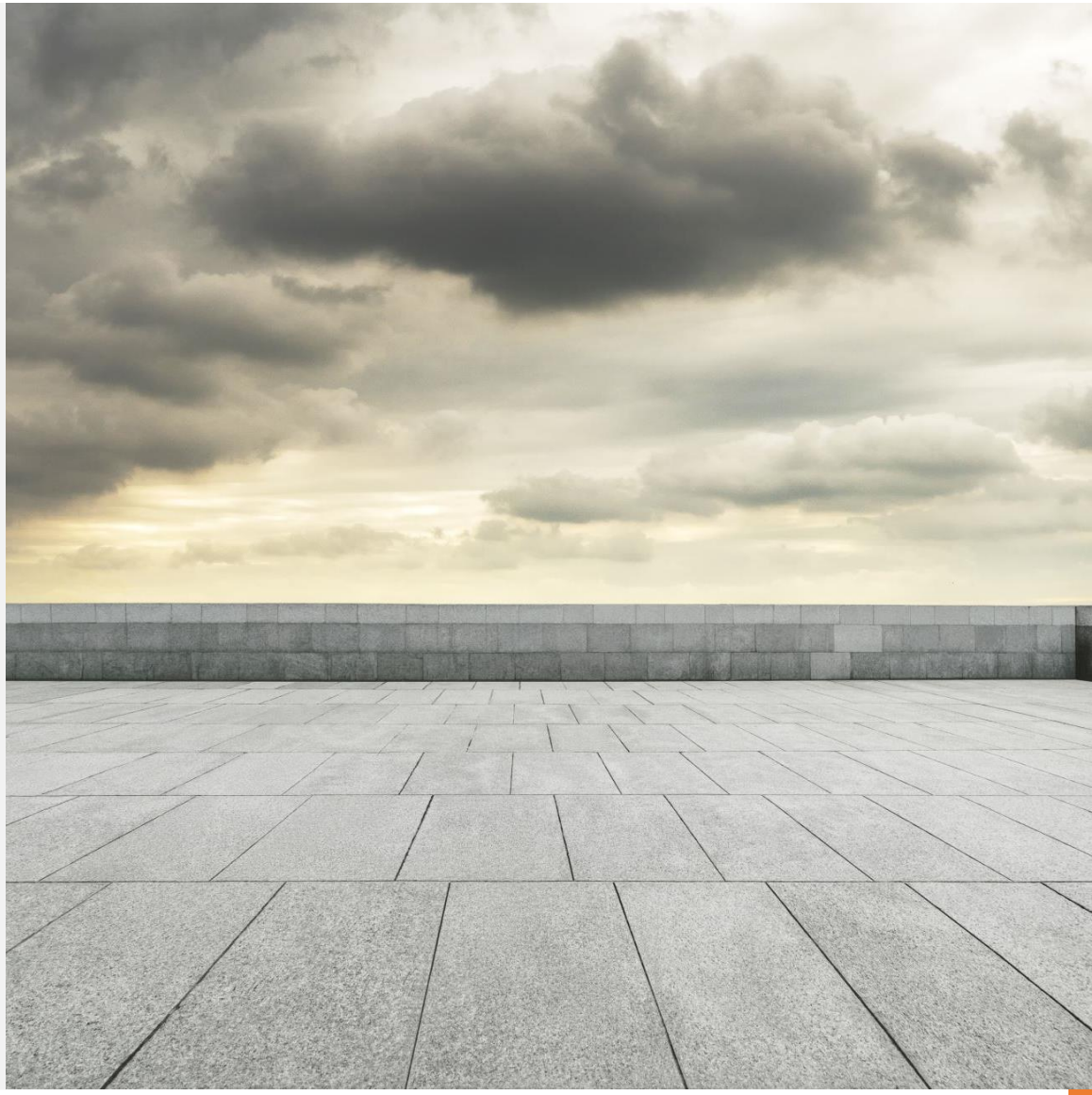
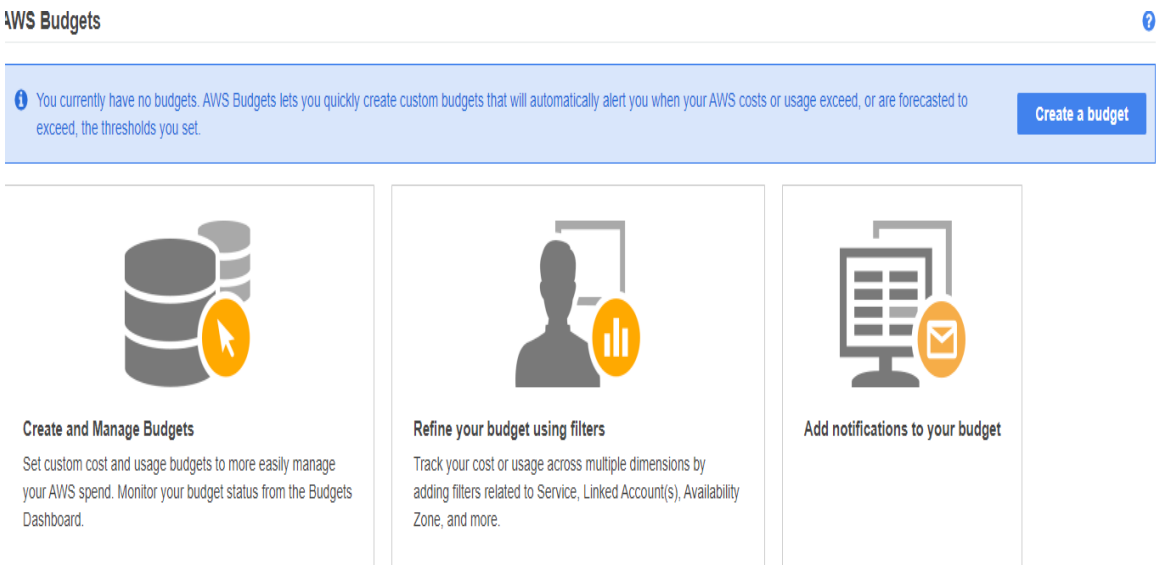
AWS Cloud Practitioner Week-3

Training Course



AWS Budget

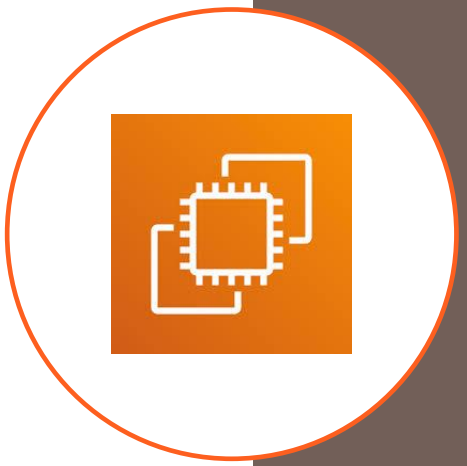
- Create a custom cost budget
  - You can budgets from the billing dashboard
- Alerts you when your cost or usage exceeds your set budget



Amazon EC2

- EC2 = Elastic Compute Cloud (**E with 2 Cs**)
- One the most popular AWS service.
  - EC2 consists of different components:
    - Virtual Volume for storing data (using Elastic Block Storage - EBS)
    - Distributing Load across EC2s (using Elastic Load Balancer – ELB)
    - Scaling the services (using Auto Scaling group (ASG)

EC2 is the first service to know in order to understand how the Cloud works.



