

2 EC2 and EBS

Wednesday, 11 September 2019 8:26 PM

IAM

Identity and access management

Users, Groups, roles, policies (AWS Managed/Custom), Service

Roles

One AWS Resource needs to communicate with another AWS

Ec2 (App) -> S3/DDB

Role. ->. Ec2 sts.assumeRole("S3FullAccessRole")

STS (Security Token Service)

Generating the temporary security credentials for a role

Elastic Compute Cloud (EC2)

AWS resizable compute service

App (Server [EC2])

Server -> Ec2 instance (VM)

Count

CPU, Storage, Memory, Port (HTTP), Software

 - - - -

e/Job Role

resource

Certificates, Location

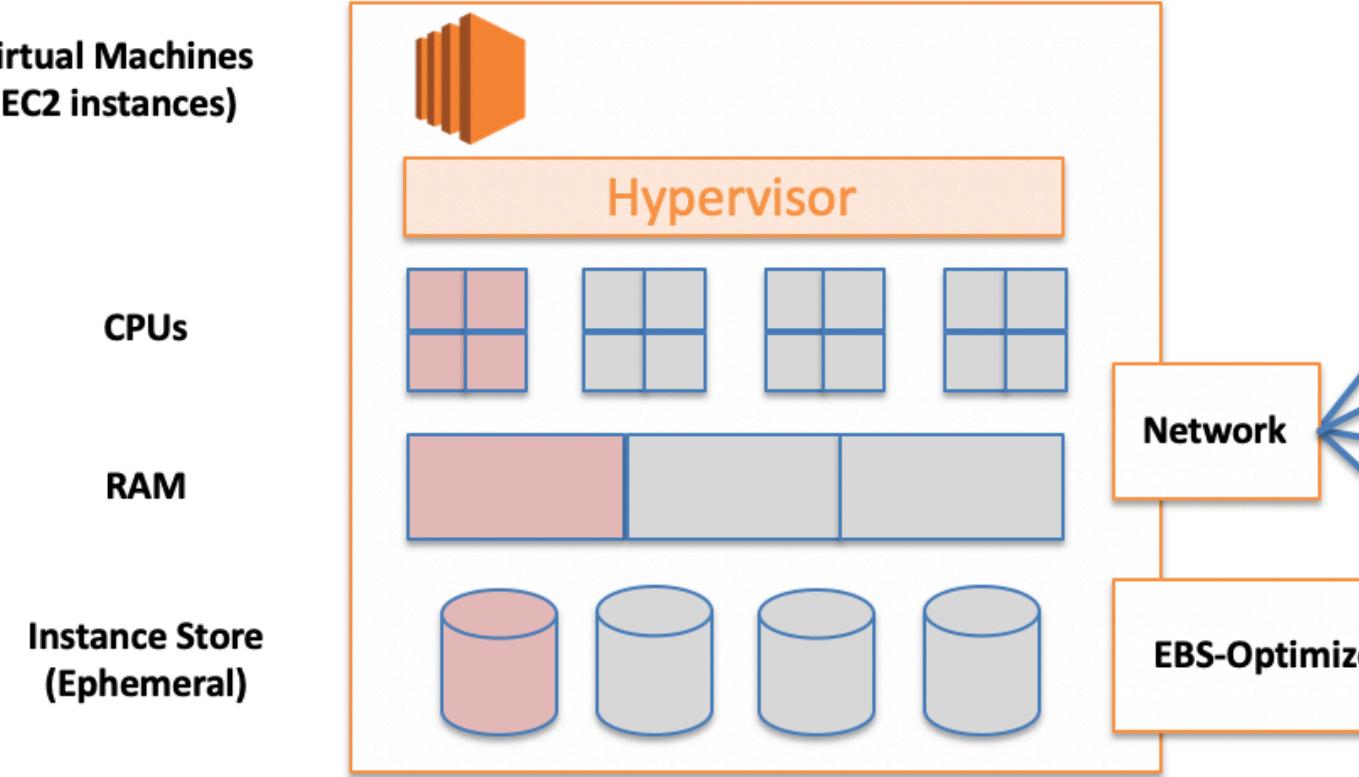
Subnets (Internet / Internal)

Operating System

Load Balancer (HA)

