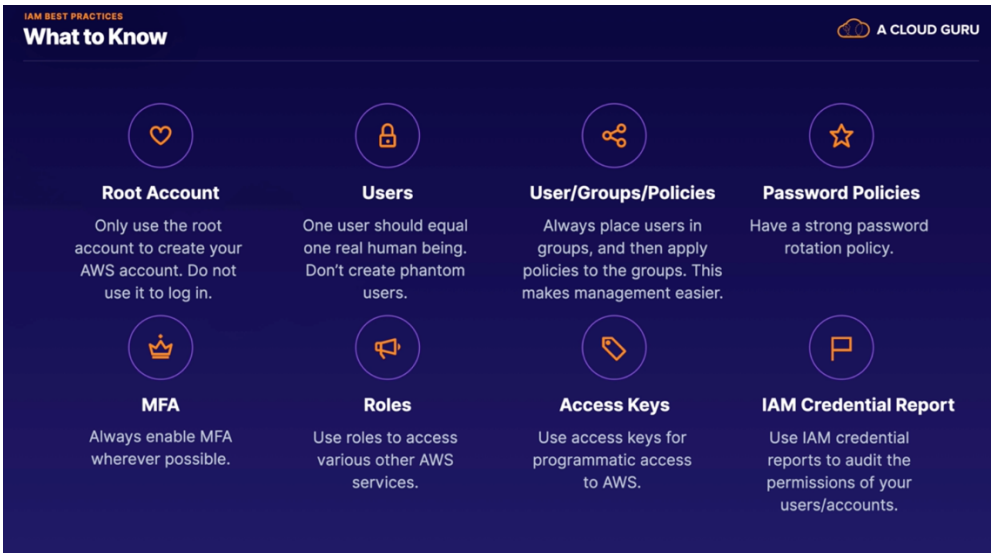
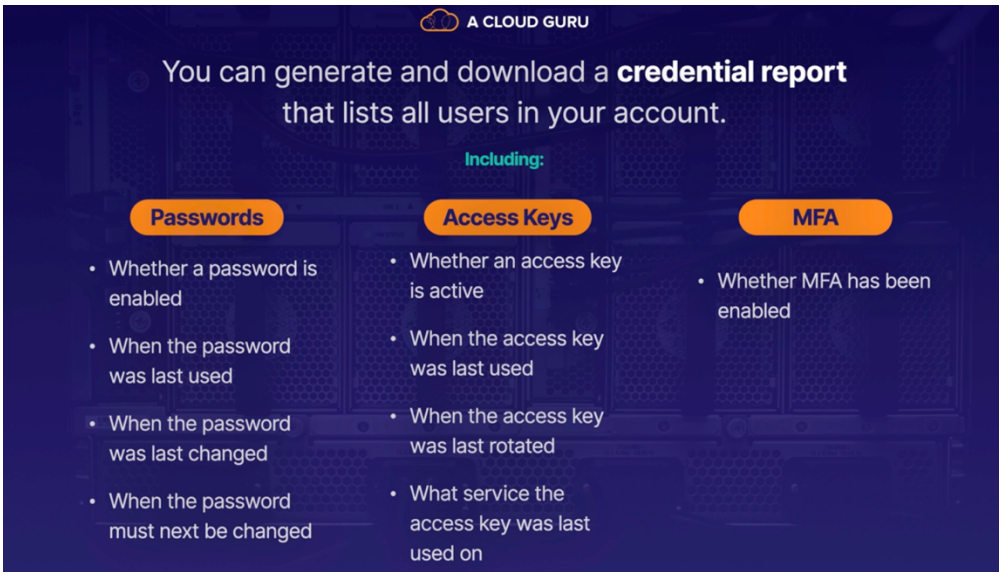


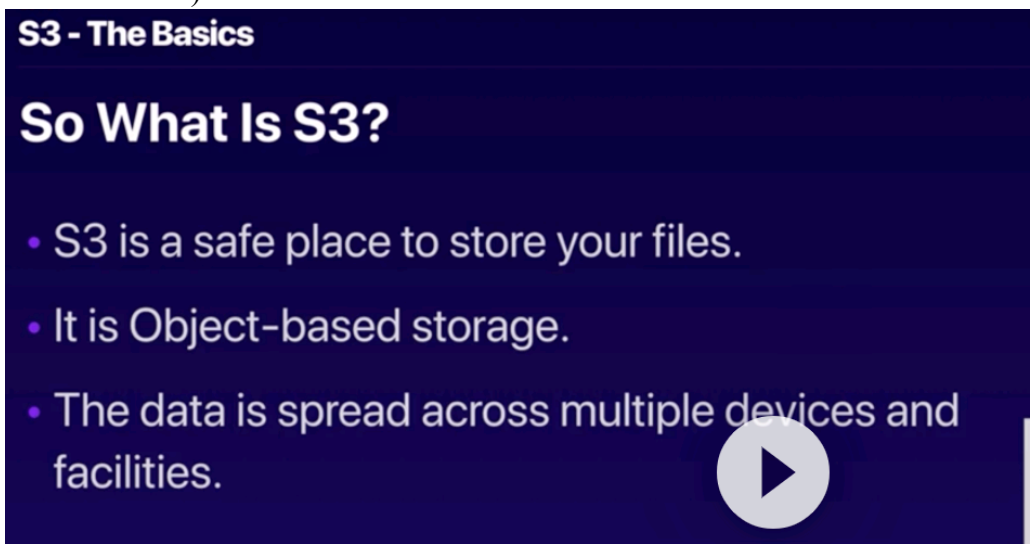
Roles :
For instance you might want to give a VM an access to s3 or the other services. then you create a role for that.

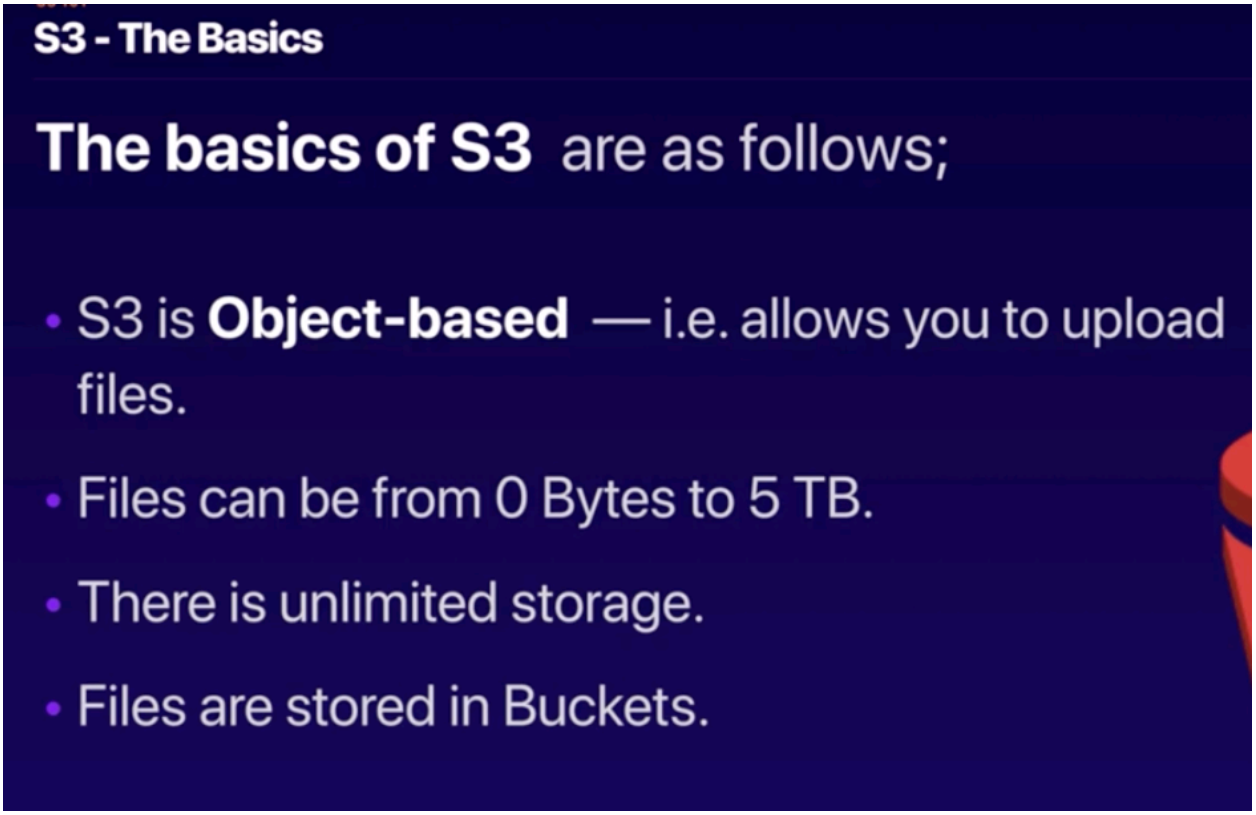
IAM credential reports:
Imagine in your organization there are 10,000 users from different group log in to AWS account and we want to know whether a password, access key or MFA is enabled and how is the situation.
We can generate and download a IMA credential reports that list all the users and it shows all the below



How to do :
IAM , credential reports , download credential reports

S3 101 :
Simple Storage Services
The longest service AWS
It s a place for storing flat files , flat files is the files that does not change like text , pictures , video , etc
Databases are not flat files since they are changing time to time
S3 is Object based storage is to store your files
Block base storage is where you save your operating system files and data bases etc (s3 is not useful for that)





S3 - The Basics

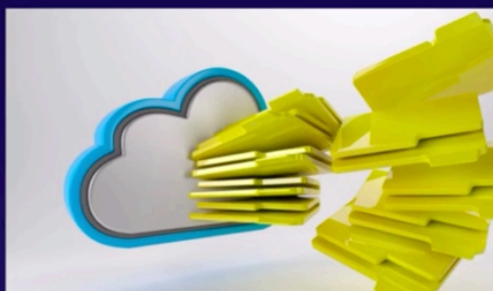
The basics of S3 are as follows;

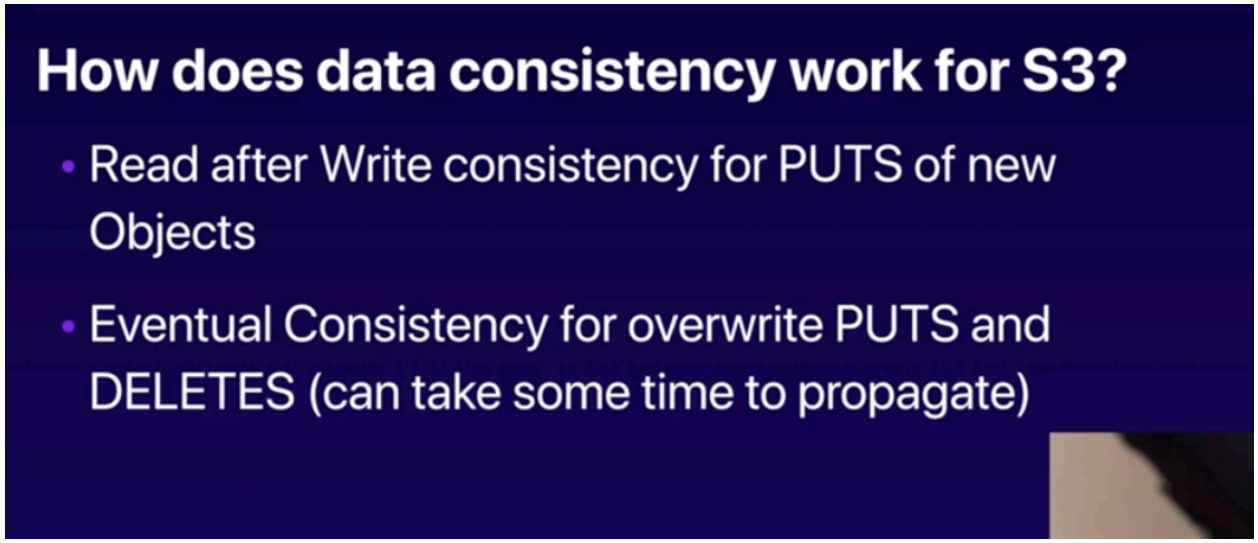
- **S3 is a universal namespace**. That is, names must be unique globally.
- https://s3-eu-west-1.amazonaws.com/acloudguru
- When you upload a file to S3, you will receive a
- **HTTP 200 code** if the upload was successful.