EC2 instance types: example

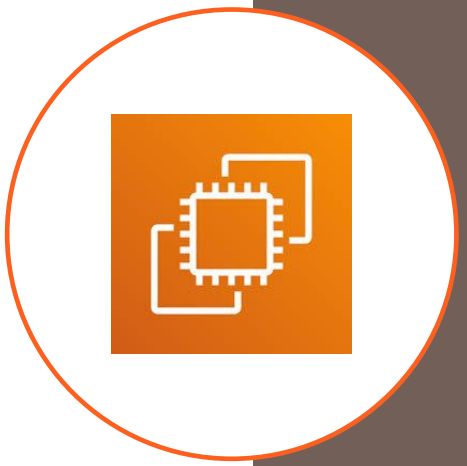
- t2.micro is part of AWS free tier (up to 750 hrs per month)
- There are huge number of different type of instances

Instance	vCPU	Mem (GiB)	Storage	Network Performance	EBS Bandwidth (Mbps)
t2.micro	1	1	EBS-Only	Low to Moderate	
t2.xlarge	4	16	EBS-Only	Moderate	
c5d.4xlarge	16	32	1 x 400 NVMe SSD	Up to 10 Gbps	4,750
r5.16xlarge	64	512	EBS Only	20 Gbps	13,600
m5.8xlarge	32	128	EBS Only	10 Gbps	6,800

https://aws.amazon.com/ec2/instance-types/

EC2 Sizing and Configurations

- Operating System (**OS**): Microsoft Windows or Linux
- How much compute power and cores (**CPU** = Central Processing Unit)
- How much memory – (**RAM** = Random-Access-Memory)
- How much Storage space:
  - Network-attached (**EBS** = Elastic Block Storage)
  - Hardware-attached (**Instance Store**)
- Network selection:
  - Speed of Virtual Network (for some cases more than one NIC can be selected)
- Firewall Rules:
  - **Security Group** attached to EC2 to allow/deny access
- Script: To run automatically during EC2 launch.
  - EC2 **User Data** - (configure at first launch)



User Data Script

- **User data runs only once during the first launch of instance**
- **This sample script**
  - Install security updates from the internet (updates)
  - Install web service on Linux server (httpd)
  - Start web services
  - Enable web services

Copy this and paste it to “User Data” section.

#!/bin/bash

yum update –y

yum install -y httpd

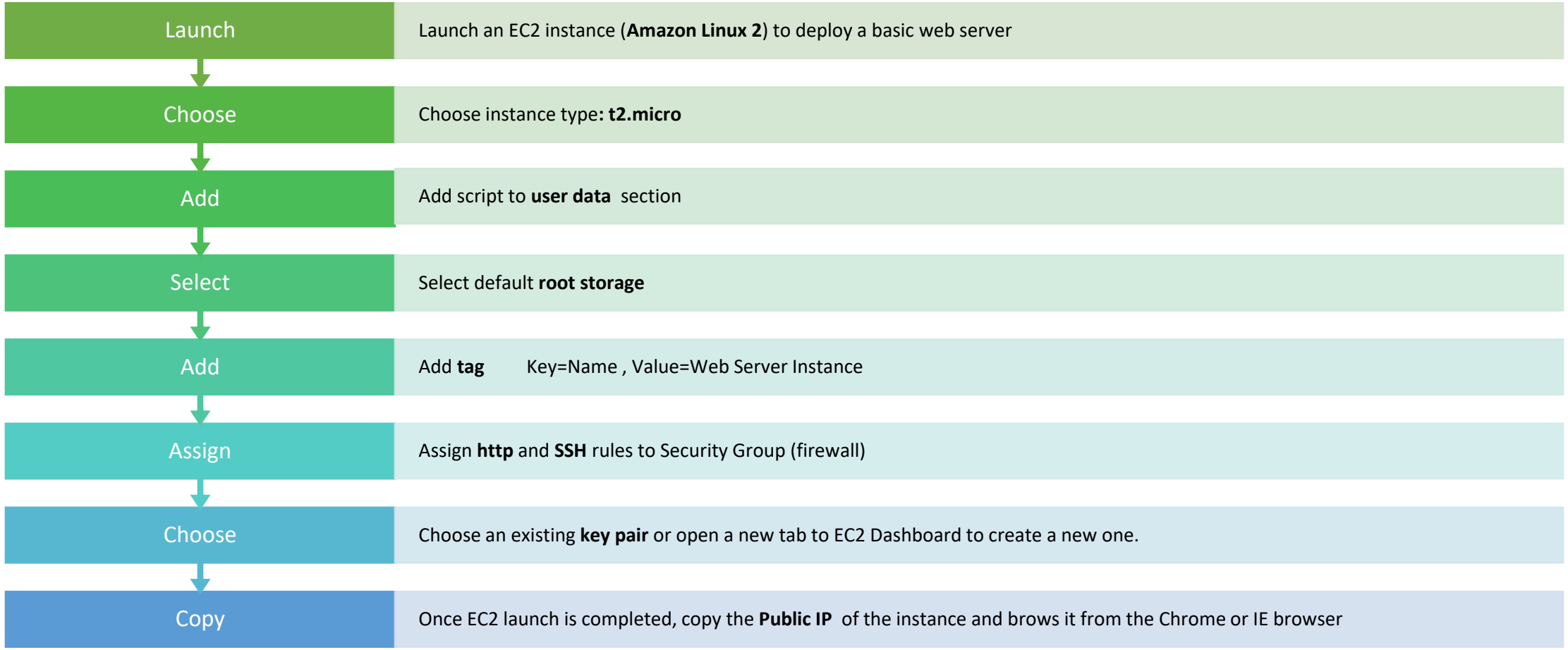
systemctl start httpd

systemctl enable httpd

echo "<h1>Welcome to Baloch Community AWS Training $(hostname -f)</h1>" > /var/www/html/index.html