2 server

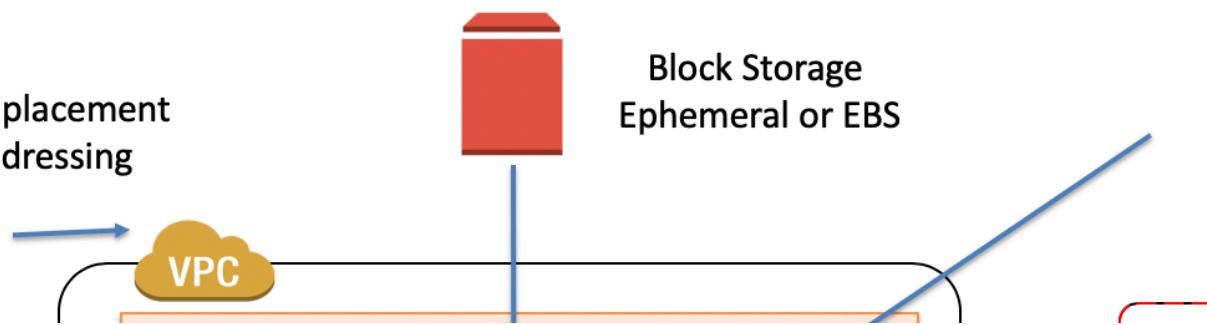
Virtual Machines (EC2 instances)

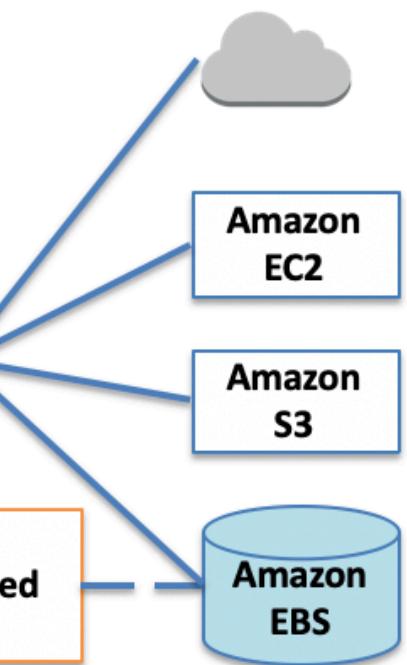


Lunching EC2 Instance

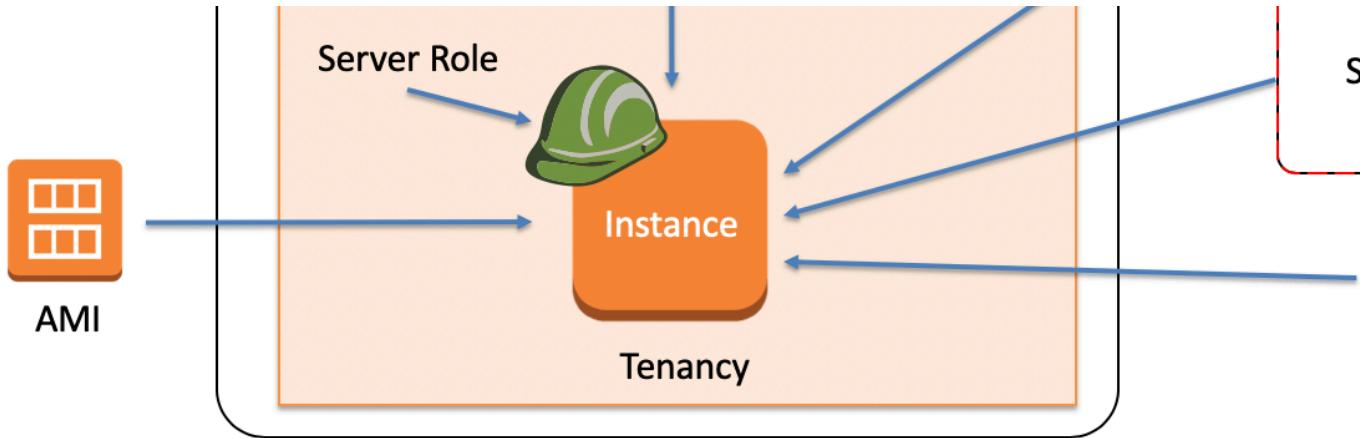
Network placement
and addressing

Block Storage
Ephemeral or EBS





User data



AMI (Amazon machine image) -> OS and Application pre-installed
Region/AZ (Subnet/Network(VPC))
Storage (How much / What kind of storage)
User-data (Bootstrap script)
(Script that you want to run on first system boot)

Security (control kind of traffic is allowed to flow in or out of e)
Keypair (public and private keys)

Create an EC2 and run a web application inside

MyAppAMI (Centos (Apache Server (Apps(Config))))

Server1

Server2

Microsoft Exchange Server (setting it up takes days)

Linux, Apache, Mysql, PHP

security groups



Key pairs

led

c2 instance)

