair requires a name. Be sure to choose a name that is easy to remember. Amazon EC2 associates the public key with the name that you specify as the key name.
- Amazon EC2 stores the public key only, and you store the private key. Anyone who possesses your private key can decrypt your login information, so it's important that you store your private keys in a secure place.
- The keys that Amazon EC2 uses are 2048-bit SSH-2 RSA keys. You can have up to five thousand key pairs per region.

Creating a Key Pair

- When you launch an instance, you should specify the name of the key pair you plan to use to connect to the instance.
- If you don't specify the name of an existing key pair when you launch an instance, you won't be able to connect to the instance.
- When you connect to the instance, you must specify the private key that corresponds to the key pair you specified when you launched the instance.
- Amazon EC2 doesn't keep a copy of your private key; therefore, if you lose a private key, there is no way to recover it.
- If you lose the private key for an instance store-backed instance, you can't access the instance; you should terminate the instance and launch another instance using a new key pair.
- If you lose the private key for an EBS-backed instance, you can regain access to your instance. You must stop the instance, detach its root volume and attach it to another instance as a data volume, modify the `authorized_keys` file, move the volume back to the original instance, and restart the instance.

Key Pairs for Multiple Users

- If you have several users that require access to a single instance, you can add user accounts to your instance.
- You can create a key pair for each user, and add the public key information from each key pair to the `.ssh/authorized_keys` file for each user on your instance. You can then distribute the private key files to your users.
- That way, you do not have to distribute the same private key file that's used for the root account to multiple users.

Key Pair Lifecycle

- Creating Your Key Pair Using Amazon EC2
- Importing Your Own Key Pair to Amazon EC2
- Retrieving the Public Key for Your Key Pair on Linux
- Retrieving the Public Key for Your Key Pair on Windows
- Verifying Your Key Pair's Fingerprint
- Deleting Your Key Pair
- Connecting to Your Linux Instance if You Lose Your Private Key

AMAZON EC2 INSTANCES

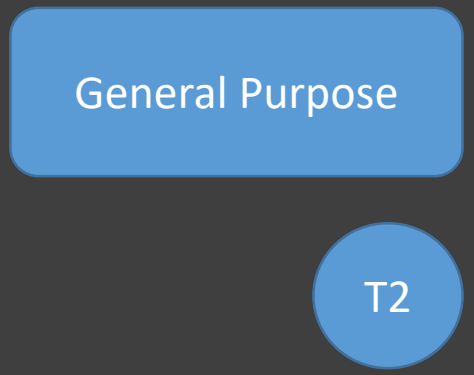
Amazon EC2 Instances Types

- General Purpose
- Compute Optimized
- Memory Optimized
- GPU Optimized
- Storage Optimized

Amazon EC2 Pricing Model

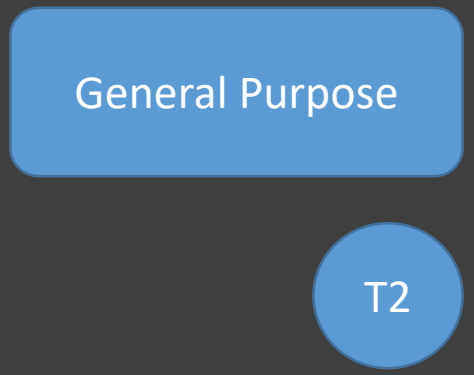
- EC2 is charged per running hour
- Here are the pricing types:
  - On-Demand instances
    - Pay for the instances that you use by the hour, with no long-term commitments or up-front payments.
  - Reserved Instances
    - Make a low, one-time, up-front payment for an instance, reserve it for a one- or three-year term, and pay a significantly lower hourly rate for these instances.
  - Spot instances
    - Specify the maximum hourly price that you are willing to pay to run a particular instance type. The Spot price fluctuates based on supply and demand, but you never pay more than the maximum price you specified. If the Spot price moves higher than your maximum price, Amazon EC2 shuts down your Spot instances.
- Detail Pricing at
  - http://aws.amazon.com/ec2/pricing/

AMAZON EC2 INSTANCES – T2



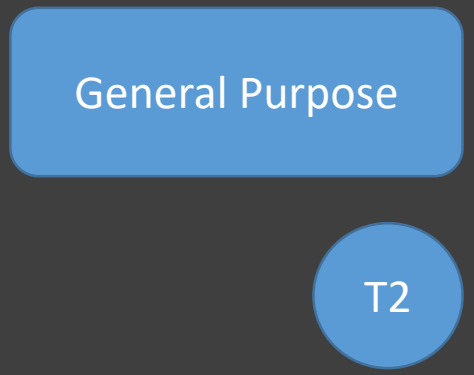
- **Features:**
- High Frequency Intel Xeon Processors with Turbo up to 3.3GHz
- Burstable CPU, governed by CPU Credits, and consistent baseline performance
- Lowest-cost general purpose instance type, and Free Tier eligible (t2.micro only)
- Balance of compute, memory, and network resources