S3 address : the s3 service , the region , the bucket name
Since it s a form of http, then the naming should be unique
S3 is an object based and by object means files :

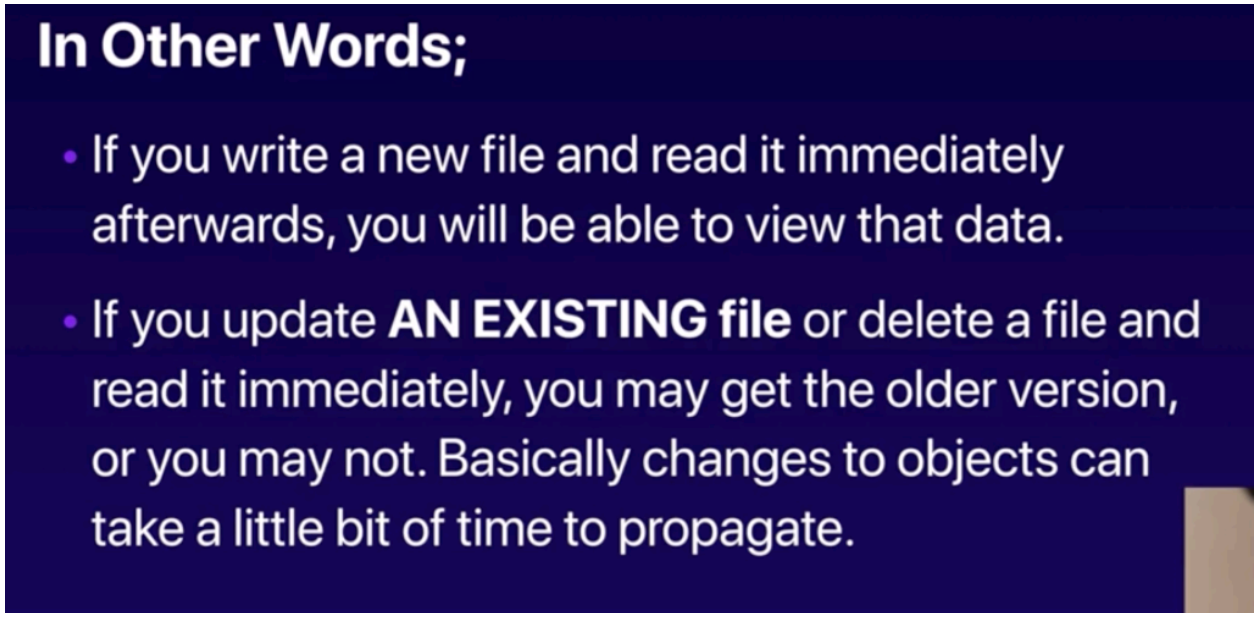
S3 is Object based. **Think of Objects just as files.**
Objects consist of the following:

- Key (This is simply the name of the object)
- Value (This is simply the data and is made up of a sequence of bytes).
- Version ID (Important for versioning)
- Metadata (Data about data you are storing
- Subresources;
  - Access Control Lists
  - Torrent



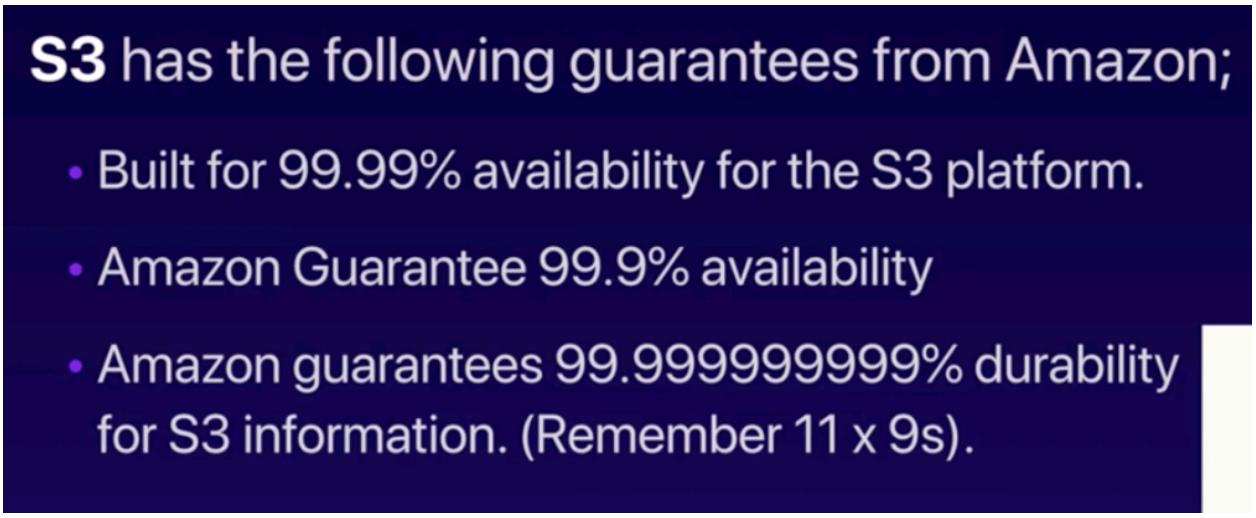


What does it mean ?



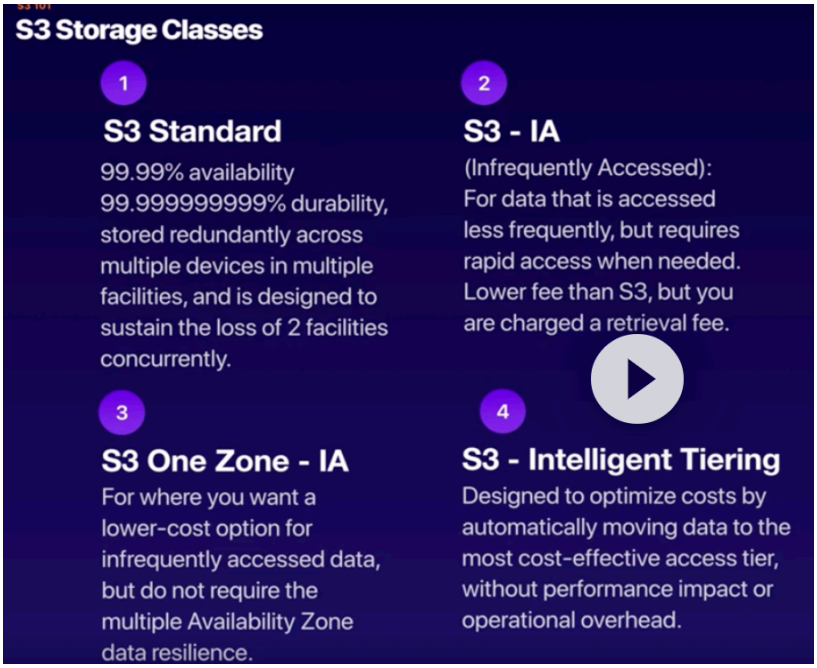
We can read the exact file immediately after we put it there , but consistency for the existing file to be changed or deleted (overwrite puts) may take some time . immediately we may not see the changes.

S3 guarantees :
99.99% availability

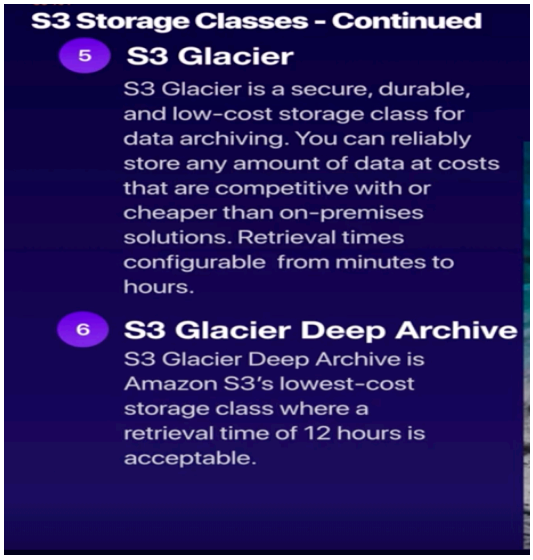


S3 features:

1. Tiered storage availability
2. Life Cycle management
    a. Over the time you can define which tier it goes to
3. Versioning
    a. Authorizing and setting back to the previous versions
4. Encryption
5. Secure your data using Access Control Lists and Bucket Policies
    a. Access control list work on individual file or object level
    b. Bucket policies work on the entire bucket



S3 intelliginet tiering is using ML to store and move data based on it s call request frequency .



	S3 Standard	S3 Intelligent-Tiering*	S3 Standard-IA	S3 One Zone-IA†	S3 Glacier	S3 Glacier Deep Archive**
Designed for durability	99.999999999% (11 9's)	99.999999999% (11 9's)	99.999999999% (11 9's)	99.999999999% (11 9's)	99.999999999% (11 9's)	99.999999999% (11 9's)
Designed for availability	99.99%	99.9%	99.9%	99.5%	N/A	N/A
Availability SLA	99.9%	99%	99%	99%	N/A	N/A
Availability Zones	≥3	≥3	≥3	1	≥3	≥3
Minimum capacity charge per object	N/A	N/A	128KB	128KB	40KB	40KB
Minimum storage duration charge	N/A	30 days	30 days	30 days	90 days	180 days
Retrieval fee	N/A	N/A	per GB retrieved	per GB retrieved	per GB retrieved	per GB retrieved
First byte latency	milliseconds	millseconds	milliseconds	milliseconds	select minutes or hours	select hours

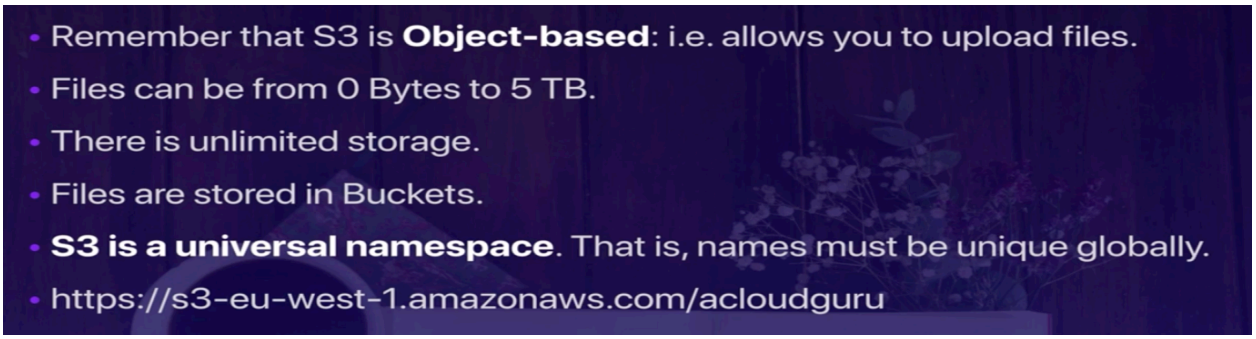
For s3 you are charged for

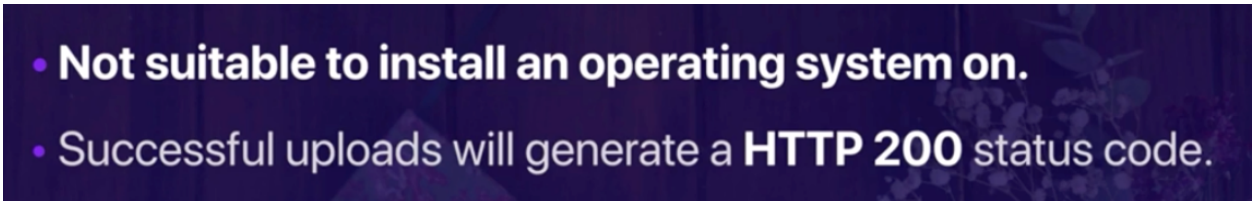
- Storage
- Requests
- Storage Management Pricing
- Data Transfer Pricing
- Transfer Acceleration
- Cross Region Replication Pricing

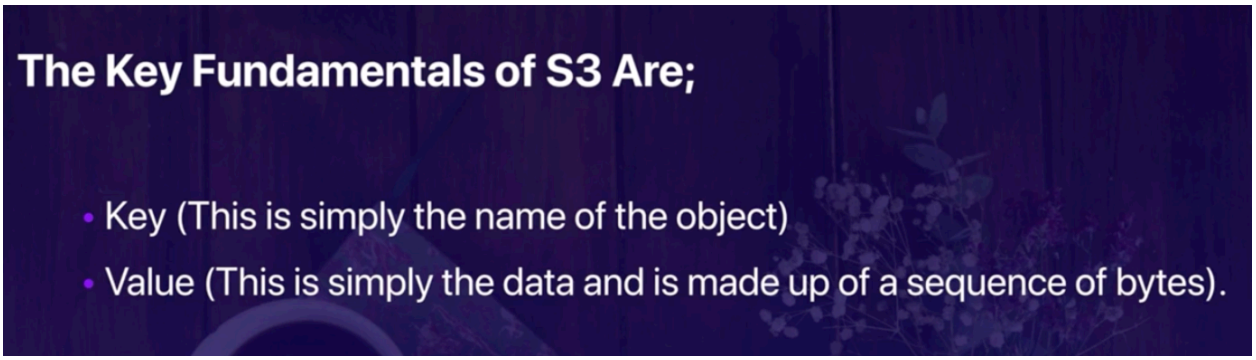
Imagine users over the globe wants to upload a file to s3 bucket, they upload it to the edge location near themselves and then it uploaded to the s3 bucket where it is hosted.