Choose an Instance Type

T4 (GP)
C5 (Compute optimized)
M (GP)
R (Memory)
I/D (Disk optimized)
G (GPU)

C1. C3 C5

Instance Storage (Local storage(that is local to my VM(EC2)))
Stop the server (lose my data)

EBS Data (Kept Intact)

Demo: Creating an EC2 Instance

AMI

Instance Types

Storage Types

User Data

Region/VPC/AZ

Tenancy

Security Group

Tags

KeyPairs

Service limits

https://docs.aws.amazon.com/general/latest/gr/aws_service_limits.html

Instance Metadata URL

Role

From:	Until:
10.0.0.0	10.255.255.255
172.16.0.0	172.31.255.255
192.168.0.0	192.168.255.255

AMI

Amazon Quickstart AMI

Marketplace

Community

Private

Instance Types

T2/3, M4/5

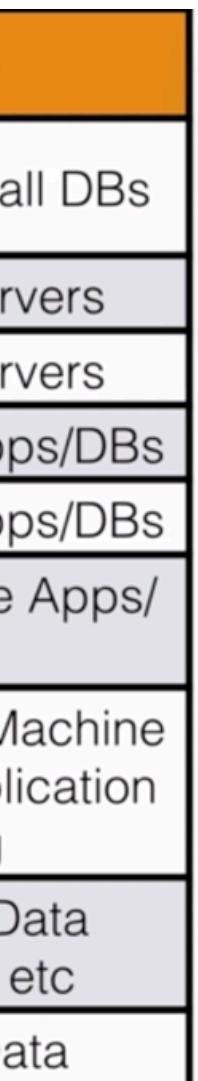
C4/5

R4/5, X1

P,G,F

I, D

Family	Speciality	Use case
T2	Lowest Cost, General Purpose	Web Servers/Small DBs
M4	General Purpose	Application Servers
M3	General Purpose	Application Servers
C4	Compute Optimized	CPU Intensive Applications
C3	Compute Optimized	CPU Intensive Applications
R3	Memory Optimized	Memory Intensive DBs
G2	Graphics/General Purpose GPU	Video Encoding/Machine Learning/3D App Streaming
I2	High Speed Storage	NoSQL DBs, Data Warehousing
D2	Dense Storage	Fileservers/Databases



Storage Types

Instance Store

Private IP (Local network)
Public IP (Identity over internet)

Google.com -> public IP

Security control traffic IN or OUT

Port/Protocol | Where?

Default SG conf for and EC2?
No incoming traffic allowed
Everything outgoing is allowed

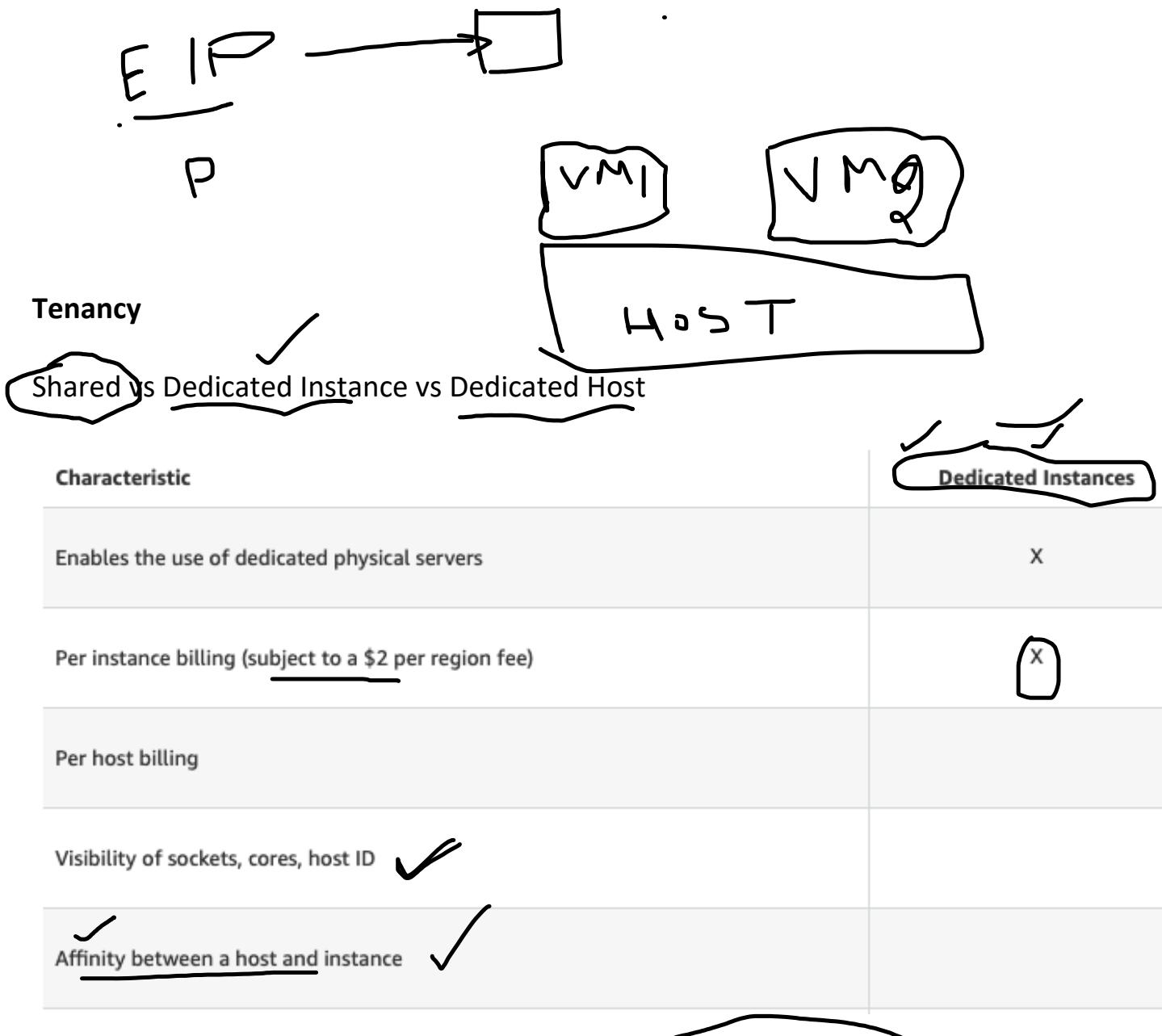
Characteristic	Reboot	Stop/Start (EBS-backed instances only)	Termination
Host computer	The instance stays on the same host computer.	The instance runs on a new host computer.	N/A