---

Launching EC2 Hands on with user data

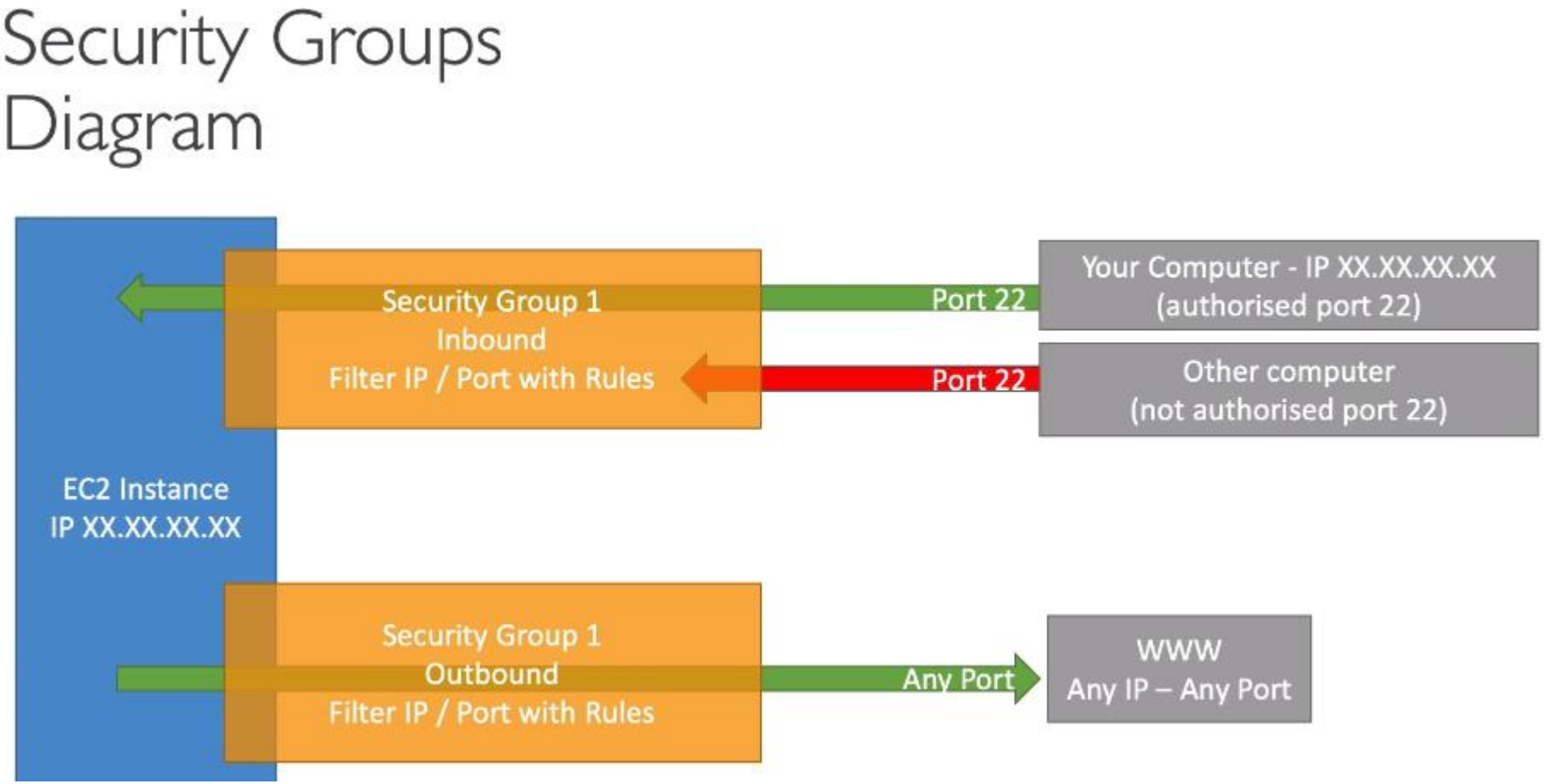


Introduction to **Security Group**

- Security groups are acting as “firewall” on EC2 instances
- They control access to ports and IP address for EC2 instances
- **Control of inbound network: (from others to the instance)**
- **Control of outbound network: (from the instance to others)**
- SGs are **stateful** –
  - any traffic is allowed to instance, response is allowed as well.
  - any traffic is initiated from the instance, response to instance is allowed in.

Type ⓘ	Protocol ⓘ	Port Range ⓘ	Source ⓘ	Description ⓘ
HTTP	TCP	80	0.0.0.0/0	test http page
SSH	TCP	22	122.149.196.85/32	
Custom TCP Rule	TCP	4567	0.0.0.0/0	java app

Security Group Diagram

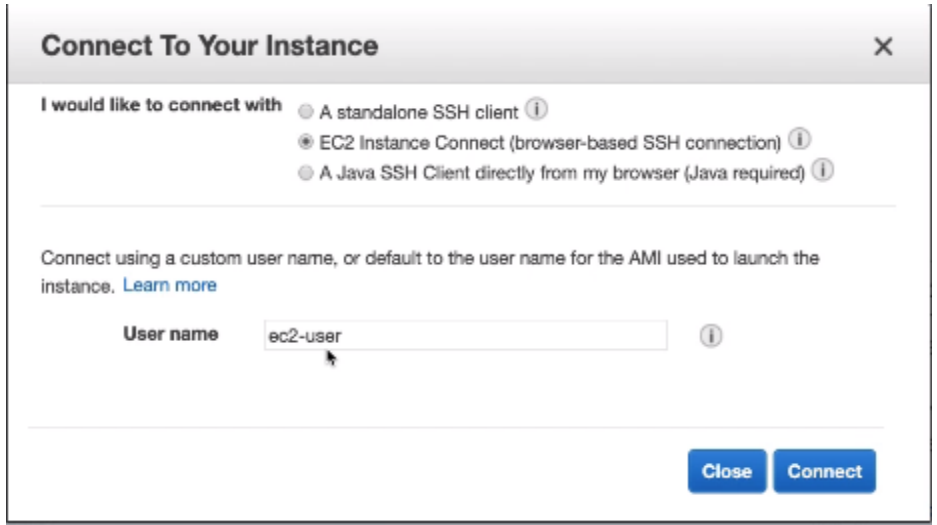


Security Group Lab

- Modify a security group to allow and deny access to a website

Browser Based SSH Connection For Amazon Linux 2

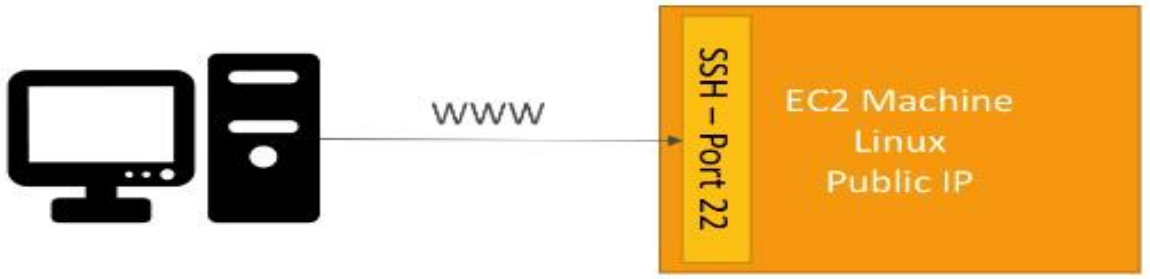
- Select your instance form EC2 Dashboard
- Click – **Connect**
- Select “EC2 Instance Connect (browser-based SSH Connection)
- User-name = ec2-user (for all Amazon Linux Instances)
- This will open a new tab and instantly connects.



