Elastic Cloud Compute (EC2)

Instance Types – Availability Zone

DR MC GIFT PX

- D – Dense (Hadoop)
- R – Memory intensive
- M – General Purpose
- C – CPU instenseive
- G – Graphics
- I – IOPS intensive
- F – FPGA
- T – cheap general purpose
- P – General GPU
- X – Memory optimized

Instance type can be changed after launch. You have to stop, change type and start again.
Key Par used to log into instance are regional.
IP (pub, priv) stay the same during reboot

- EC2 can assume role through instance profile (container)

Reserved Instances

```
- If specified AZ, then it guarantees capacity in that zone
- can change instance type withing the same class
- canNOT change system (Linux to Window )
```

VM Import/Export

```
- Can import VM to
    - EC2 instance
    - AMI
```

AMI – Regional

```
1. Creating AMI
    - Start with existing AMI or VM Import/Export
    - Do modification
    - Add necesary EBS & Instance store volumes
    - click on Create AMI
    - Takes a while
2. AMI has specific Virtualiztion (paravirtual or HVM)
3. Block Device Mapping allows you to specify additional EBS or Instance Store
volumes

If instance type has less instance stores than in Block Device Mappings it will
launch with lower nubmer
[Block Device Mapping]
(http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/images/block_device_mapping
_figure.png)

Region:
    - AMI exists in a region, can be copied to another region
    - different ids in regions

Encryption
    - Can use encrypted EBS
    - Can be encrypted using CopyImage from unencrypted
        - Can encrypt from unencrypted root volume
    - Can have EBS encrypted root
    - You cannot turn of encryption

Sharing
    - You can make AMI public (non encrypted)
    - You can share AMI with specific account
        - you have to grant access to snapshot or s3 bucket (Instance Store
backed)
        - you can share encrypted but you also have to share the key
        - can be copied to new account (+ reencrypt)
```

Network And Security

```
## Security Groups - Regional (VPC)
    - When multiple Security Groups are assigned to the instance - union is
used.
    - Exists on only within VPC
    - Statefull
    - Inbound and Outbound
    - Applied to instance
    - You can have multiple security groups associated to the instance
    - Security groups are associated with network interfaces. Changing an
instance's security groups changes the security groups associated with the
primary network interface (eth0)
    - You can assing specific security group to additional interface (Network
Interfaces)
    - Rules are block by default
    - Only Allow rules can be added
    - Rule can have:
        - Protocol
        - Port Range
        - ICMP Type
        - Source or Destination (in or out):
            - IP Address (range, CIDR)
            - Another Security Group
        - Description
## Network Interfaces
    - You can add multiple network interfaces to the same instance
    - For instances launched in a VPC, a private IPv4 address remains
associated with the network interface when the instance is stopped and
restarted, and is released when the instance is terminated.
    - Public IP Adresses are released when instance is stopped
    - Public IP adress is released when Elastic IP Adress is attached
## Elastic IP Address - Regional
    - Does not support Tagging
    - Static public IP Adress
    - Can be assinged to one instance at a time
    - Cost only when not assigned
    - Has to be released
## Placement Group
    - Places Instance within AZ close to each other (logical gropuing)
    - Can be used only with some instances
    - You can get insufficient capacity error if you try to extend number of
instances
    - Stop and start might fail if there's not enough capacity
    - To resolve - stop and start again all instances
    - Placement Group can span peered VPC
    - You can't move existing instance to Placement Group
    - Name has to be unique within AWS Account
    - You can't merge placement groups
```

EFS – REGIONAL

```
- Uses NFSv4 protocol
- Can be attached to multiple servers at a time
- Multi AZ, you can attach EFS to multiple instances in Multiple AZ !!!
- Only within singe VPC at a time
- You can attach to different VPC when you delete all mount points

## Mount target
    To access your Amazon EFS file system in a VPC, you create one or more
mount targets in the VPC. A mount target provides an IP address for an NFSv4
endpoint at which you can mount an Amazon EFS file system
    - One mount per Availability Zone
    - Can be accessed from on-prem using DirectConnect but not VPN
    - You can attach Security Group against your mount target

## Encryption
    - Can be encrypted at rest
    - Have to specified when created
    - You can't enable encryption after EFS is enabled
## Modes
    - Max IO
    - General Purpose
```

Billiong

Billing commences when Amazon EC2 initiates the boot sequence of an AMI instance. Billing ends when the instance terminates, which could occur through a web services command, by running "shutdown –h", or through instance failure.

Assuming a Linux operating system is in use, pricing is per instance–second consumed for all instance types except Dedicated instances, which still bills on an hourly basis, where partial instance–hours consumed are billed as full hours. Windows instances of all types are still billed at on a per–hour basis.