adoop

minate

A

Private and public IP addresses	Stay the same.	Instance keeps its private IP address and gets a new public IP address.	N/A
Elastic IP addresses (EIP)	EIP remains associated with the instance.	EIP remains associated with the instance.	The instance
Instance store volumes	The data is preserved.	The data is erased.	The instance
EBS volume	The volume is preserved.	The volume is preserved.	The volume
Billing	Instance billing hour doesn't change.	You stop incurring charges as soon as state is changed to stopping.	You stop



A

The EIP is disassociated from the instance.

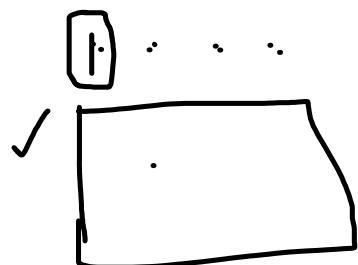
The data is erased.

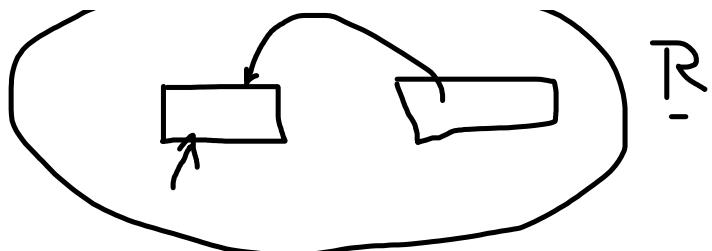
The volume is deleted by default.

You stop incurring charges as soon as state is changed to Shutting-down.