How to Connect to a Linux Instance via SSH from your PC

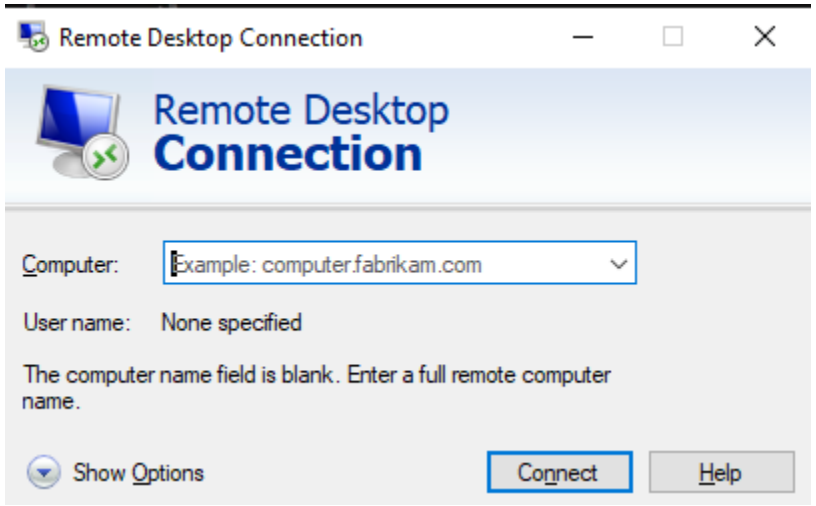
- SSH = Secure Shell
- SSH allows you to connect to remote machine using command line.
- From a command line:

ssh –I *<location of the keypair file>* *ec2-user@<instance_ipaddress>*



How to Connect to a Windows Instance via RDP connection.

- RDP = Remote Desktop Protocol
- RDP allows you to connect to remote Windows machine.
- RDP comes with your Windows 10 PC.
- It needs to be downloaded and installed if you are using a Mac PC.



For Exam

- You should know these basic Ports and their usage:

  - 22 = SSH (Secure Shell) – Access login into a **Linux** Instance
  - 3389 = RDP (Remote Desktop Protocol) – Access into a **Windows** Instance
  - 21 = FTP (File Transport Protocol) – Upload files into a file share
  - 22 = SFTP (Secure File Transport Protocol) – upload files using SSH
  - 80 = HTTP – (HyperText Transfer Protocol) - access un-secured websites
  - 443 = HTTPS – (HyperText Transfer Protocol Secure) access secured websites

AWS Cli 2

- Command Line interface used to manage your AWS services.
- This tool is already on all Amazon Linux instances.
- For Windows instance, you need to download and install it if this become necessary.
- You need this tool when you are mostly working on doing coding to automate the tasks, instead of using AWS Console.

- More info: https://aws.amazon.com/cli/
- Download for Windows: https://awscli.amazonaws.com/AWSCLIV2.msi

AWS Tags

- AWS Tagging is a label that you assign to AWS resources.
- Consists of Key and Value.
- Benefits:
  - Cost allocation: break down AWS costs for multiple departments using tags.
  - Tags for automation such stop/start an EC2 in your code.
  - Tags for access control, mentioned in a policy to allow/deny
- Use AWS Tagging on resources to identify instances

EC2 Instance Roles Demo

IAM Policy to practice:

Policy-1: IAMReadOnlyAccess

Policy-2: AmazonEC2ReadOnlyAccess

Policy-13: AmazonEC2FullAccess

Commands:

1 # aws iam list-users

2 # aws ec2 describe-instances

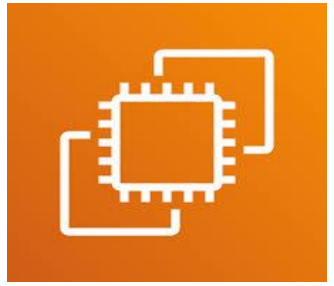
3 # aws ec2 describe-instances –filters "Name=tag:Name,Value=Web Server" This command lists instances that have the tag Name=Web Server

- Create a role called "**my-ec2-role"**
- Attach **policy-1** to the role
- Attach the **role** to the instance.
- From the EC2 command line, type the above **command -1**
- This will output the result.
- Detach the policy from the role.
- From the EC2 command line, run the above **command -1** again.
- Repeat this for other two policies.

EC2 Instances Purchasing Options

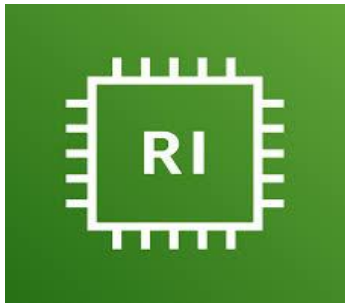
- **EC2 On-Demand Instances**
- EC2 **Reserved Instances**
- EC2 **Spot Instances**
- EC2 **Dedicated Host**

EC2 On-Demand Instances



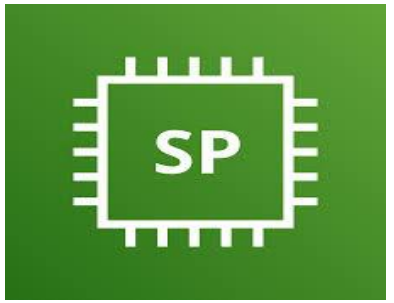
- **On-Demand Instances**:
  - Pay as you go use:
  - Linux: billing per second after the first minute.
  - Windows: billing per hour.
- Highest cost for no upfront payment.
- No long-term commitment
- Recommended for short-term and un-interrupted workloads.

EC2 Reserved Instances



- Up to 75% discount compared to on-demand.
- Big saving with 1 year commitment.
- Even bigger saving with 3 years commitment.
- No upfront, partial upfront or all upfront.
  - Useful for long workloads, such as **databases.**
- **Convertible Reserved Instances**:
  - Allow to change the EC2 instance type
  - Up to 54% discount
- **Scheduled Reserved Instances**:
  - Reserve for specific time of the year
  - Launch instances within the time
- You can sell your reserved instanced to other customers in the AWS **Marketplace** if you don’t need them anymore during the commitment.

