

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 resource

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

— — — — —

Job Role

Resource

Certificates, Location

Subnets (Internet / Internal)

Operating System

Load Balancer (HA)

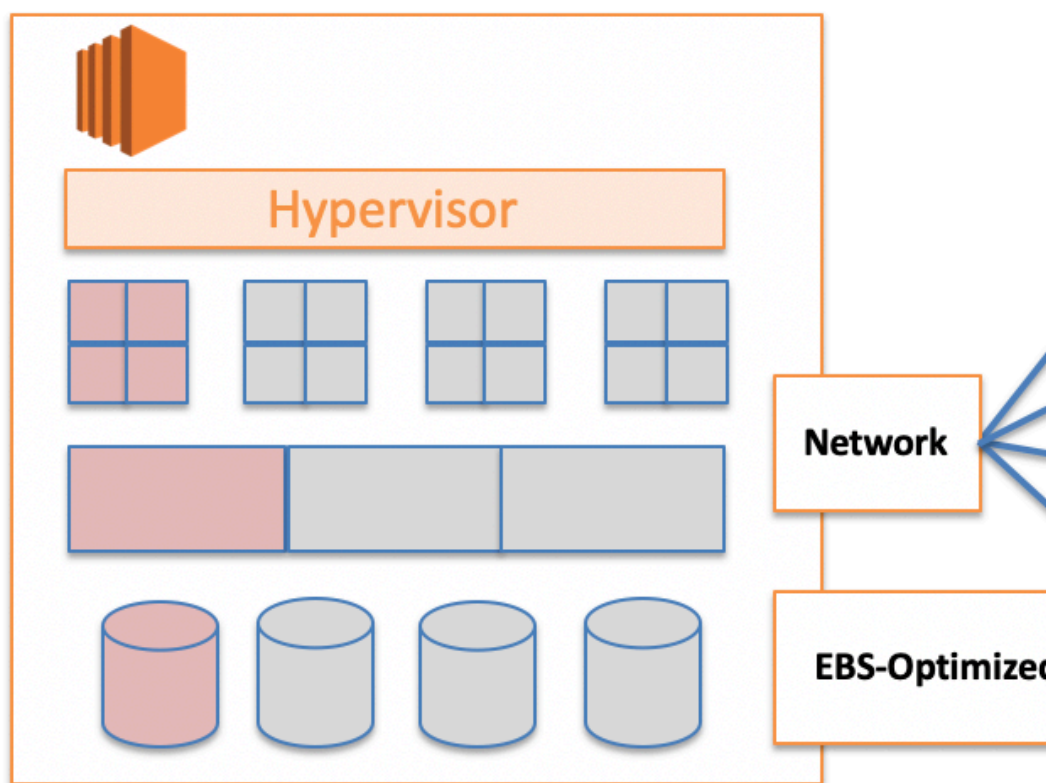
2 server

**Virtual Machines
(EC2 instances)**

CPUs

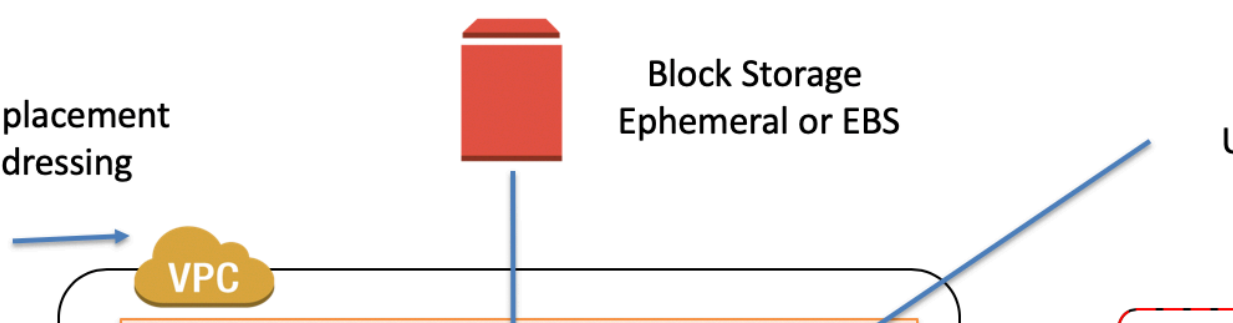
RAM

**Instance Store
(Ephemeral)**

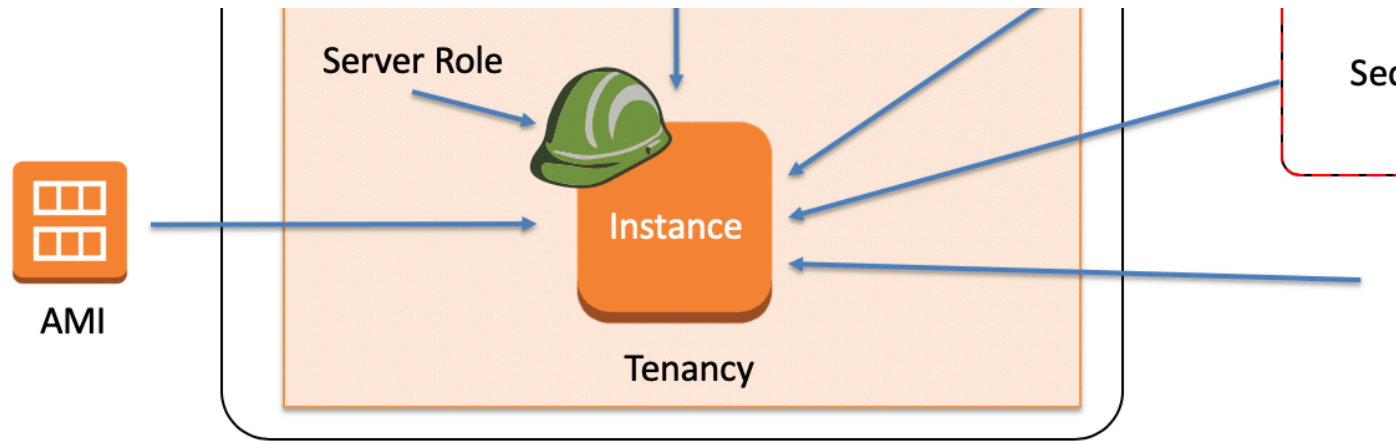


Lunching EC2 Instance

**Network placement
and addressing**







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 ec2)

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

curity groups



Key pairs

ed

2 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 (loose 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
M4	General Purpose	Application Serv
M3	General Purpose	Application Serv
C4	Compute Optimized	CPU Intensive App
C3	Compute Optimized	CPU Intensive App
R3	Memory Optimized	Memory Intensive DBs
G2	Graphics/General Purpose GPU	Video Encoding/M Learning/3D Appli Streaming
I2	High Speed Storage	NoSQL DBs, D Warehousing e
D2	Dense Storage	Fileservers/Da

all DBs
vers
vers
os/DBs
os/DBs
Apps/
achine cation
ata etc
ta

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?
---------------	--------

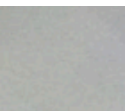
Default SG conf for and EC2?