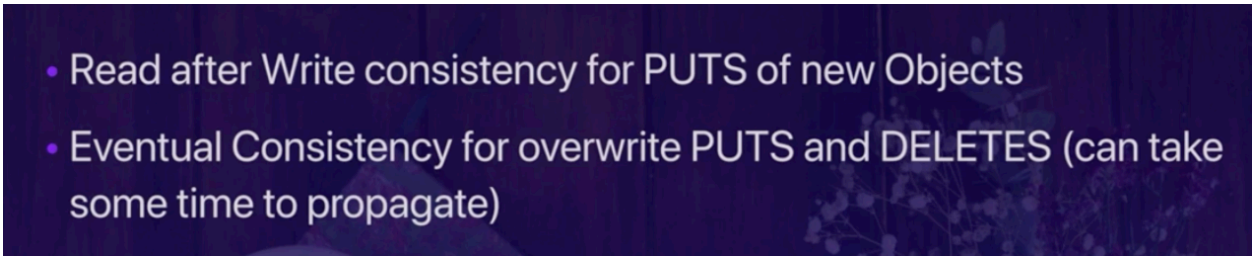
Cross Region replication:
Having a backup bucket in another region. when you upload a file to the primary one, it is replicated and stored in the secondary one as well.

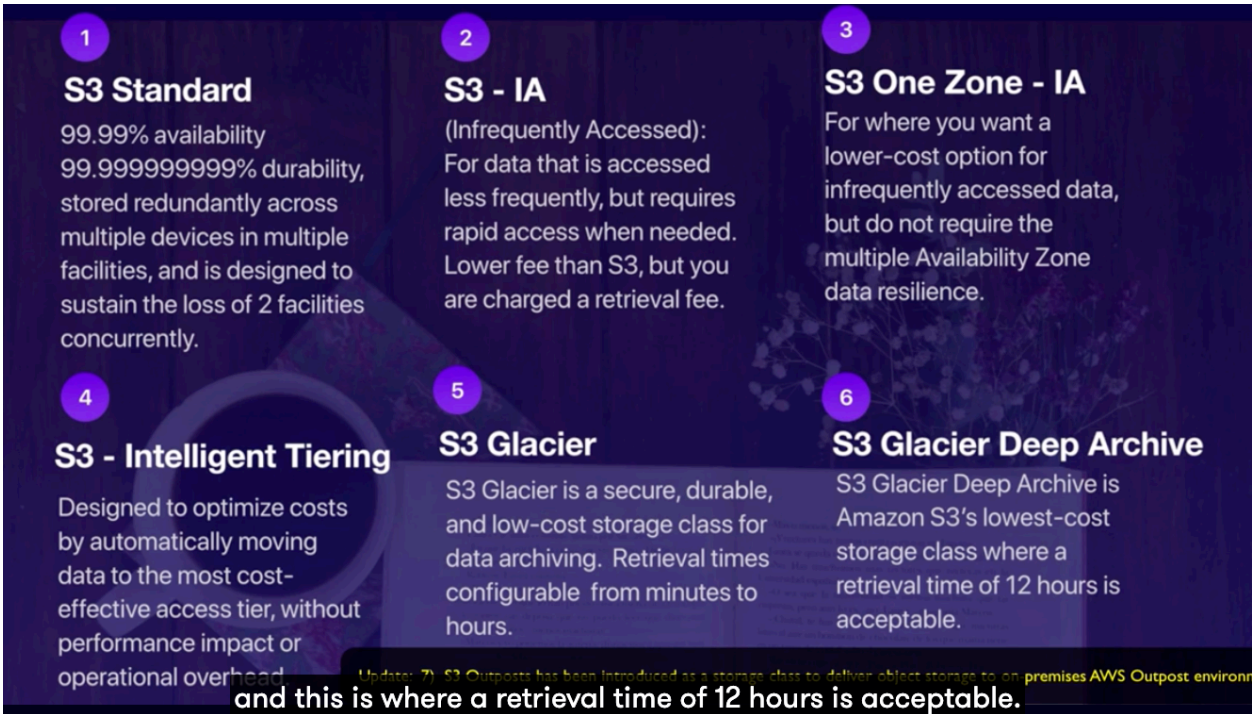
TIPS











How to create a bucket
In s3 dashboard , the region changes automatically to global and it s a gloabal service
Bucket name should be unique
Buckets by default is not public unless you make it public

Lets a create a bucket and add an object to it . if we click on the object it opens the infor of the file and there is a public URLs if we click on that we get the access denied xml file , why because the file (bucket) by default is not open to the public.

There is also object management overview where we can enable versioning or some other configuration
There is also storage class where we can change it from standard to IA or one zone IA , etc .
How to make a bucket public : in the permission tab , unclick the block all public access . and then we can check the status of accessibility of the bucket.
Then we need tro click on the certain object and make it public. Then if we click on the URL then the file becomes accessible to every ine. So making bucket public is not enough we have to make the object also public . click on it and action make it public.

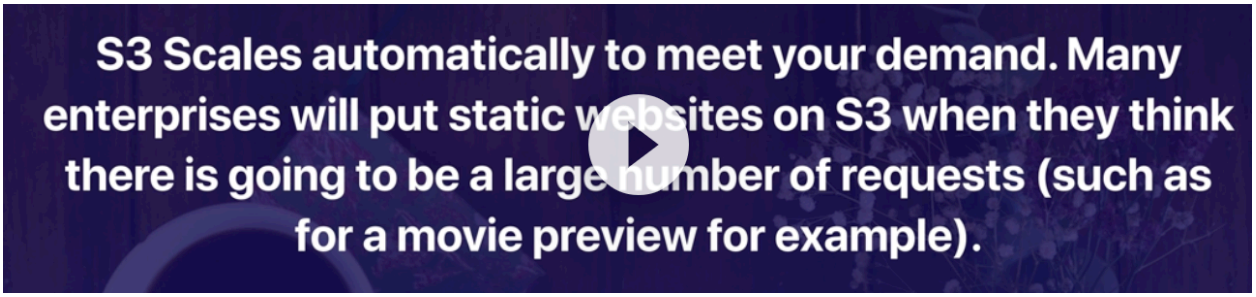
Transfer accelation :
Bucket properties > transfer acceleration
If you click on more, we navigate to another page where we can find the simulator saying what could have happened if we had the transfer acceleration tool on.

TIPS :
Bucket name should be unique .
You view thee buclet gloabally but actuallty there in some / one individual regions.
We can replicate our buckets by cross region replication
Storage class and encryption
    Standard
    IA , IA one zone , intelligence , glacier , deep glacier
S3 transfer acceleration:
- How : see above using edge location
- Where : in bucket properties and transfer acceleration
- Also we can see the demo tool for that

Restricting access:
- Bucket policy : apply across the whole bucket
    - How : permission , unclick the block access
- Object policy
    - How : select the file and by action make it public
- IAM policies to users & Group : access to some buckets or not

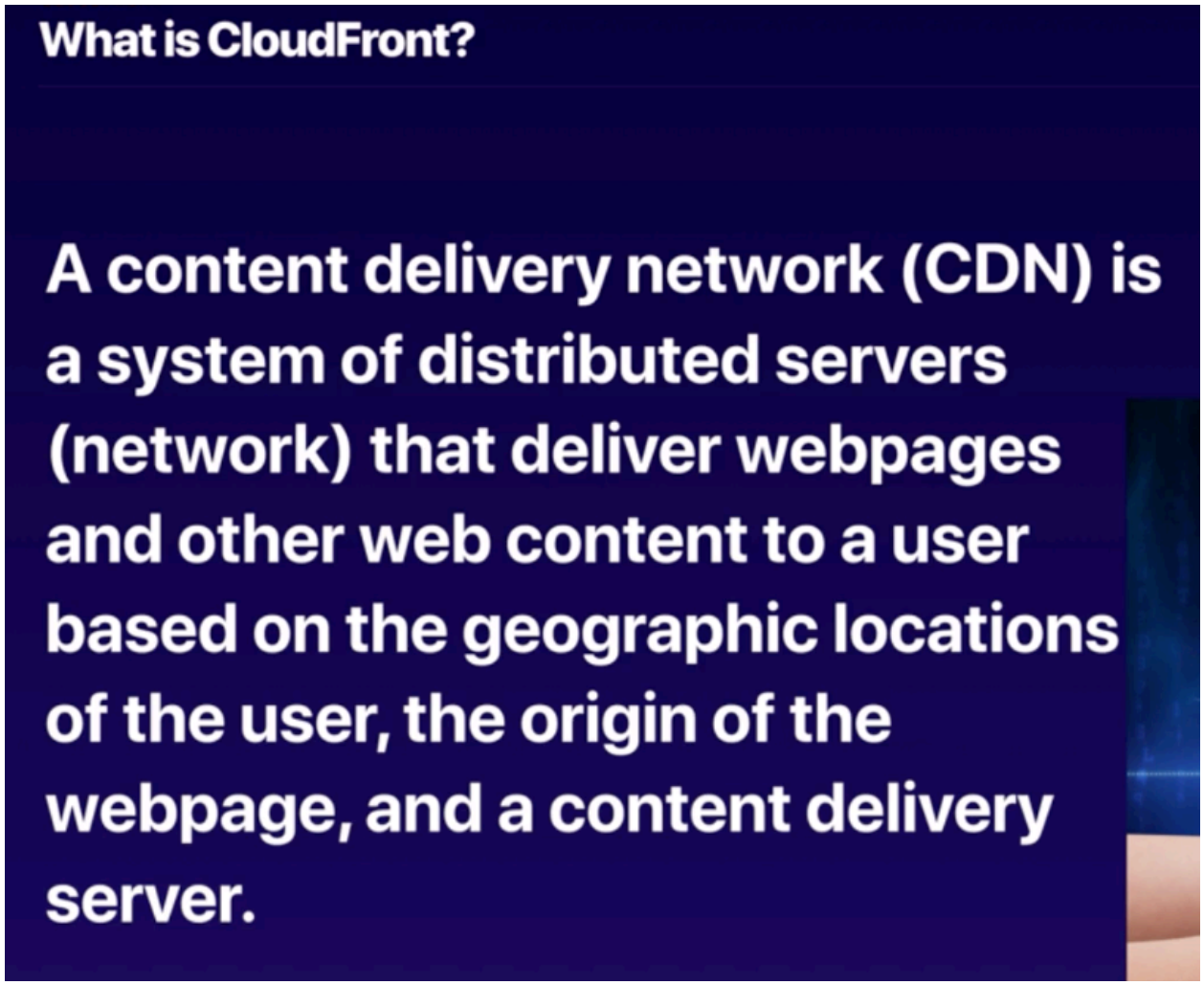
How to make a whole bucket public without making every single file make public ?
- Permission > bucket policies
- Download a policy example , in text editor , we copy that one and put as our new policy and make sure to update arn with our arn in the resource section of json file. Help from https://docs.aws.amazon.com/AmazonS3/latest/dev/example-bucket-policies.html

How to create a website on s3 bucket ?
- After making it public
- Properties > edit static hosting website > enable
- We insert our html file and error file for the web site we would like to be static like index.htl and error.htm and we upload them as well.