EC2 Spot Instances

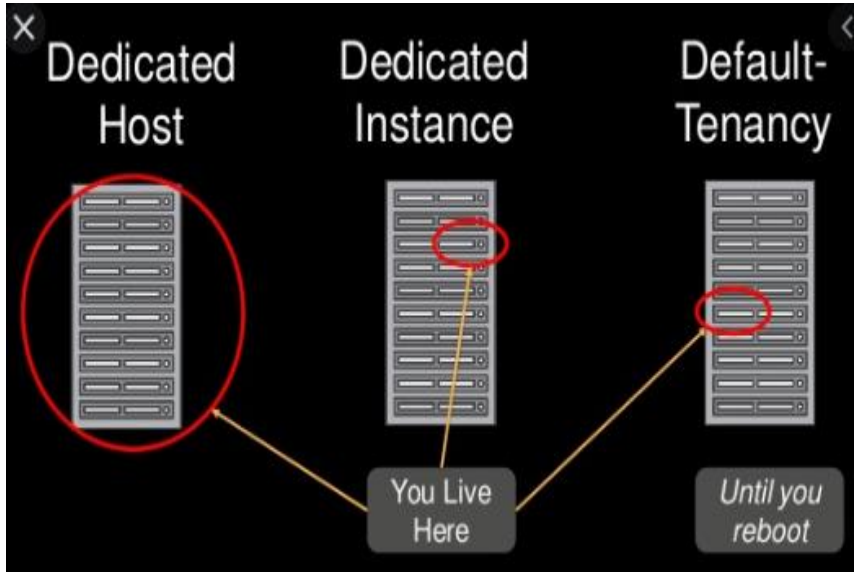


- Provide highest discount, up to 90% but
- You can lose the spot instances if your max price is less then the current spice price.
- Spot prices change from time to time.
- Good for short workload for on day or for few hours.
- Useful for:
  - Batch jobs
  - Data analysis
  - Image processing
  - Any distributed workloads.
  - Not good for databases.

EC2 Dedicated Hosts

- EC2 dedicated host is a physical server with EC2 instance capacity dedicated to your use only.
- More expensive
- Allocated for your account for a 3-year period reservation.
- Allow to bring (BYOL – Bring your Own License) such as for Windows, MS SQL Server.
- Increased network performance.
- Or for company that have strong **compliance** regulations
- You get the visibility into the physical hosts from the AWS Console.

- Gives you control over how instances are placed on the physical server and how deploy your instances to the same physical server over time.

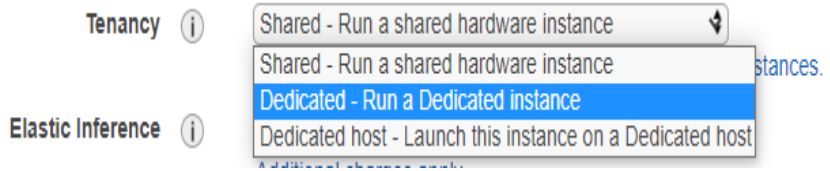


EC2 Dedicated Instance

- Instances are running on hardware dedicated to you.
- Private Network is created on physical server.
- May share hardware with other instances in the same account.
- Some organization require this type instances for isolation of data due to Compliance policy.

Characteristic	Dedicated Instances	Dedicated Hosts
Enables the use of dedicated physical servers	x	x
Per instance billing (subject to a $2 per region fee)	x	
Per host billing		x
Visibility of sockets, cores, host ID		x
Affinity between a host and instance		x
Targeted instance placement		x
Automatic instance placement	x	x
Add capacity using an allocation request		x

- Setup:
  - A custom **VPC** (Virtual Private Cloud) is created on the physical server.
  - Then EC2 instances are launches by selecting:
    - Dedicated – Run a Dedicated instance



Instance Price Example

Price Comparison
Example – m4.large – us-east-1

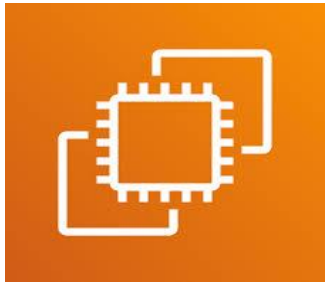
Price Type	Price (per hour)
On-demand	$0.10
Spot Instance (Spot Price)	$0.032 - $0.045 (up to 90% off)
Spot Block (1 to 6 hours)	~ Spot Price
Reserved Instance (12 months) – no upfront	$0.062
Reserved Instance (12 months) – all upfront	$0.058
Reserved Instance (36 months) – no upfront	$0.043
Reserved **Convertible** Instance (12 months) – no upfront	$0.071
Reserved **Scheduled** Instance (recurring schedule on 12 months term)	$0.090 – $0.095 (5%-10% off)
Dedicated Host	On-demand price
Dedicated Host Reservation	Up to 70% off

Shared Responsibility for EC2

- Infrastructure (global network security)
- Isolation on physical hosts
- Replacing faulty hardware
- Compliance validation

- Security Groups rules
- Operating-system patches and updates
- Software and utilities installed on the EC2 instance
- IAM Roles assigned to EC2 & IAM user access management
- Data security on your instance

EC2 Summary – For Exam



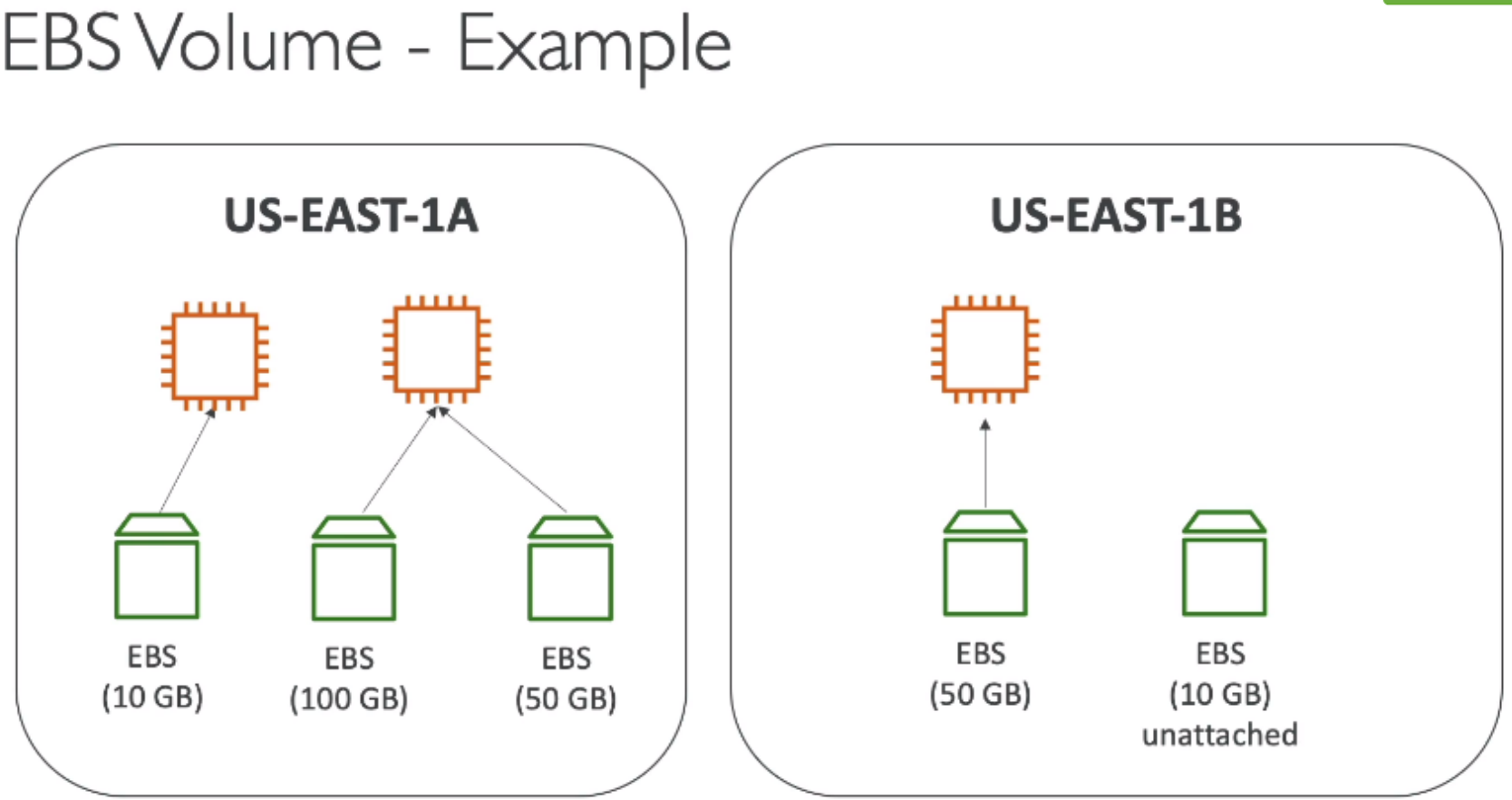
- **EC2 Instance:** OS + Instance Size (CPU+RAM) + Storage + Security group + User Data
- Security Groups: – Firewall attached to the EC2 Instances
- **EC2 User Data**: (for automation during first launch of the instance
- **SSH**: Used to connect to a Linux Instance on port 22
- **RDP**: Used to connect to a Windows Instance on port 3389.
- **EC2 Instance Roles**: Link to IAM Roles to issue commands from the instance.
- **EC2 Purchasing Options**: On-Demand, Reserved, Spot, Dedicated Host and Dedicated Instance.