AMAZON EC2 INSTANCES – T2



- T2 Instances are Busrtable Performance Instances
- Burstable Performance Instances provide a baseline level of CPU performance with the ability to burst above the baseline like CPU Overclocking
- Each T2 instance would get CPU credits based on the Instance Size
- CPU Credits equals to pie of a CPU Core Capacity
- Consider CPU core is 3.3 Ghz (ie 3.3 * 1000 * 1000 * 1000 process per second), a CPU core will have 10 CPU credit then 1 credit is equal to 0.33 ghz
- Now a T2 Instance will have assigned credit for example a t2.small instance have 10 credits per hour assigned that means it can use up to .33 ghz of CPU power

AMAZON EC2 INSTANCES – T2



- If T2 instances does not use the credit in the given hour it will store that as a CPU Credit balance
- For example the T2.small instance gets 10 cpu credit within 1AM to 2 AM but it only uses 6 CPU credits , It will store 4 CPU credits as Credit Balance.
- At 6 AM to 7 AM you need CPU speed more than 0.33 ghz then it will take the CPU credit balance and scale more.
- CPU credit balance reset once in 24 hours

AMAZON EC2 INSTANCES – T2

General Purpose

T2

T2 Instance Variants

Model	vCPU	CPU Credits / hour	Mem (GiB)	Storage
t2.nano	1	3	0.5	EBS-Only
t2.micro	1	6	1	EBS-Only
t2.small	1	12	2	EBS-Only
t2.medium	2	24	4	EBS-Only
t2.large	2	36	8	EBS-Only

AMAZON EC2 INSTANCES – T2

General Purpose

T2

- Use Cases: This instance are used when you have variable Compute Requirement like low traffic Web servers, Development Environment and small databases
- Management: Over time, if you find your workload needs more CPU Credits than you have, or your instance does not maintain a positive CPU Credit balance then scale up the size of instance.

AMAZON EC2 INSTANCES – M4

General Purpose

M4

- This family provides a balance of compute, memory, and network resources, and it is a good choice for many applications.
- Features:
  - 2.4 GHz Intel Xeon® E5-2676 v3 (Haswell) processors
  - EBS-optimized by default at no additional cost
  - Support for Enhanced Networking
  - Balance of compute, memory, and network resources
- Use Cases
  - Small and mid-size databases, data processing tasks that require additional memory, caching fleets, and for running backend servers for SAP, Microsoft SharePoint, cluster computing, and other enterprise applications.

AMAZON EC2 INSTANCES – M4

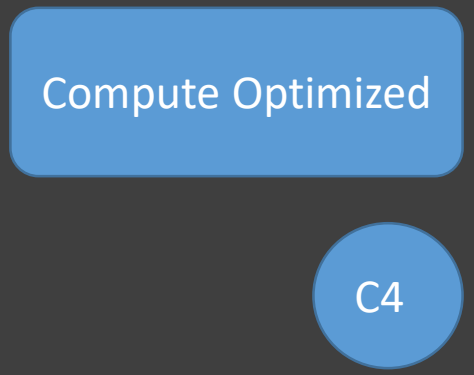
General Purpose

M4

Model	vCPU	Mem (GiB)	SSD Storage (GB)	Dedicated EBS Throughput (Mbps)
m4.large	2	8	EBS-only	450
m4.xlarge	4	16	EBS-only	750
m4.2xlarge	8	32	EBS-only	1,000
m4.4xlarge	16	64	EBS-only	2,000
m4.10xlarge	40	160	EBS-only	4,000

AMAZON EC2 INSTANCES – C4 – Compute Optimized

Course and Labs



- C4 instances are the latest generation of Compute-optimized instances, featuring the highest performing processors and the lowest price/compute performance in EC2.
- Features:
  - High frequency Intel Xeon E5-2666 v3 (Haswell) processors optimized specifically for EC2
  - EBS-optimized by default and at no additional cost
  - Ability to control processor C-state and P-state configuration on the c4.8xlarge instance type
  - Support for Enhanced Networking and Clustering
- Use Cases
  - High performance front-end fleets, web-servers, batch processing, distributed analytics, high performance science and engineering applications, ad serving, MMO gaming, and video-encoding.