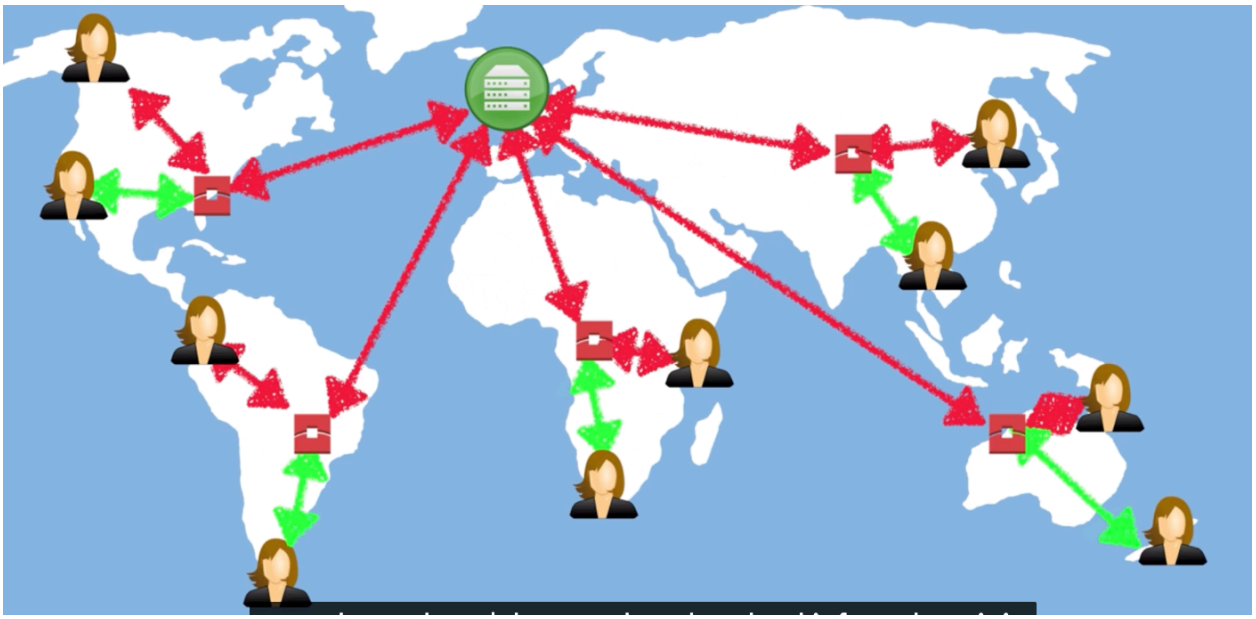


S# versioning : it s enough for the exam
Properties > versioning > enable
If we go back to the bucket beside action tabs we can see list versioning button.
We can always see old versions , includes all writes and even if you delet an object
Create backup tools
Versioning cannot be disabled , it can be suspended
Integrates with lifecycle
Versioning with MFA delete capability

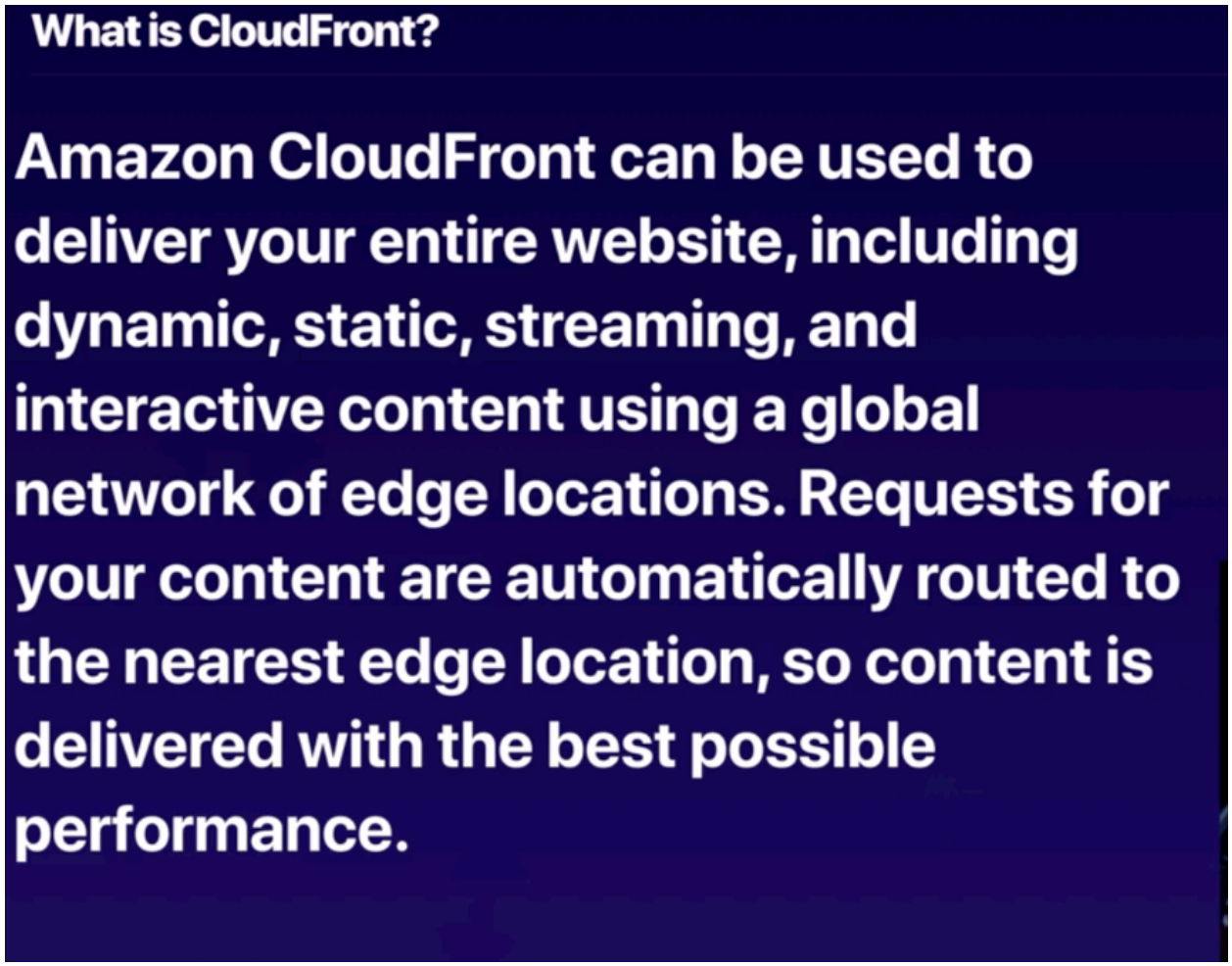
AWS Cloud front :



Let s assume there's a video sitting on a server somewhere and people from all over the globe wants to see that video, without CDN content delivery network , it takes quite time for each of them depending on their location their connection speed and etc.
Edge location: the location where the content is cashed
Origin: the origin of the file it can be s3 or ec2 or any elastic load balancer or rout 53
Distribution: this is the name given the CDN which consists of a collection of edge locations



So the first user is getting the file at alatency and the file is cashed on edge location and the second users (green) get the file from the edge
TTL , time to live is the span of time the file exists in the edge location and it is defined in seconds by default it will be sitting there for 48 hrs ,



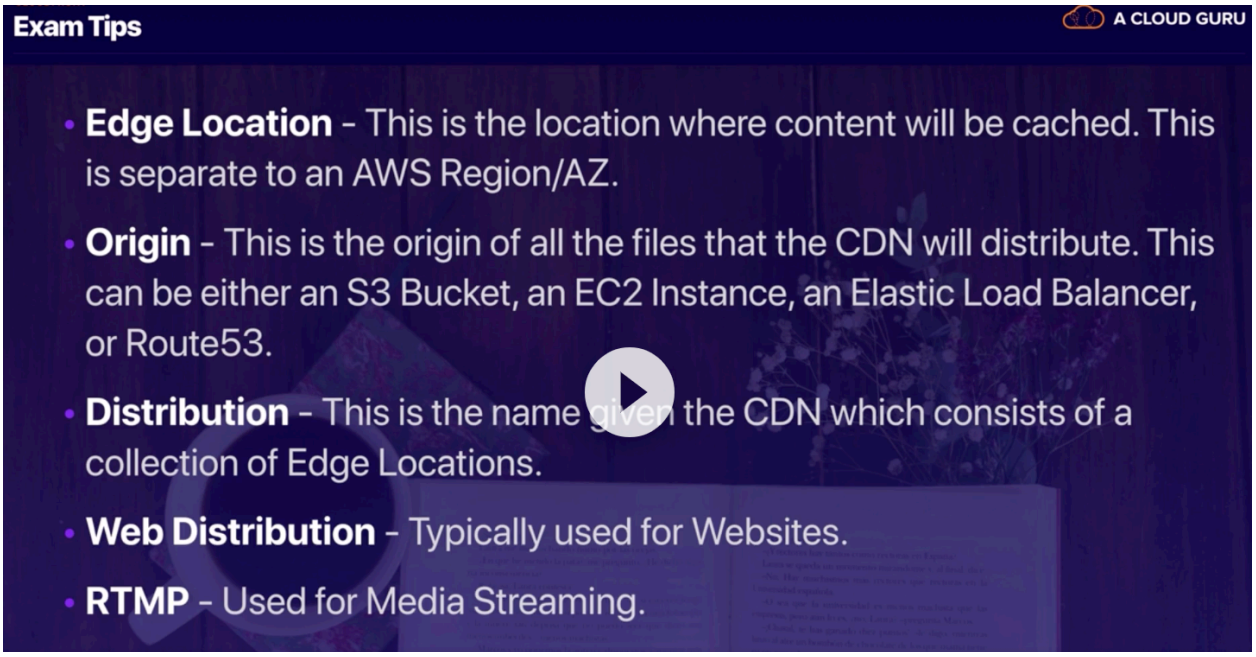
Cloud front distribution :

- Web Distribution : used for website
- RTMP – used for media streaming

Setting up cloud front :

- Network and content delivery > cloud front >
- giving the address of the bucket name (endpoint)
- after it s deployed , it gives the address ,
- if we put the address/object (object is a file name in the bucket) == > it would be fetched very quickly

it takes about half an hour to be deployed
copy the link / the file in the bucket and it s being fetch fairly quick