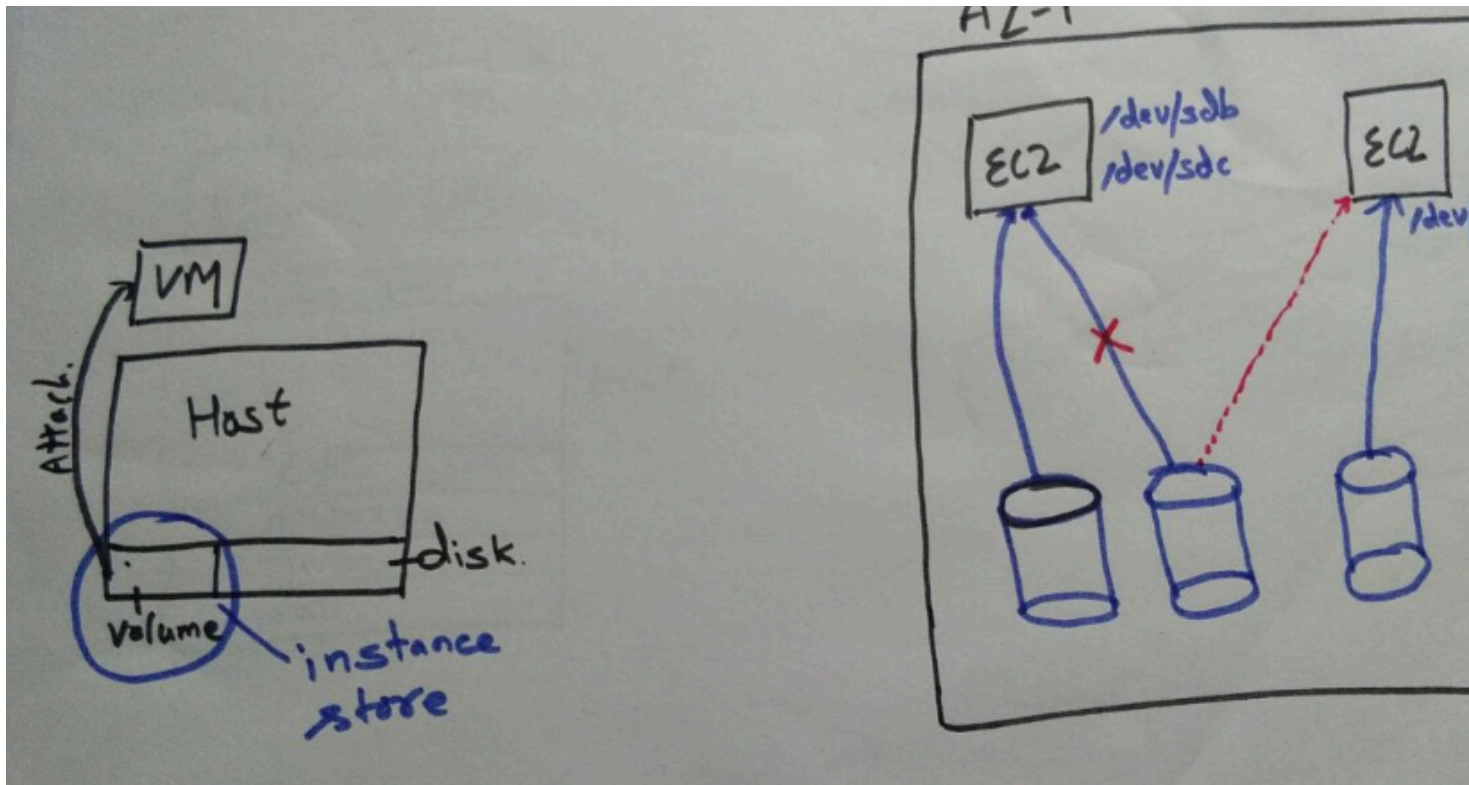
No incoming traffic allowed

Everything outgoing is allowed

EBS

doop





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

Magnetic

PIOPS SSD

EBS GP SSD

Throughput Optimized HDD

Cold HDD

Magnetic

Cold HDD

**Throughput
Optimized HDD**

**General
SSD**



Purpose SD	Provisioned IOPS SSD
---------------	-------------------------

Max volume size	1 <u>TiB</u>	16 <u>TiB</u>	16 <u>TiB</u>	16 <u>TiB</u>
Max IOPS/volume	40 to 200	250	500	10,000
Max throughput/volume	40 to 90 <u>MiB/sec</u>	250 <u>MiB/s</u>	500 <u>MiB/s</u>	160 <u>MiB/s</u>
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 • Small • Medium • Dev & test

PIOPS – IOPS and Throughput limits

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

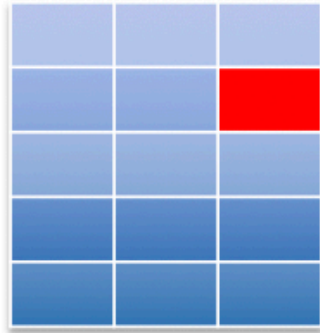
TiB	16 TiB
000	20,000
MiB/sec	320 MiB/sec
volumes all to um DBs and Test onments	<ul style="list-style-type: none">I/O-intensive workloadsRelational DBsNoSQL DBs