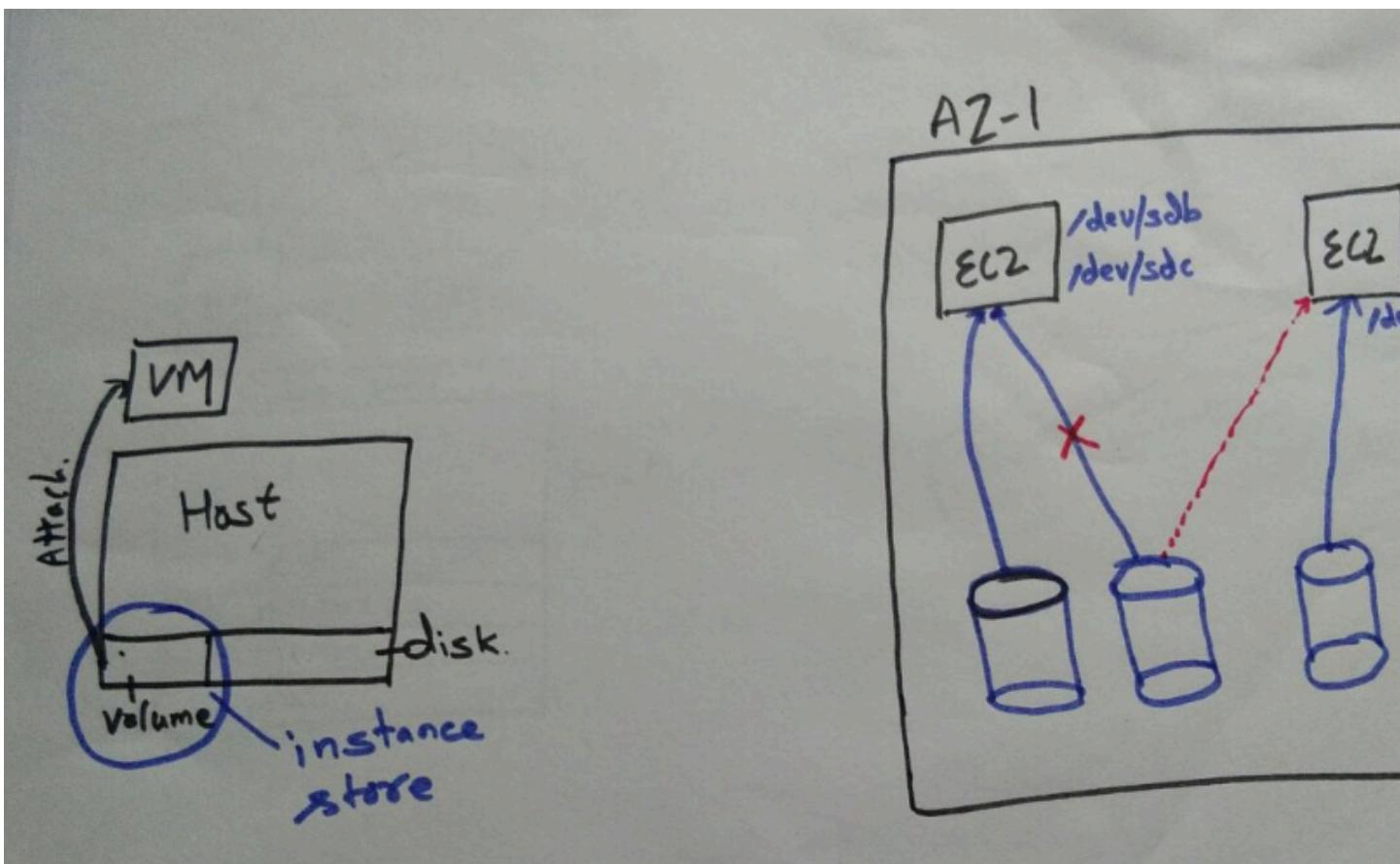


Dedicated Hosts





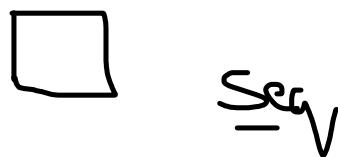
EBS



EBS instructions used in the demo

lsblk

```
sudo file -s /dev/xvdf
sudo mkfs -t xfs /dev/xvdf
sudo mkdir /data1
sudo mount /dev/xvdf /data1
```



Magnatic

PIOPS SSD

EBS GP SSD

Throughput Optimized HDD



Cold HDD

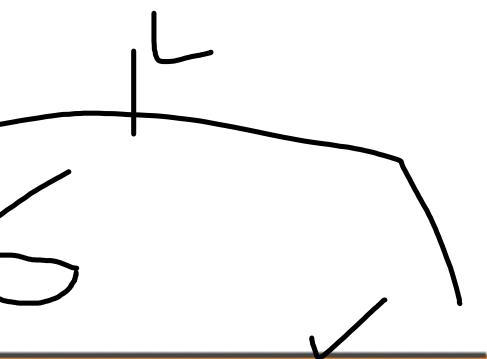
Latency -> time it take to perform the ops (1 read / 1 ms)

Throughput. -> (10 read/ 1 KB/ 10KB ps)

	Magnetic	Cold HDD	Throughput Optimized HDD	General
Max volume size	1 TiB	16 TiB	16 TiB	16 TiB
Max IOPS/volume	40 to 200	250	500	1000
Max throughput/volume	40 to 90 MiB/sec	250 MiB/s	500 MiB/s	160 MiB/s
Use cases	<ul style="list-style-type: none"> Infrequent data access 	<ul style="list-style-type: none"> Workloads involving large, sequential I/O 	<ul style="list-style-type: none"> Workloads involving large, sequential I/O 	<ul style="list-style-type: none"> Boot Smart Media Deployment