AMAZON EC2 INSTANCES – C4 – Compute Optimized

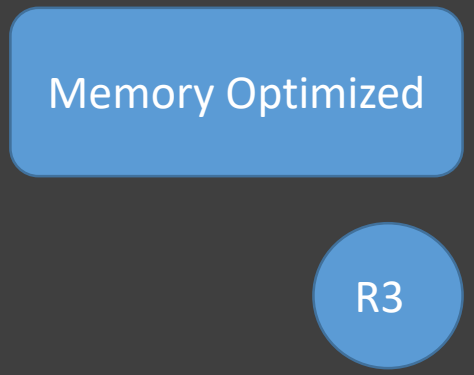
Compute Optimized

C4

Model	vCPU	Mem (GiB)	Storage	Dedicated EBS Throughput (Mbps)
c4.large	2	3.75	EBS-Only	500
c4.xlarge	4	7.5	EBS-Only	750
c4.2xlarge	8	15	EBS-Only	1,000
c4.4xlarge	16	30	EBS-Only	2,000
c4.8xlarge	36	60	EBS-Only	4,000

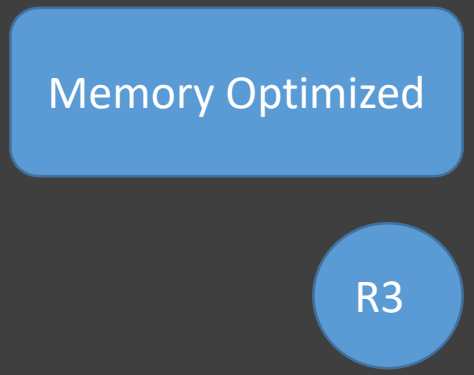
AMAZON EC2 INSTANCES – R3 – Memory Optimized

Course and Labs



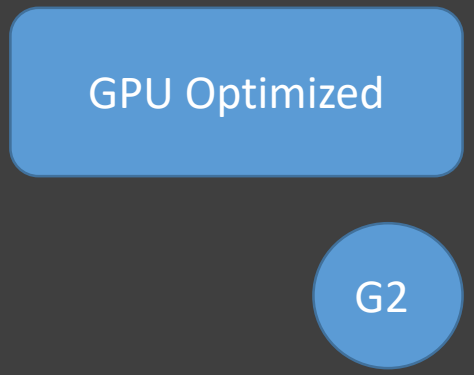
- R3 instances are optimized for memory-intensive applications and have the lowest cost per GiB of RAM among Amazon EC2 instance types.
- Features:
  - High Frequency Intel Xeon E5-2670 v2 (Ivy Bridge) Processors
  - Lowest price point per GiB of RAM
  - SSD Storage
  - Support for Enhanced Networking
- Use Cases
  - We recommend memory-optimized instances for high performance databases, distributed memory caches, in-memory analytics, genome assembly and analysis, larger deployments of SAP, Microsoft SharePoint, and other enterprise applications.

AMAZON EC2 INSTANCES – R3 – Memory Optimized



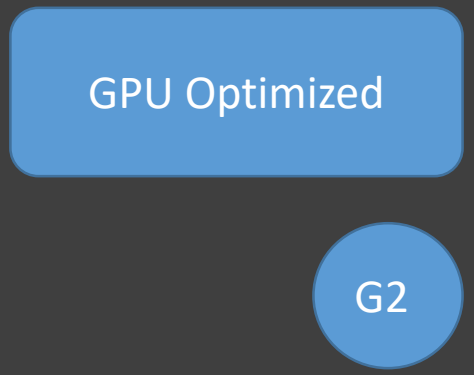
Model	vCPU	Mem (GiB)	SSD Storage (GB)
r3.large	2	15.25	1 x 32
r3.xlarge	4	30.5	1 x 80
r3.2xlarge	8	61	1 x 160
r3.4xlarge	16	122	1 x 320
r3.8xlarge	32	244	2 x 320

AMAZON EC2 INSTANCES – G2 – GPU Optimized



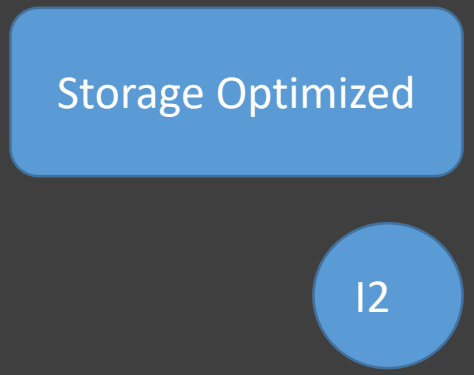
- This family includes G2 instances intended for graphics and general purpose GPU compute applications.
- Features:
  - High Frequency Intel Xeon E5-2670 (Sandy Bridge) Processors
  - High-performance NVIDIA GPUs, each with 1,536 CUDA cores and 4GB of video memory
  - Each GPU features an on-board hardware video encoder designed to support up to eight real-time HD video streams (720p@30fps) or up to four real-time full HD video streams (1080p@30fps)
  - Support for low-latency frame capture and encoding for either the full operating system or select render targets, enabling high-quality interactive streaming experiences
- Use Cases
  - 3D application streaming, machine learning, video encoding, and other server-side graphics or GPU compute workloads.