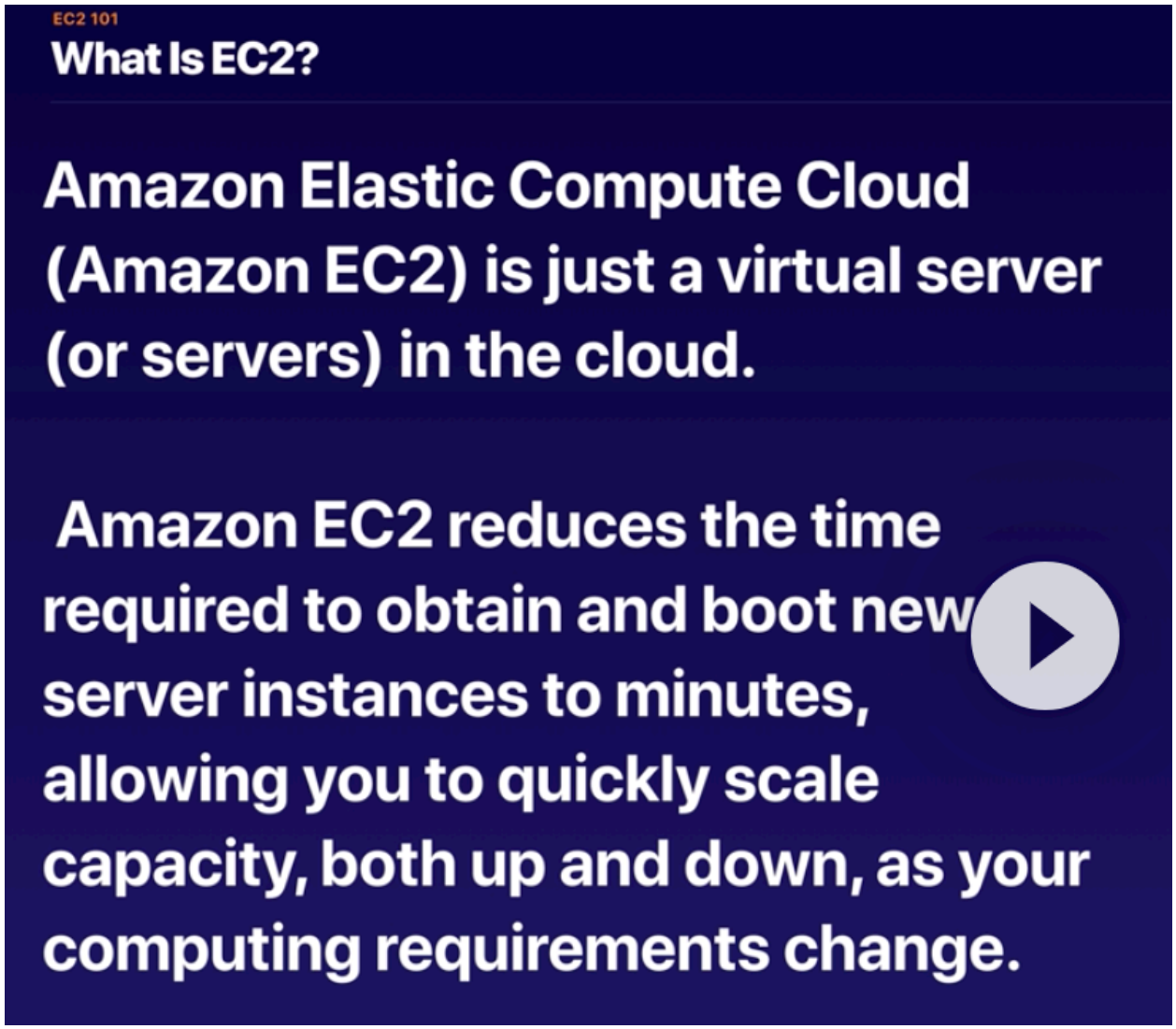


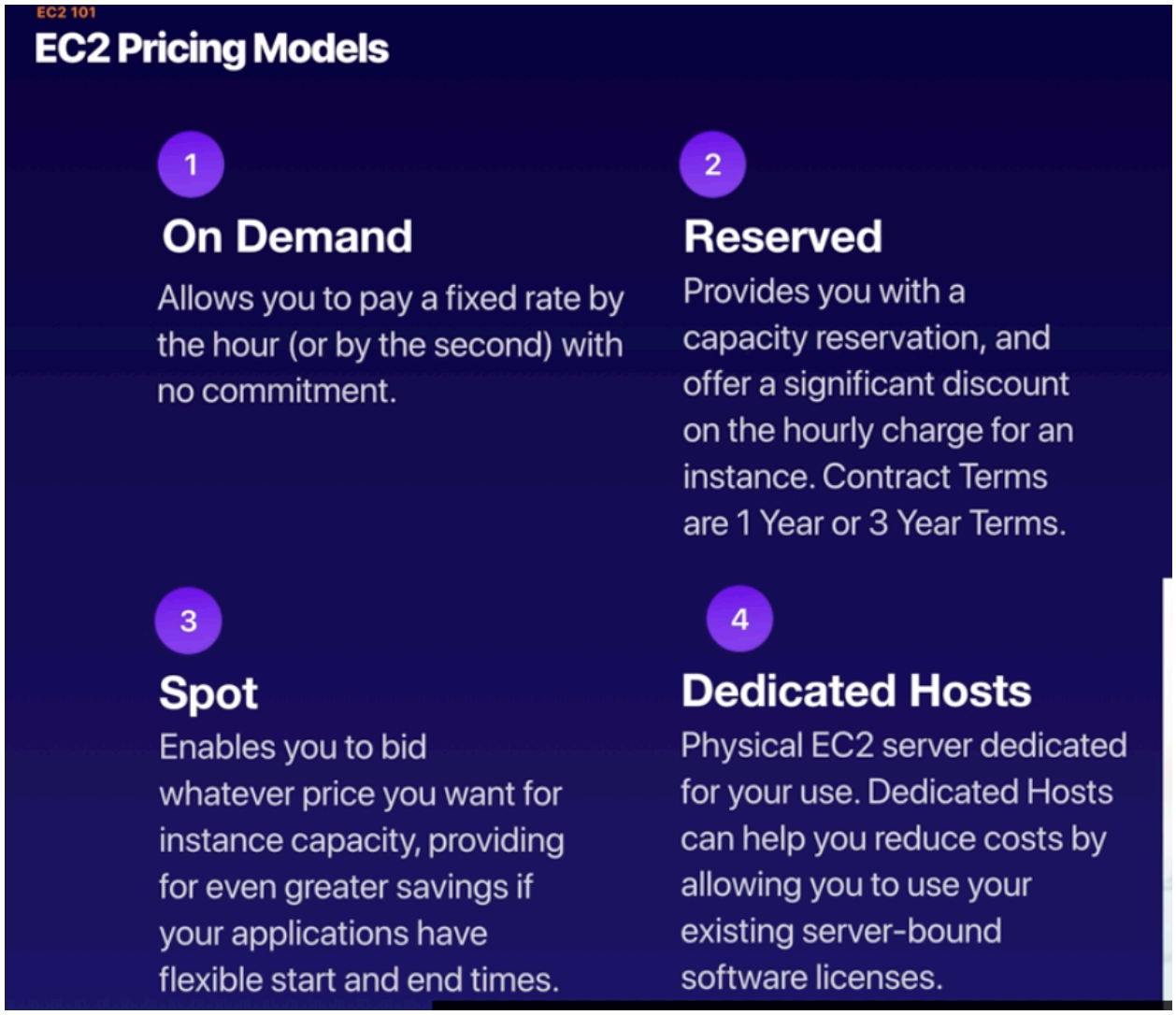
Edge location are not just read only and we can write as well. Using the tranfrom acceleration
Objects are cashed for TTL (in seconds)
You can clear cashed object, but you are charged to do that

- Network and content delivery > cloud front >
- Disable
- Delete

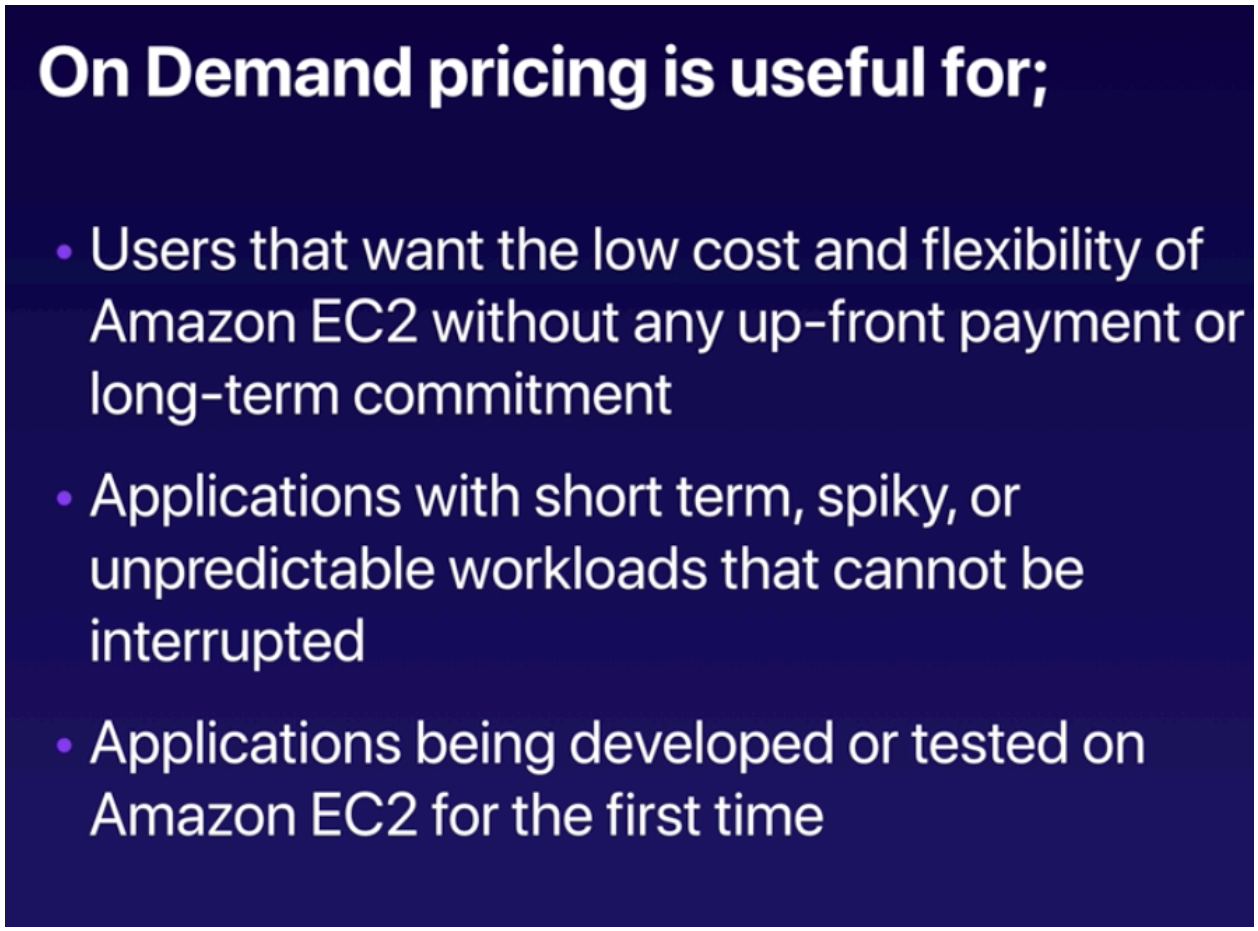
Note that origin can be s3 bucket, Ec2, elastic load balancer, route 53!

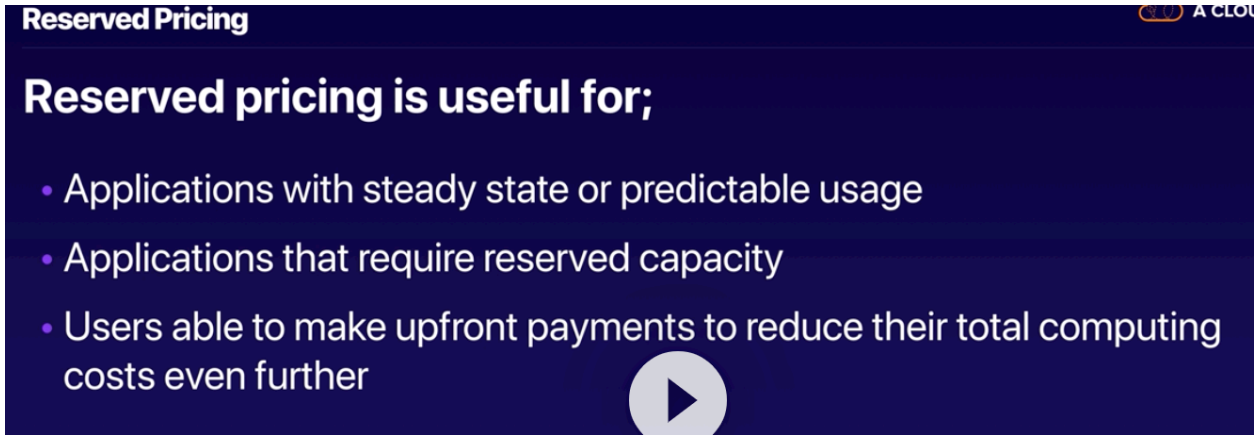
EC2:


EC2 101
What Is EC2?
Amazon Elastic Compute Cloud (Amazon EC2) is just a virtual server (or servers) in the cloud.
Amazon EC2 reduces the time required to obtain and boot new server instances to minutes, allowing you to quickly scale capacity, both up and down, as your computing requirements change.



Dedicated host are useful when you have some especial software licenses or something with specified protocols.