PIOPS – IOPS and Throughput limits

Provisioned IOPS	Max Throughput (MBps)	Max Random 16 KiB I/Os per second	Max Random 256 KiB I/Os per second
1250	320	1250	1250
10000	320	10000	1250
20000	320	20000	1250



General Purpose SSD	Provisioned IOPS SSD
6 TiB	16 TiB
10,000	20,000
MiB/sec	320 MiB/sec
Small volumes Small to medium DBs Dev and Test environments	<ul style="list-style-type: none"> • I/O-intensive workloads • Relational DBs • NoSQL DBs

(point in time) Snapshot. -> Volume(AZ1). -> Ec2 (AZ1)

Ec2 (AZ2)

1. -> Create a EBS volume in N.V. (us-east-1a (AZ)).
2. -> Attach the EBS Vol to EC2 instance
3. -> Take a backup
4. -> Copy the snapshot to a different region
5. -> Create another volume in (us-east-1b) containing the same data of earlier EBS.
6. -> Attach that to an instance running in us-east-1b
7. -> detach the volumes
8. -> delete the volumes
9. -> delete the snapshots
10. -> Block yourself an EIP address and associate that to the EC2 instance running in AZ
11. -> Stop and start your Ec2 instance and observe if the Public IP change?
12. Reboot your ec2 instance and observe if the public/private IP change?

Answer the question:

- You need to run an application/workload that runs under stress and requires a consistent storage choice is best suited to this application?
 - PIOPS
- You need to run an application that requires 2K IOPS consistently and this application of storage can be used here?
 - GP2
- You want to run HDFS cluster(distributed/replicated cluster of many nodes), what kind of storage you suggest ?
 - Throughput intensive
 - HDD type of disk
- I and D type of instances, instance storage



(us-east-1a)

istent IOPS of 15000, what kind of

n is latency and cost sensitive, what kind

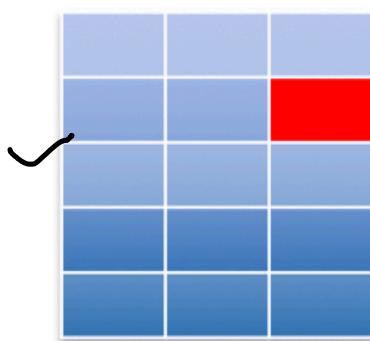
nd of ec2 instance and storage would



What if you want to change one character in a 1-G

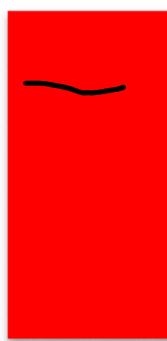
Block Storage

Change one block (piece of the file) that contains the character



Object Storage

Entire file must be changed



A Z

EBS Snapshots / AMI

Amazon EBS Lifecycle

Vast amounts of unused space

Create

Call CreateVolume
1 GB to 16 TB

Attach

Call AttachVolume
one Amazon EC2

GB file?