EC2 Instance Storage – EBS Volume

- **EBS**: (Elastic Block Store)
  - A network drive you can attach to your instance.
  - Data on EBS volume are persistent.
  - They are bound to a specific Availability Zone, cannot be across multiple Azs.
    - To move a volume across, you first need to snapshot it.
  - Root EBS volume is mounted to one instance at a time.
  - You can detach and attach the volume to another instance.
  - Root volume gets terminated along with the instance.

  - Free tier allows you up to 30GB of free EBS storage of gp2 (General Purpose) per month.

EBS Volume Diagram

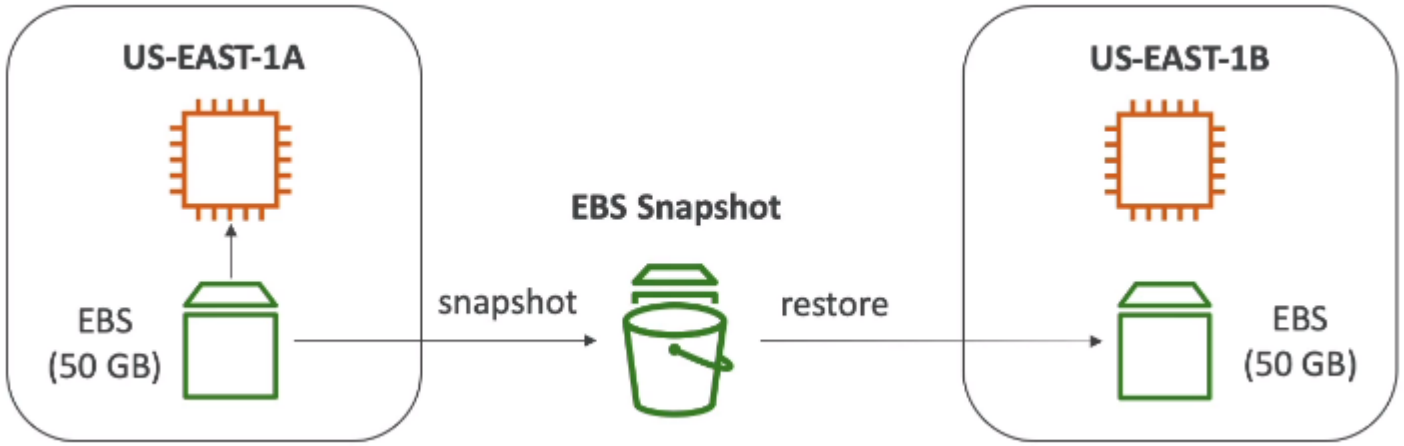


EBS Volume Lab

- Create a second EBS volume in the same AZ as the instance.
- /dev/sdf
- Create a volume in the second AZ.

EBS Snapshot

- A backup of the whole EBS volume attached to a running instance
- No need to detach the volume
- You can copy snapshots across AZ and Region.



EBS Snapshot - Demo

1. Create a snapshot from an EBS volume
2. Possible to copy a snapshot to another AZ
3. Create a volume from the Snapshot
4. Attach the volume to EC2 instance

Amazon AMI

- AMI = Amazon Machine Image
- A customization of an EC2 instance
  - Install your own software, anti-virus agent, web services
- AMIs are build in a specific regions and can be copied across regions.
- You can launch EC2 Instances from:
  - A **Public AMI**: AWS Provided.
  - Your own AMI: You customize and maintain.
  - AWS **Marketplace AMI**: AMI created by other company, developers and sell them in AWS Marketplace. Such AMI with Webserver for running Web Site.

AMI Process - Demo

- Start an EC2 instance and customize it with User Data Script.
- Stop the instance
- Build an AMI from the instance
- Launch an instance from the created AMI without User Data.
- Launching instances from other AMI

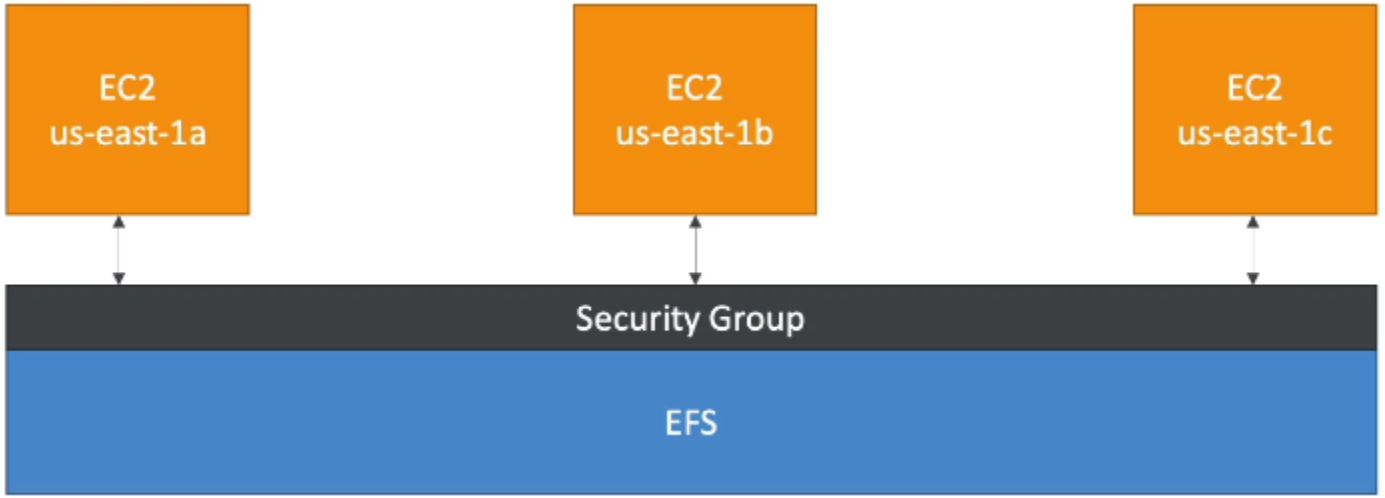
EC2 Instance Store

- EBS volumes are network good but limited performance
- Instance store are with high disk read/write performance