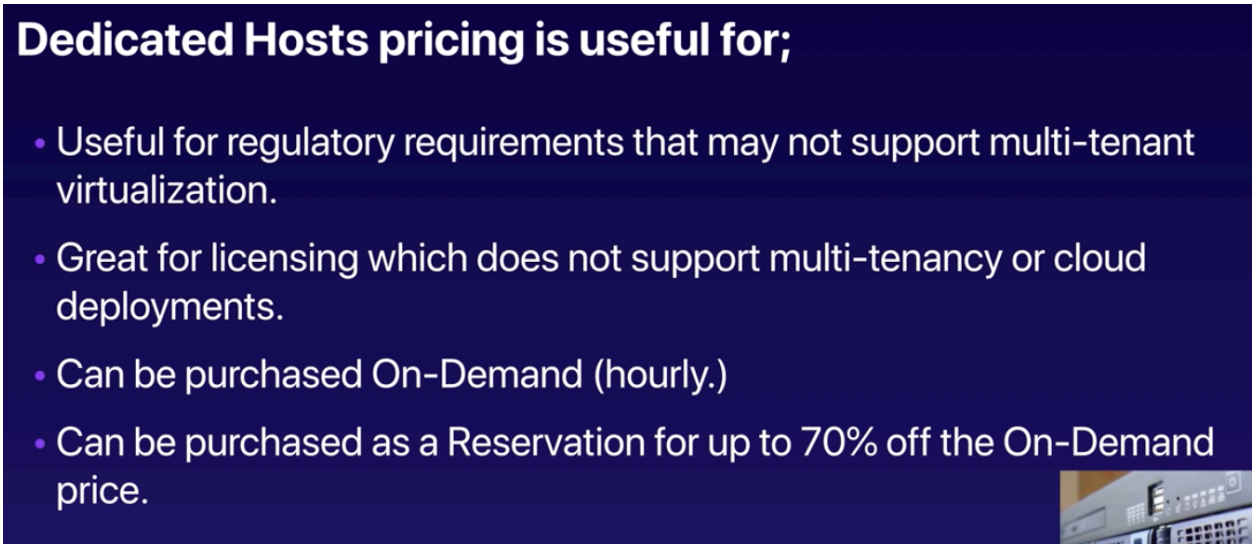


Reserved instances :

- Standards : you can not change the instance
- Convertible : you can chnag efrom one class of instance to the other class
    - Many classes of EC2 exists for high computation or memory performance
- Scheduled : there are available at the specific time frames

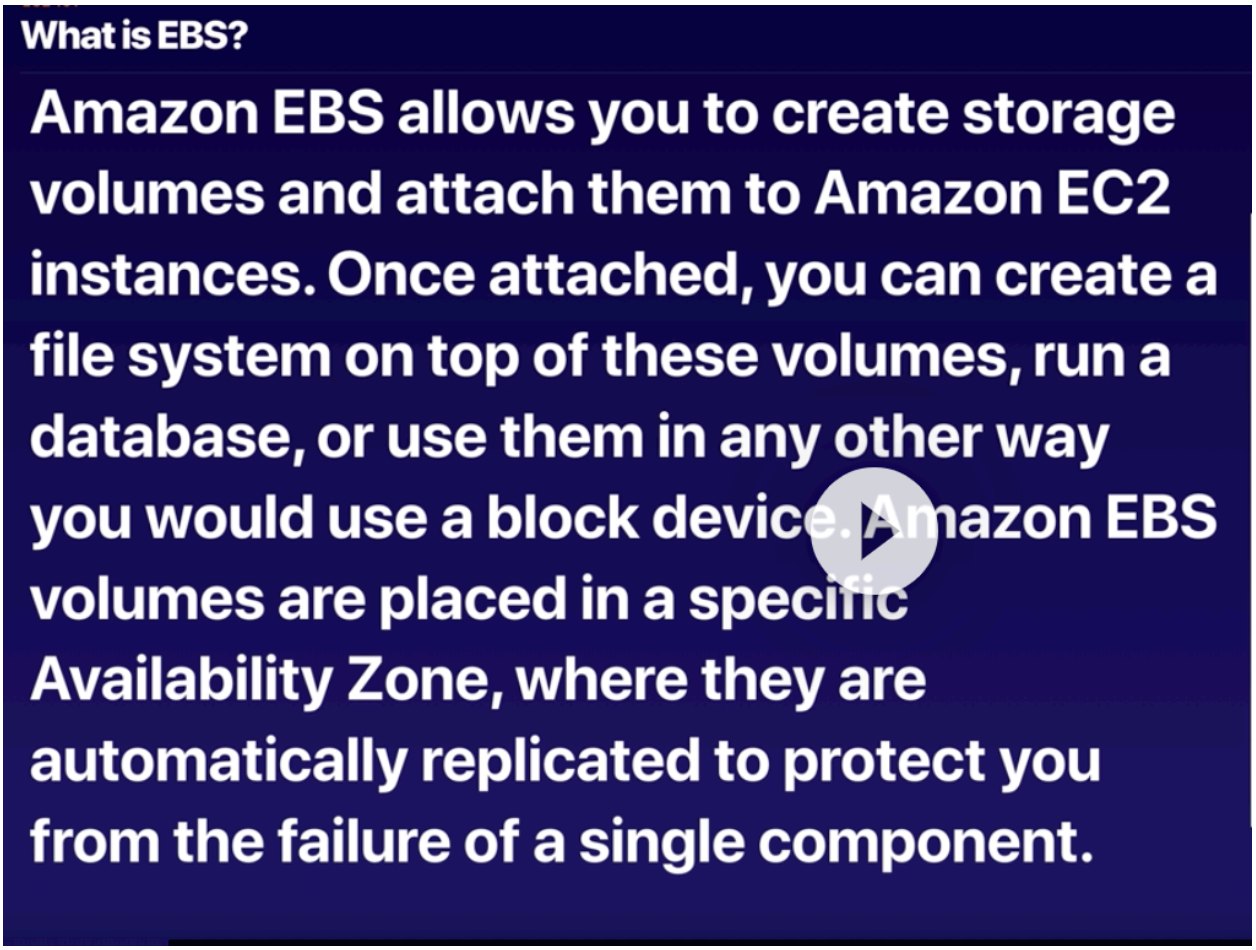
Spot pricing:

- Apllications having flexible start and end time
    - Like research labs , they can bid to have an instance , and run their job
- Applications that re feasible at a very low compute price (search , genom sequence)
- Urgent need , we can bid higher than demand and have our instance very quickly



Fight Dr. McPxz au (Australia)

Family	Speciality	Use case
F1	Field Programmable Gate Array	Genomics research, financial analytics, real-time video processing, big data etc
I3	High Speed Storage	NoSQL DBs, Data Warehousing etc
G4	Graphics Intensive	Video Encoding/ 3D Application Streaming
H1	High Disk Throughput	MapReduce-based workloads, distributed file systems such as HDFS and MapR-FS
T4g	Lowest Cost, General Purpose	Web Servers/Small DBs
D2	Dense Storage	Fileservers/Data Warehousing/Hadoop
R6g	Memory Optimized	Memory Intensive Apps/DBs
M6g	General Purpose	Application Servers
C6g	Compute Optimized	CPU Intensive Apps/DBs
P3	Graphics/General Purpose GPU	Machine Learning, Bit Coin Mining etc
X1e	Memory Optimized	SAP HANA/Apache Spark etc
Z1D	High compute capacity and a high memory footprint.	Ideal for electronic design automation (EDA) and certain relational database workloads with high per-core licensing costs.
A1	Arm-based workloads	Scale-out workloads such as web servers
U-12TB1	Bare Metal	Bare metal capabilities that eliminate



EBS : virtual hardware disk for EC2 on the cloud
Your EC2 instance should be always be in the same availability zone where EBS is

What is EBS?

A CLOUD GURU

SSD

General Purpose SSD (GP2) - balances price and performance for a wide variety of workloads.

Provisioned IOPS SSD (IO1) - Highest-performance SSD volume for mission-critical low-latency or high-throughput workloads