AMAZON EC2 INSTANCES – G2– GPU Optimized



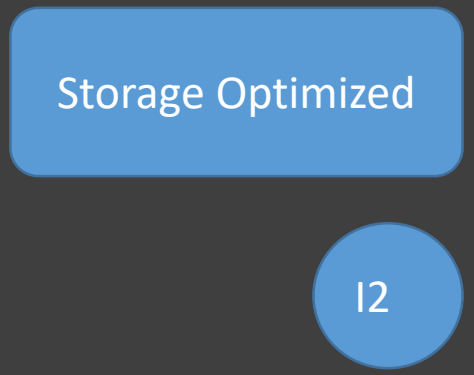
Model	GPUs	vCPU	Mem (GiB)	SSD Storage (GB)
g2.2xlarge	1	8	15	1 x 60
g2.8xlarge	4	32	60	2 x 120

AMAZON EC2 INSTANCES – I2 – Storage Optimized - High I/O Instances



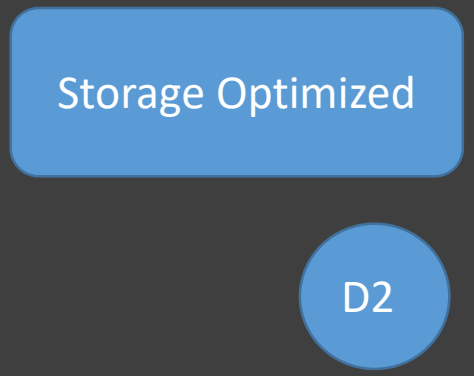
- This family includes G2 instances intended for graphics and general purpose GPU compute applications.
- Features:
  - High Frequency Intel Xeon E5-2670 v2 (Ivy Bridge) Processors
  - SSD Storage
  - Support for TRIM
  - Support for Enhanced Networking
  - High Random I/O performance
- Use Cases
  - NoSQL databases like Cassandra and MongoDB, scale out transactional databases, data warehousing, Hadoop, and cluster file systems.

AMAZON EC2 INSTANCES – I2 – Storage Optimized - High I/O Instances



Model	vCPU	Mem (GiB)	Storage (GB)
i2.xlarge	4	30.5	1 x 800 SSD
i2.2xlarge	8	61	2 x 800 SSD
i2.4xlarge	16	122	4 x 800 SSD
i2.8xlarge	32	244	8 x 800 SSD

AMAZON EC2 INSTANCES – D2 – Storage Optimized - Dense-storage Instances



- D2 instances feature up to 48 TB of HDD-based local storage, deliver high disk throughput, and offer the lowest price per disk throughput performance on Amazon EC2.
- Features:
  - High-frequency Intel Xeon E5-2676v3 (Haswell) processors
  - HDD storage
  - Consistent high performance at launch time
  - High disk throughput
  - Support for Amazon EC2 Enhanced Networking
- Use Cases
  - Massively Parallel Processing (MPP) data warehousing, MapReduce and Hadoop distributed computing, distributed file systems, network file systems, log or data-processing applications

AMAZON EC2 INSTANCES – D2 – Storage Optimized - Dense-storage Instances

Storage Optimized

I2

Model	vCPU	Mem (GiB)	Storage (GB)
d2.xlarge	4	30.5	3 x 2000 HDD
d2.2xlarge	8	61	6 x 2000 HDD
d2.4xlarge	16	122	12 x 2000 HDD
d2.8xlarge	36	244	24 x 2000 HDD

Amazon EC2 Service Level Agreement

- Amazon EC2 and Amazon EBS each available with a Monthly Uptime Percentage (defined below) of at least 99.95%, in each case during any monthly billing cycle (the “Service Commitment”). In the event Amazon EC2 or Amazon EBS does not meet the Service Commitment, you will be eligible to receive a Service Credit as described below.

Less than 99.95% but equal to or greater than 99.0%	10%
Less than 99.0%	30%