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



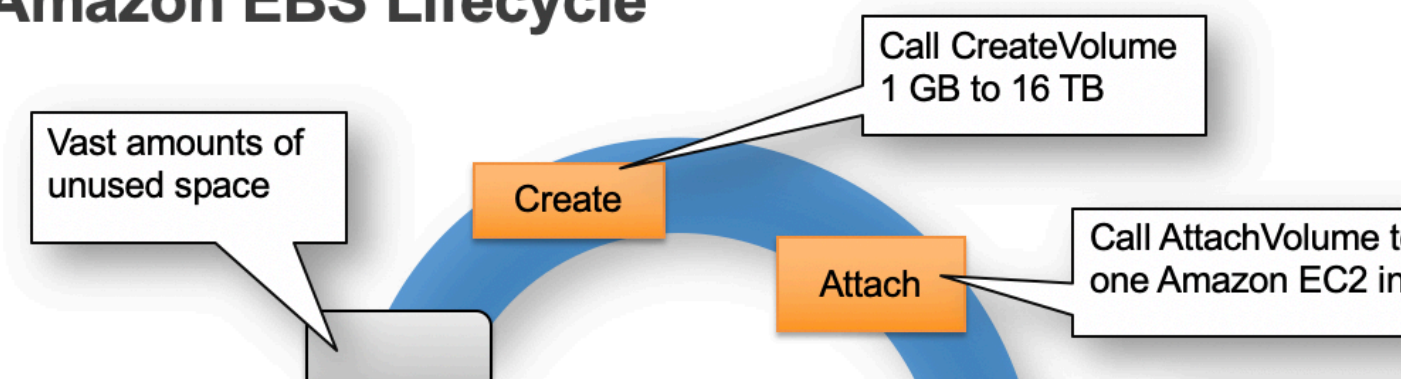
Object Storage

Entire file mu



EBS Snapshots / AMI

Amazon EBS Lifecycle



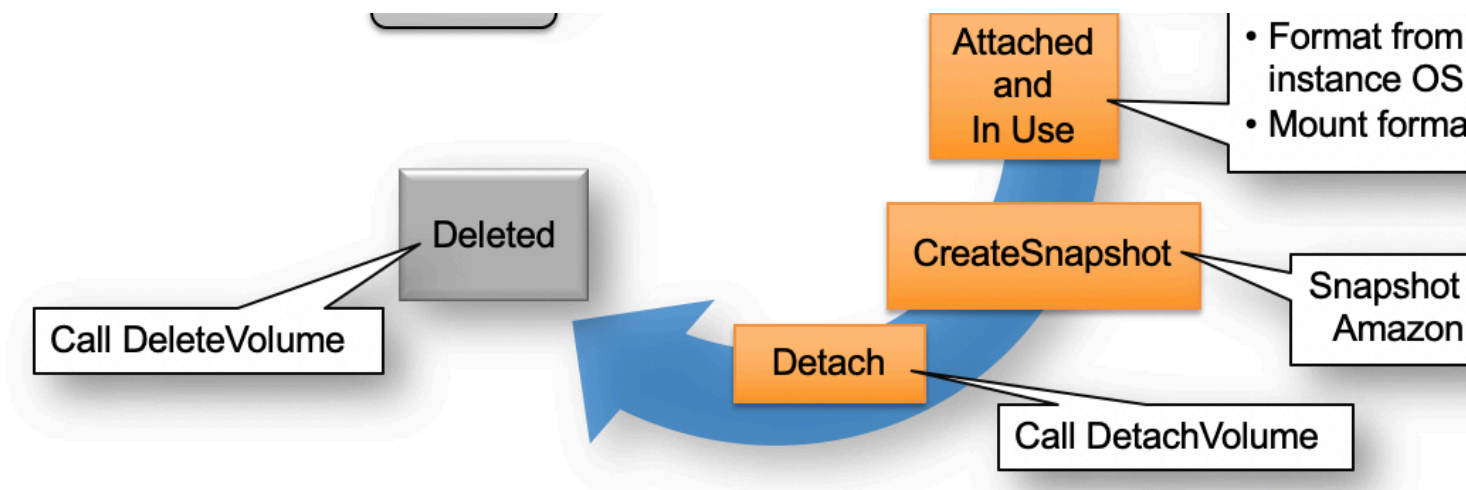
B file?

ge

st be updated



o affiliate with
stance



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
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 is terminated.
Instance store volumes	The data is preserved.	The data is erased.	The data is lost.
EBS volume	The volume is preserved.	The volume is preserved.	The volume is preserved.
Billing	Instance billing hour doesn't change.	You stop incurring charges as soon as state is changed to stopping.	You stop incurring charges as soon as the instance is shut down.

Amazon EC2

tted drive

to
S3

minate

EIP is disassociated from the
ance.

data is erased.

volume is deleted by default.

stop incurring charges as
n as state is changed to
ting-down.

Tenancy

Shared vs Dedicated Instance vs Dedicated Host

Characteristic	Dedicated Instances
Enables the use of dedicated physical servers	X
Per instance billing (subject to a \$2 per region fee)	X
Per host billing	
Visibility of sockets, cores, host ID	
Affinity between a host and 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/variious-userdata.txt>

Dedicated Hosts

X

X

X

X

Ex 1.2: https://aws.amazon.com/getting-started/tutorials/launch-a-virtual-machine/?trk=gs_card (window)

Ex 1.3: https://aws.amazon.com/getting-started/tutorials/launch-a-wordpress-website/?trk=gs_card

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 still within its first year.
2. Explore the Configure Instance Details, Add Storage, and Add Tags pages. The default settings should work fine.
3. On the Configure Security Group page, make sure there's a rule for SSH (port 22) traffic. It should be there by default.
4. Before letting you launch the instance, AWS will require you to create a key pair. Follow the instructions.
5. Once the instance is launched, you can return to the Instances page until everything is running properly.
6. Click the Actions pull-down and then the Connect item for the instance to connect to the instance from your local machine. Then connect 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 Character**

1. With an instance running, open the Instances Dashboard. Select the instance and click the Monitor link in the bottom left.

[=gs_card](#) (linux)
ows)

[trk=gs_card](#)

d select a Linux AMI and
if your AWS account is

dd Tags pages—although

rule permitting incoming

u to select—or create—a

ces Dashboard to wait

nstructions on how to
nect and take a look at

nge its instance Type

elect the instance you're

of the instance. That's