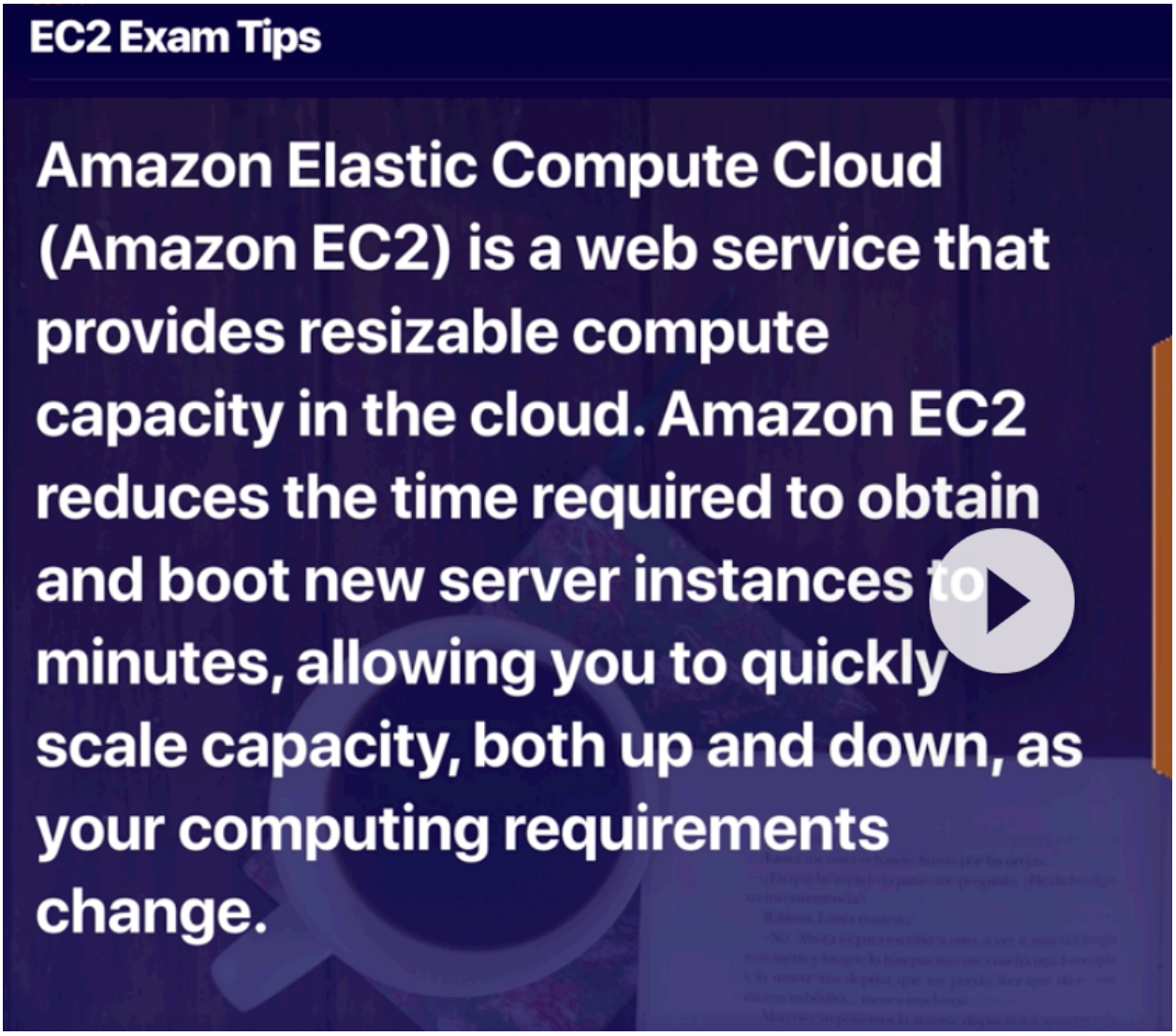
Magnetic

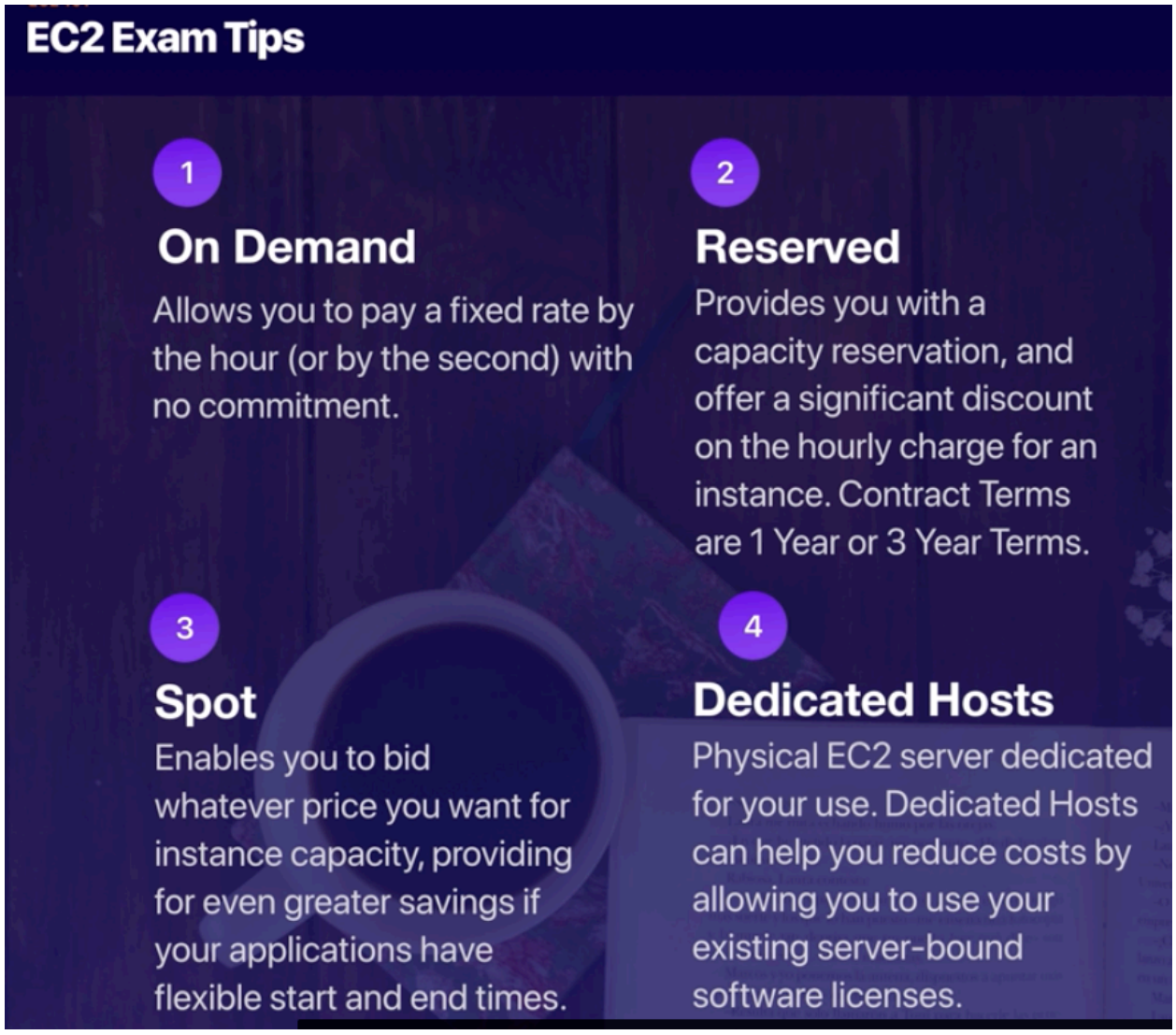
Throughput Optimized HDD (ST1) - Low cost HDD volume designed for frequently accessed, throughput-intensive workloads

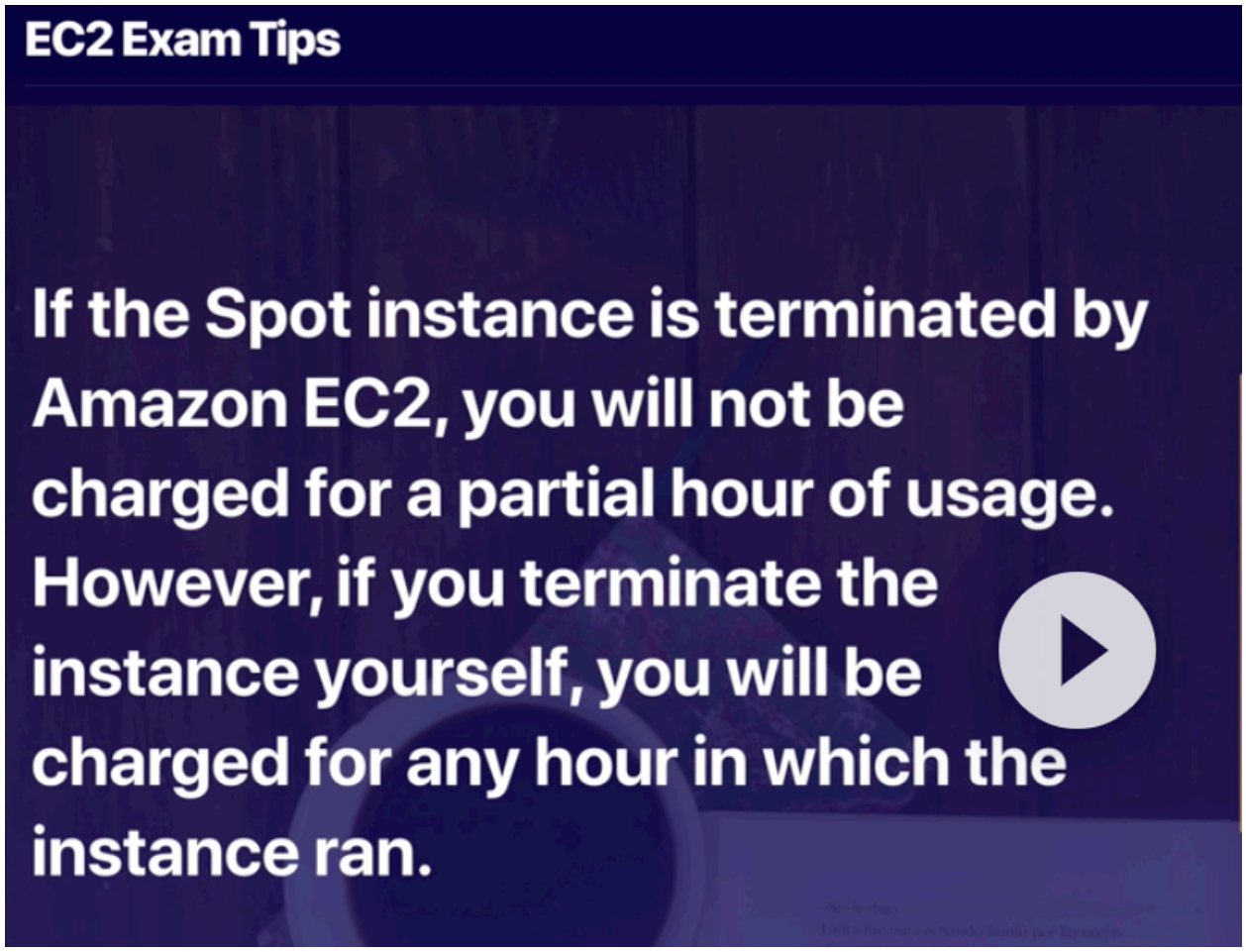
Cold HDD (SC1) - Lowest cost HDD volume designed for less frequently accessed workloads **(File Servers)**.

Magnetic - Previous Generation.

TIPs ;


EC2 Exam Tips
Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides resizable compute capacity in the cloud. Amazon EC2 reduces the time required to obtain and boot new server instances to minutes, allowing you to quickly scale capacity, both up and down, as your computing requirements change.


EC2 Exam Tips
1
On Demand
Allows you to pay a fixed rate by the hour (or by the second) with no commitment.
2
Reserved
Provides you with a capacity reservation, and offer a significant discount on the hourly charge for an instance. Contract Terms are 1 Year or 3 Year Terms.
3
Spot
Enables you to bid whatever price you want for instance capacity, providing for even greater savings if your applications have flexible start and end times.
4
Dedicated Hosts
Physical EC2 server dedicated for your use. Dedicated Hosts can help you reduce costs by allowing you to use your existing server-bound software licenses.

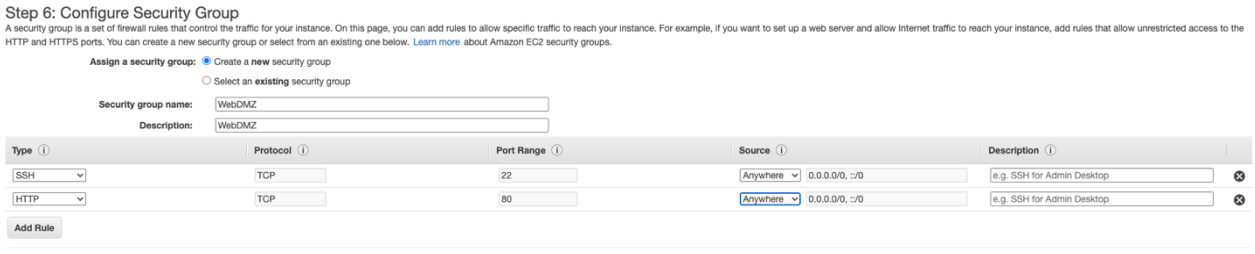


If the price goes beyond what you prepared for , AWS terminate the instance and you are not paying for the partial hour that you use . If you terminate the instance and you ran for 58 minutes , you pay for it .

Linus talks through ssh port on port 22
Windows talks through Remnote Desktop Protocols (RDP) port 3389
HTTP , port 80
HTTPS port 443
So remote computer (EC2 which is linux) talk through ssh connection
Port 22 will dictate the server (EC2) that it is a ssh connection .
Then source (local computer) can be any one or just a specific person
Meaning that if we put 0.0.0.0::0 means every one with any port can talk to the computer
However if we put it as my ip it takes just port 32 (of my local computer) and let me conncet to the server to the port 22 (this way the server understand it is a ssh connection)

To let everyone in and talk to port 22 (imagine it is linux), 0.0.0.0/0 meaning that we let everyone with any IP and port be in and talk through the computer with port 22
But if we want to limit it to just ourselves as admin, we select my/IP port 32

- For web service since we want to spread out the content, we need to allow everyone to connect
- For may be computation or admin, we may need to just lock down every one and let it be open to just our IP,
    - If in my source I click on my IP, it allows my computer (local to connect and) and if I disconnected and get another IP I have to reset it inorder to connect again



We have to create the key , the public key and private key .

- Public key : is the you can share it around
- Private : it is needed to log in

There is a public ip address

How to connect :
Using dashboard ec2 connect :

Sudo su
Yum update -y (getting the security patched)

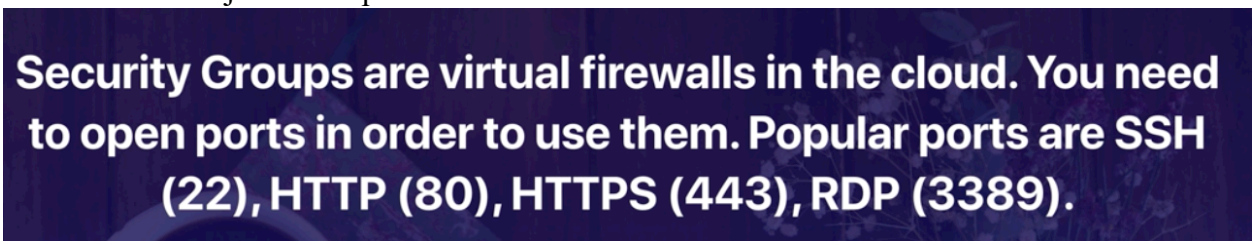
Using integrated terminal (mac)

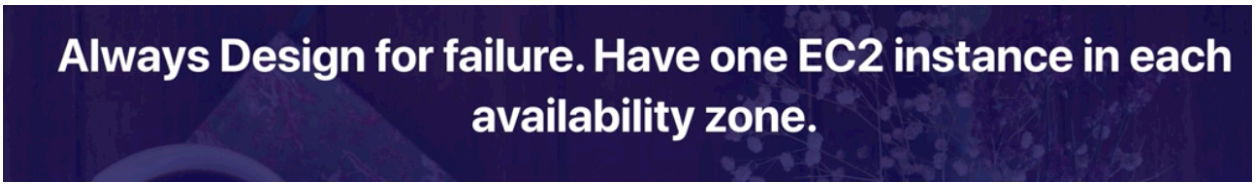
1. `chmod 400 mykey.pem`
2. `ssh -i "mykey.pem" ec2-user@ec2-54-234-161-122.compute1.amazonaws.com`
3. Sudo su
4. Yum update -y (getting the security patched , like the WebMDZ)

Using potty

Exams tip :

- EC2 is a compute based service , it s not serversless , it s a server.
- You need to connect using private key
- Linus ssh port 22
- Microsoft windows RDP 3389
- HTTp : port 80
- https port 443
- when you using security group you are using virtua firewall
    - to let every one in : 0.0.0.0/0
    - to just on e: Ip/32





EC2 Command line

If you remember using IAM m we created a user and for that user we created programtic access key (public and secret key) . If you don't save that , we can make it inactivate , delete it and activate new one.