ge

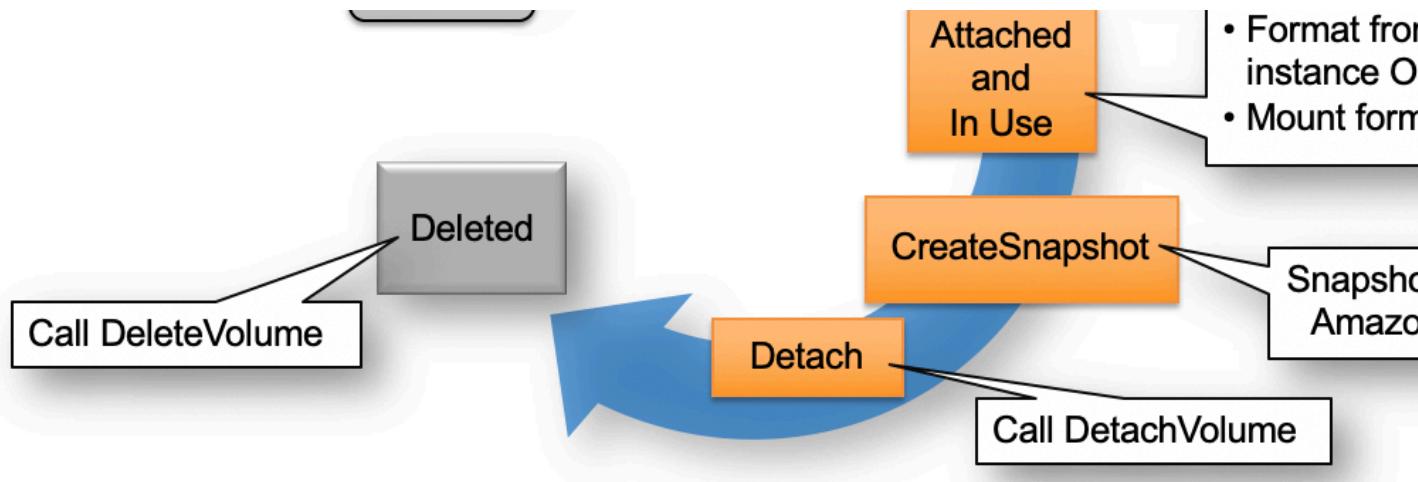
ust be updated



R



e to affiliate with
instance



User Data

https://github.com/imcloudstudent/misc/blob/master/ec2_webapp_exercise.sh
<https://gist.github.com/mahtabgodara/06143c1040c16f20fec680197a723b70>
<https://github.com/imcloudstudent/misc/blob/master/userdata-samples.txt>
<https://github.com/imcloudstudent/misc/blob/master/various-userdata.txt>

Ex 1.1: <https://aws.amazon.com/getting-started/tutorials/launch-a-virtual-machine/?trk=docs-new-tutorials-launch-vm>

Ex 1.2: <https://aws.amazon.com/getting-started/tutorials/launch-windows-vm/?trk=gs-launch-vm>

Amazon EC2
S
natted drive

ot to
on S3

[k=gs_card](#) (linux)

[card](#) (windows)

Ex 1.3: <https://aws.amazon.com/getting-started/tutorials/launch-a-wordpress-website/>

Ex 1.4: Launch an EC2 linux instance and log in using SSH

1. From the EC2 Dashboard, click to launch a new instance and select an instance type. Remember, the t2.micro is Free Tier-eligible and is available for free as long as it's still within its first year.
2. Explore the Configure Instance Details, Add Storage, and Advanced Details sections. Most of the default settings should work fine.
3. On the Configure Security Group page, make sure there's at least one security group assigned to the instance. Make sure there's an inbound rule allowing SSH (port 22) traffic. It should be there by default.
4. Before letting you launch the instance, AWS will require you to select a key pair. Follow the instructions.
5. Once the instance is launched, you can return to the Instances Dashboard to monitor its status until everything is running properly.
6. Click the Actions pull-down and then the Connect item for your instance. This will provide you with the IP address and port number to connect to the instance from your local machine. Then connect using Putty or SSH to your virtual cloud server.

Connect Using Putty

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/putty.html>

Connect Using SSH

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/AccessingInstancesLinux.html>

Ex 1.5: Assess the free Capacity of a running instance and Change the Configuration

1. With an instance running, open the Instances Dashboard. Select the instance you're interested in and click the Monitoring tab in the bottom header bar. This is a good place to see what percentage of compute and network resources your instance has been using over the past hours or weeks.

?trk=gs_card

and select a Linux AMI and
e if your AWS account is

Add Tags pages—although

a rule permitting incoming

you to select—or create—a

nces Dashboard to wait

instructions on how to
nnect and take a look at

Change its instance Type

Select the instance you're
half of the screen. That's a
ork resources you've been

Now pretend that your instance is nearly maxed out and consider the following.

2. Stop the instance. (Remember, your public IP address might not start up again.)
3. From the Actions drop-down, click Instance Settings and then Select a new type.
4. Restart the instance and confirm that it's running properly.

Stop and Ec2 instance (stopped)

EBS volume (incur)

10 instance (RI) , sale days (on-demand/spot)

Not use RI (if I am not sure about consistent/steady pattern)

Instance Pricing Types

Amazon EC2 Pricing Options

	On-Demand Instances	Reserved Instances (RIs)	Spot Instances
Term	Pay as you go	One year or three years	Bid on usage; instances are out of term
Benefit	Low cost and flexibility	Predictability ensures compute capacity is available when needed	Large savings for workloads
Cost	Pay for what you use	Pay low or no upfront fee; overall cost is lower	Spot price is lower than demand
Use case	<ul style="list-style-type: none">• Short-term, spiky, or unpredictable workloads• Application development or testing	<ul style="list-style-type: none">• Steady state or predictable usage workloads• Applications that require reserved capacity, including	<ul style="list-style-type: none">• Applications that start at specific times• Applications with very low usage

change the instance type as

ht be different when you

hen Change Instance Type.