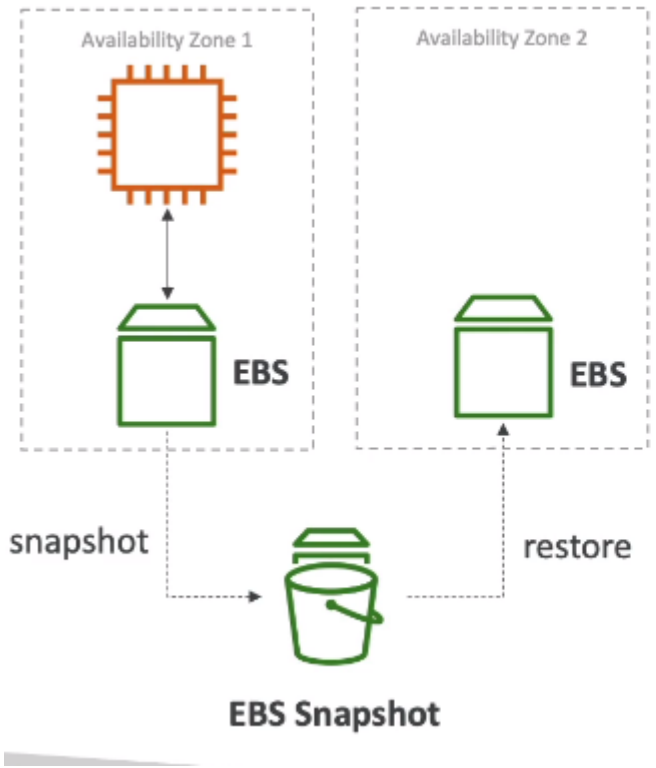
- Good for buffer, temporary data, cache
- Data on “instance store” storage gets wiped out if the instance is stopped.
- You cannot do a snapshot on instance store.
- You backup or copy the data to EBS volume.

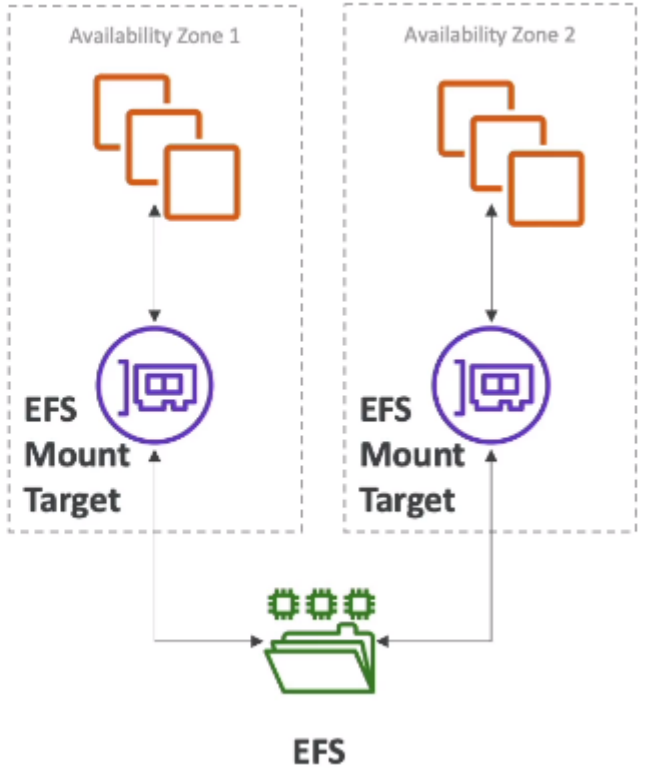
EFS - Network File System

- Shared Network Storage
- EFS can be attached to a group of EC2 instances
- EFS works on Linux EC2 instances
- Highly available across multi-AZ



EBS vs EFS


Availability Zone 1
Availability Zone 2
EBS
EBS
snapshot
restore
EBS Snapshot


Availability Zone 1
Availability Zone 2
EFS
Mount
Target
EFS
Mount
Target
EFS

Shared Responsibility for EC2 Storage

- Infrastructure
- Replication for data for EBS volumes & EFS drives
- Replacing faulty hardware
- Ensuring their employees cannot access your data

- Setting up backup / snapshot procedures
- Setting up data encryption
- Responsibility of any data on the drives
- Understanding the risk of using EC2 Instance Store

EC2 Storage Summary:

- EBS Volumes:
  - Network Drives attached to ONE EC2 instance at a time.
  - Mapped to an Availability Zone.
  - Create snapshots for backup purpose
- AMI: a customed image created by you.
- EC2 Instance Store:
  - High Performance hardware disk attached to EC2 Instance
  - Storage is lost if instance is stopped or terminated.
- EFS: Network file system (NFS)
  - Can be attached to multiple instances in region.
  - Use for file share among multiple organization departments.

Question-1

- **Which EC2 Storage would you use to create a shared network file system for your EC2 Instances?**

1. **EBS Volume**
2. **EC2 Instance Store**
3. **EBS Snapshots**
4. **EFS (Elastic File System)**

Question-2

- What are AMIs Not used for?

1. Add your own software license
2. Customize the configurations
3. Add your own Operating System
4. Add your own IP Address

Question-3

- **EBS Volumes CANNOT be attached to multiple EC2 instances at a time.**

1. **True**
2. **False**

Question-4

- **An EBS Volume is a network drive you can attach to your instances while they run, so your instances' data persist even after their termination.**

1. **True**
2. **False**

Question-5

- **Which statement is CORRECT regarding EC2 Instance Store?**

1. **Not good for cache contents**
2. **Better performance but data is lost if the EC2 Instance is stopped**
3. **Data is always safe with EC2 Instance Store**

Question-6

- **What is an EBS Snapshot?**

1. **The Operating System on an EC2 Instance**
2. **Backup of your EBS Volume**
3. **CPU and RAM of an EC2 instance**

Question-7

- Where can you find a third party's AMI to launch?