.

Spot Instances

unused capacity;
es can be lost if you
oid

scale, dynamic
d

ce based on supply
nand

ations with flexible
nd end times
ations only feasible at
w compute prices

of testing

reserved capacity, including

disaster recovery

- Users able to make upfront payments to reduce total computing costs even further

very i

- Users needs additional

On-Demand Instances

Pay by the hour.

Reserved Instances

Purchase at significant discount.
Instances are always available.

1-year to 3-year terms.

Scheduled Instances

Purchase a 1-year RI for a recurring period of time.

Spot Instances

Highest bidder uses instance at significant discount.
Spot blocks supported.

with urgent computing
for large amounts of
capacity

Dedicated Hosts

Physical host is fully dedicated to run your instances. Bring your per-socket, per-core, or per-VM software licenses to reduce cost.

Instance Type	Pricing Model	Cost/Hour
t2.micro	On-demand	\$0.0058
t2.micro	Reserve (three-year term)	
g3.4xlarge	On-demand	\$1.14
g3.4xlarge	Reserve (three-year term)	

Global Service vs Region/AZ level services

IAM (Global)
EBS (AZ)
EC2 (AZ) (HA/DR of Ec2)

EIP -> Ec2 X
EIP -> Ec2
Monitoring (Cloudwatch)

Cost/Year

\$50.81

\$38.33

\$9986.40

\$4432.56

Ex 1.6: Create and launch an Ami Based on an Existing instance

1. If necessary, launch an instance and make at least some temporary changes to its volume. This could be something as simple as typing **touch /tmp/testfile** on the instance to create an empty file.
2. Create an image from the instance's volume (you'll access this via the Actions pull-down menu in the Instances Dashboard).
3. Launch an instance from the console and select the new AMI.
4. Log into the instance and confirm that your previous changes have been applied.

Ex 1.7: Create Ec2 instance with CLI command

AWS CLI Example (EC2 Instance)

<https://gist.github.com/mahtabgodara/ff87acf9b9b369ff5cedc432d26d94b1>

Ex 1.8: Clean up unused EC2 resources

Since you've probably been launching resources while experimenting, it's a good idea to clean up after yourself. You want to make sure you haven't accidentally left anything running that you don't need, which can waste money. So, take a good look through the console and kill off what you don't need.

Here are some things to consider:

1. Remember to check any other AWS regions where you might have launched resources.

ce
oken change to the root
n **test.txt** on a Linux

the dialog through the

AMI from the My AMIs tab.
ge has persisted.

menting with AWS, you'll
ing that could cost you
hat shouldn't still be alive.

ght have done some work—

- only a single region's resources will show up in the console
- 2. Some resources can't be deleted because they're in use by something else. A snapshot used by a private AMI is one example. You'll need to delete them in the right order.
- 3. When you're logged into your AWS account, you can check the AWS CloudWatch Metrics Management Dashboard in the console (<https://console.aws.amazon.com/cloudwatchmetrics/>). This Dashboard will show you whether, taking into account your usage, you stand to run up a bill in the current month.

Server (Ec2)

Storage (Instance store, EBS)

Instance store (DAS)

EBS (SAN) vol can only be attached to a single EC2 instance at a time

Fast

Low latency

Block

Ec2 Ec2

Disk (NFS/ NAS) / EFS (Elastic File System)

EFS	EBS
	Shared volumes. EBS vol to one Ec2 at a time

e.

y other resources. A snap-
shut those down in the

k out your Billing And Cost
[ws.amazon.com/billing](https://aws.amazon.com/billing)).

t your current resource

a given time.

Mounted on linux sys	Mounted on linux sys
Expensive	Relatively cheaper
Region	AZ
Scale, Taken care by AWS	DIY
HA , Taken care by AWS	HA to some extent
Linux	All OS, you decide the file system
Managed Service	No so much
NFSv4.x	
SAMBA	
File Store	Block store

Windows
CIFS

So far,
Basics
AWS global Infra
IAM
Ec2
EBS
EFS
Pricing options
FAQS

Next
S3

Glacier
Snowball
DynamoDB

EFS (Elastic File System)

https://aws.amazon.com/getting-started/tutorials/create-network-file-system/?trk=gs_camp

SUMMARY

Understand how to choose the right hardware/software profile.
Understand EC2 pricing models and how to choose one to fit your deployment profile.

Know how to access a running instance.

Understand the features and behavior of storage volume types.

Know how to create a snapshot from a storage volume and how to move it to a different instance.

rd

**file for your workload
your needs.
ess with security to match**

**es.
ow to attach the snapshot**