1. Public AMIs
2. My own AMIs
3. AWS Marketplace AMIs

Question-8

- **What is an EBS Volume tied to?**

1. **A region**
2. **A data center**
3. **An Edge location**
4. **An Availability Zone**

Amazon S3 Storage

- Amazon S3 = Simple Storage Service (with 3s, called S3)
- Provide Storage via Internet
- **Object** level as EBS is **block** level storage
- A Global Service
- Highly Available 99.99999 %
- Unlimited Storage Capacity

Use Cases

- Backup and storage
- EBS volume snapshot stored in S3 (not visible)
- Disaster Recover to copy data across Regions
- Archive Data
- Media hosting, videos
- Data Lake & Big Data Analytics
- Software storage
- Static Website

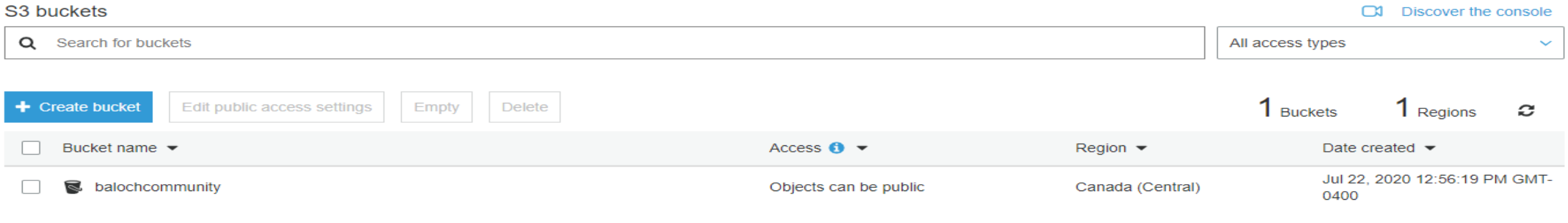
Amazon S3 - Buckets

- When you create a S3 storage, it is called a “bucket”
- You store objects (files/folders) in buckets.
- Bucket must have a unique name globally (across all Regions)
- It is a global service, but buckets are created in a specific Region.
- **Naming convention for Bucket:**
  - No uppercase
  - No underscore
  - 3-63 characters long
  - Not an IP address
  - Must start with lowercase letter or number

Amazon S3 - Objects

- Objects can be accessed as:
  S3://my-bucket/my_file.txt
  S3://my-bucket/my_folder/my_file.txt
  My_folder = is called Key

- Object max size is 5TB (5000GB)
- If uploading more than 5GB, must use “Multi-part upload”
- You can set versioning on bucket to make a copy of the object.



Amazon S3 - Demo

- Create a bucket
- Upload an object
- View the object
- Delete an object
- Enable versioning
- Generate a policy for “Bucket Policy” to make the bucket public

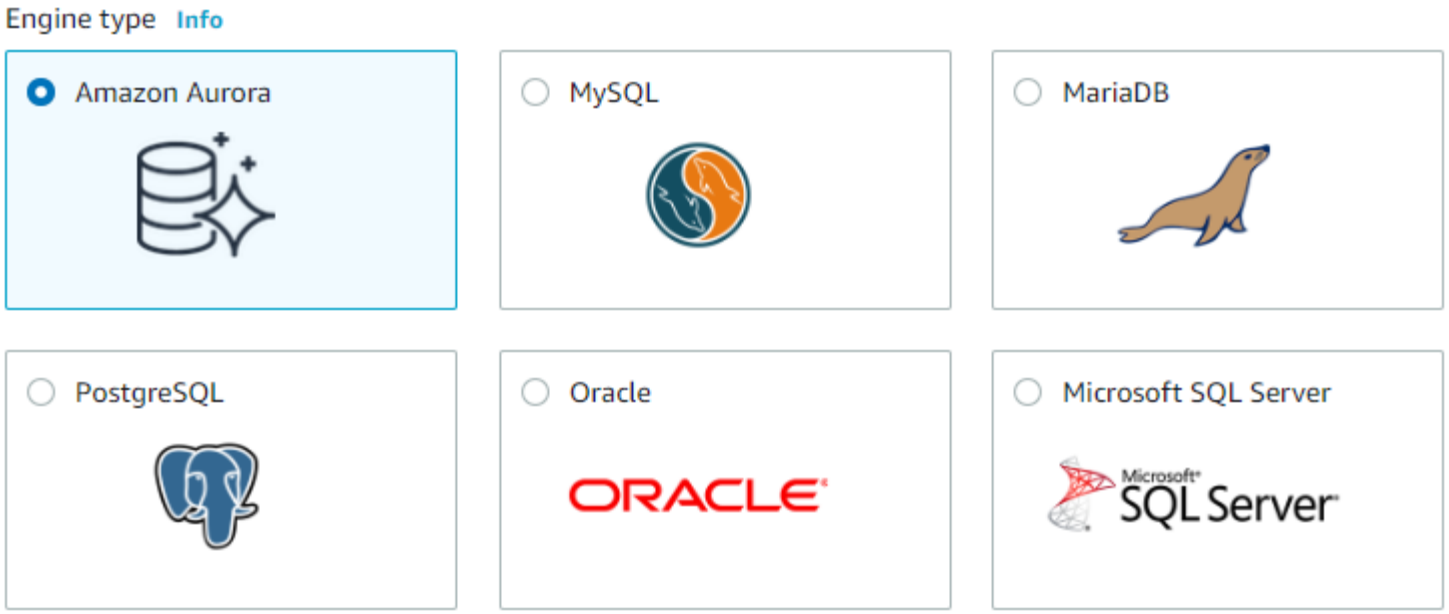
Bucket Policy

This bucket policy allow to access the object publicly, allow you to download objects from S3 bucket (s3:GetObject).

```
{
  "Id": "Policy1596393490758",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Stmt1596393487706",
      "Action": [
        "s3:GetObject“
      ],
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::balochcommunity/*",          ( replace the bucket name to the one you created ).
      "Principal": "*"
    }
  ]
}
```

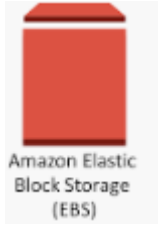
Amazon RDS

- RDS = Relation Database Service
- RDS is a managed service
- Supported Engines:



Cost Optimization

- **EBS Volume:**
  - EBS cost if not in use
  - Delete un-used EBS volumes,
  - Snapshot storage is cheaper, take snapshot if your need to keep the data
  - Provision-IOPS volumes cost more
  - Downsize volume that has more than 80% free space



- **Elastic IP (EIP):**
  - EIP cost money when not in use
  - Having more then one EIP assigned to an instance cost more money
  - EIP on stopped instances cost money

Cost Optimization (cont’d)

Amazon RDS DB Instance:

- Snapshot unused DB instanced and delete them if they 0 connections over time
- Use CloudWatch to check the RDS connection
  - CloudWatch is an AWS Resource monitoring Service.

Amazon Trusted Advisor:

- Trusted Advisor provides recommendations on Cost Optimization

Links

- Dedicated Instances and Dedicated Hosts
- https://www.privoit.com/resources/dedicated-instances