Using either connect instance or SSH

aws s3 mb s3://hniakan. == > aws s3 make bucket name hniakan
error unable to locate credentials
ec2 instance is unable to locate credentials

```
ttps://aws.amazon.com/amazon-linux-2/

ec2-user@ip-172-31-39-35 ~]$
ec2-user@ip-172-31-39-35 ~]$ sudo su
root@ip-172-31-39-35 ec2-user]# yum update -y
oaded plugins: extras_suggestions, langpacks, priorities, update-motd
mzn2-core
o packages marked for update
root@ip-172-31-39-35 ec2-user]# ls
root@ip-172-31-39-35 ec2-user]# aws s3 mb s3://hniakan
ake_bucket failed: s3://hniakan Unable to locate credentials
root@ip-172-31-39-35 ec2-user]#
```

As we can see below , I had to put my programmatic key to my configure
I made a mistake in putting my default region I had some error and I had to reconfig again , while reconfiguring whatever yo don't want to change just hit enter and correct whatever you would like
Then ask aws s3 to create the bucket for you
Then aws s3 ls .. list all the buckets related to that user

```
[ec2-user@ip-172-31-39-35 ~]$
[ec2-user@ip-172-31-39-35 ~]$ sudo su
[root@ip-172-31-39-35 ec2-user]# yum update -y
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
amzn2-core
No packages marked for update
[root@ip-172-31-39-35 ec2-user]# ls
[root@ip-172-31-39-35 ec2-user]# aws s3 mb s3://hniakan
make_bucket failed: s3://hniakan Unable to locate credentials
[root@ip-172-31-39-35 ec2-user]# aws configure
AWS Access Key ID [None]: AKIASW7JBJGQDPDGCYXS
AWS Secret Access Key [None]: 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
Default region name [None]: us-0east-1
Default output format [None]:
[root@ip-172-31-39-35 ec2-user]# aws s3 mb s3://hniakan
make_bucket failed: s3://hniakan Could not connect to the endpoint URL: "https://hniakan.s3.us-0east-1.amazonaws.com/"
[root@ip-172-31-39-35 ec2-user]# aws s3 mb s3://hniakan1234
make_bucket failed: s3://hniakan1234 Could not connect to the endpoint URL: "https://hniakan1234.s3.us-0east-1.amazonaws.com/"
[root@ip-172-31-39-35 ec2-user]# aws s3 ls

Could not connect to the endpoint URL: "https://s3.us-0east-1.amazonaws.com/"
[root@ip-172-31-39-35 ec2-user]# aws configure
AWS Access Key ID [****************CYXS]:
AWS Secret Access Key [****************YtgP]:
Default region name [us-0east-1]: us-east-1
Default output format [None]:
[root@ip-172-31-39-35 ec2-user]# aws s3 mb s3://hniakan
make_bucket: hniakan
[root@ip-172-31-39-35 ec2-user]# aws s3 ls
2020-11-30 04:40:19 hamedniakan
2020-12-06 05:05:03 hniakan
2020-08-20 00:22:14 sagemaker-us-east-2-186782927264
[root@ip-172-31-39-35 ec2-user]#
```

So we can create a file and upload it to s3
So basically we created a file on ec2 and upload it to s3
In home directory of ec2 there is config and credentials file
Vi credentials

```
[root@ip-172-31-39-35 ec2-user]# cd ~
[root@ip-172-31-39-35 ~]# cd .aws
[root@ip-172-31-39-35 .aws]# ls
config  credentials
[root@ip-172-31-39-35 .aws]# vi credentials
```

We can see our credentials what happens if my ec2 gets hacked , they can go to the home directory and get the config .. one way tro get around is after we r done with ec2 change our credential with some random stuff
By saying aws configuration and just put bad input to them

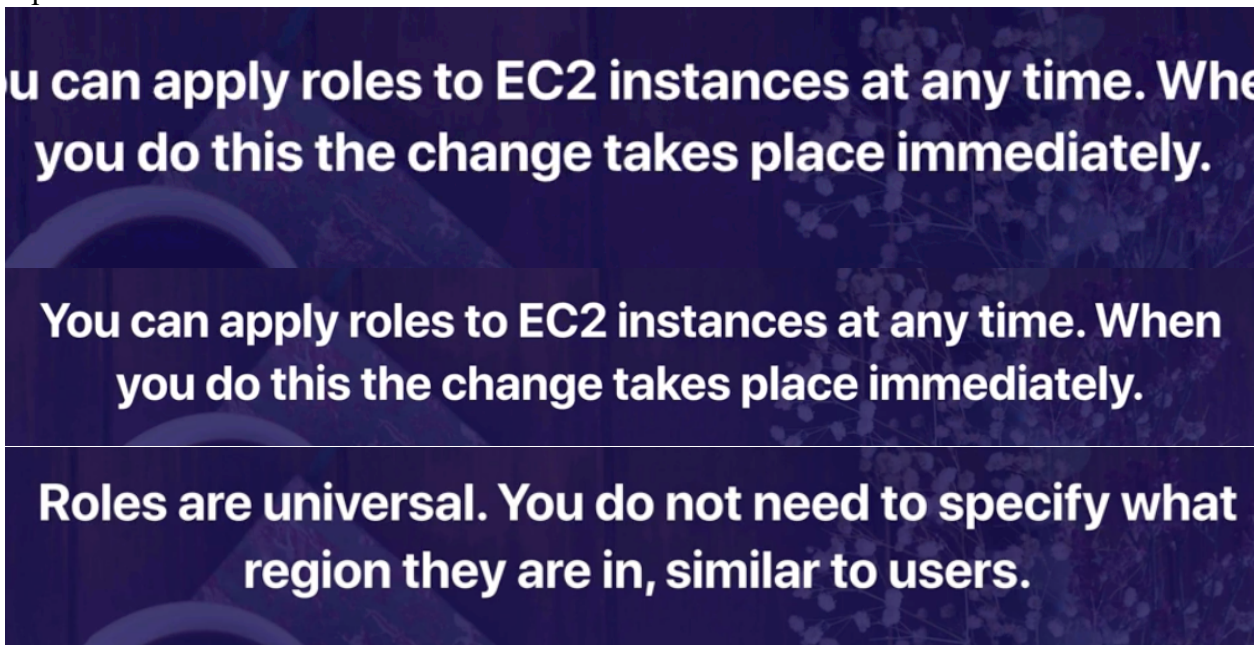
SDK is for programming language .

ROLES
More secure way to communicate with aws services
Roles : accessibility for services in the aws (resources)
Create , select service (ec2) , attach policy (se3 fill read write access) , tag , name so we have crated that role but we need to attach that role to ec2 instance as well.
So in ec2 instance , action , we attach that policy

Now if we connect to ec2 again … if we try to communicate with s3 like aws s3 ls
We ll get error
Why ? since we give it some bad input for our credential fro sake of not getting hacked
So .. we can remove our .aws folder in th ehom edirectory
And then try … this time ec2 uses the policy attached to it and it does not ask for any credential or their validity
So .. if the instance gets hacked .. yes the hacker can have a full access to our s3 since we gave our instance the full access to s3 policy . but they don't have fiull access to the whole aws environment .

And the soon we delet our instance their access would be gone as well. The safest is using roles instead of credentials.

Tips :



Elastic Load balancer
- Load balancer routes the traffic to different availability zones

3 types of load balancer
- HTTP / HTTPS
  - Intelligence decision for routing and good for application
- TCP

    - Higj performance with static IP (always connecting from a certain instance maybe !!!)
- Previous Generations
    - Fpr test/dev and just cheap

Under EC2 , load balancer / http/https

- Give it a name
- VPC : virtual private cloud (covers later) the default is where our instances right now is and every ec2 comes with a default one , but we want it in other availability zones
- We select all the availability zones to have VPC
- SELECt webDMZ security group this is the one we already created before when running our intsnace
    - We created earlier an instance and create index.html in it
    - Our instance had a WebDMZ patch security group

- Configure the routing
    - Giving a name
    - Heath check
        - By default it looks at the /index.htm unless something else is given
    - And then config the heathy check interval and time out
- Register the target
    - Registering the webserver behind your application load balancer
        - We are adding the webserver we earlier created and registere it behind the load balancer
    - It takes some time
- Now we need to create another web server instances (EC2) in different availability zone
    - In the new one in ythe subnet we ise another Az
    - In advance
        - Bootstrap scripts : a script that runs when your instance is run instead of doing them manually
            - #!bin/bash : anything under this would be run when the instance boots
            - Yom update -y
            - Yum install httpd -y
            - Service httpd start
            - Checkconfig on
            - Cd /var/www/html
            - Echo “<html><body><h1>kos nane ramin this is web 2 </h1></body></html>” > index.html
            - It would create the index.html with that info in it
            - Using existing private key and launch it
- So if we see our instances we can see we have two instance up and running
    - 1. We created manyullay
    - 2 . we cretwed using bootstrapt script
    - Both has WebDMZ patch .. showing that they are webservice

    - They both has httpdt service on
    - /var/www/html this is the root to the website and by default instance look at index.htm that's why the path in the configure the routing , if it is empty it look for this path
    - So they (instances know) where they look for it
- Remember we said registering the target may take time , soo after it is registered , by default it is resolved to another ec2 instance and if we get its dsn anme and put it there we can see the content pull up from the index.htm and actually sometimes it s from instance
- We earlier registered one instance to the load balancer but we need to add the new one as well , so we go to the target groups edit and add the new instance (the one we created with bootstrap scripts) to the load balancer target as well.
- Then if we use the dsn of load balancer put in a brwser and referesh we see the content of html.index but actually it is sometimes from webserver 1 sometimes from 2

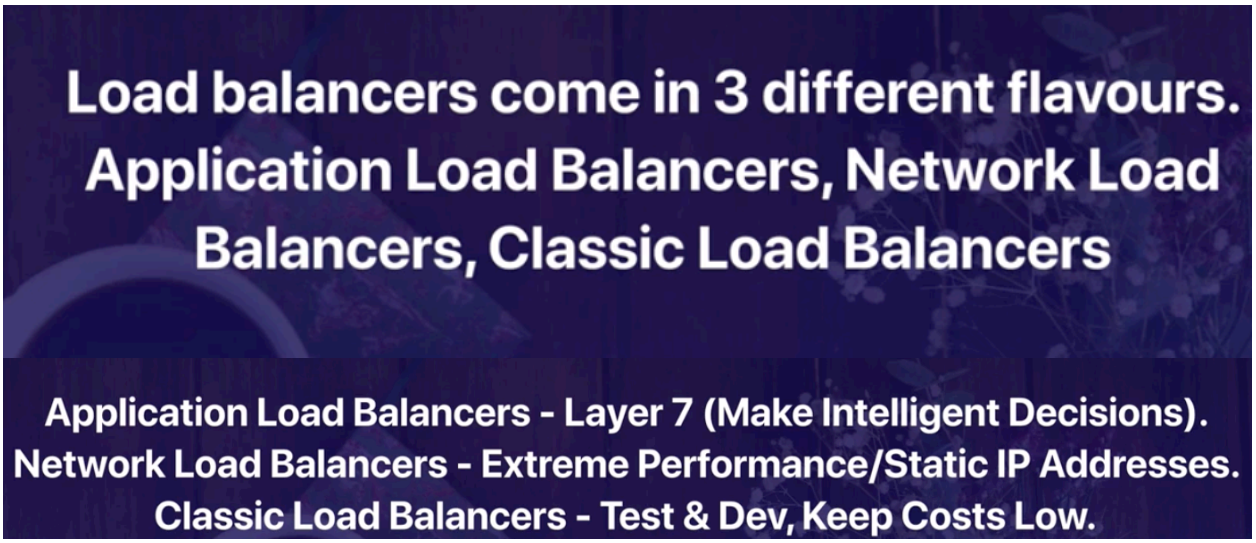
Below is the example of creating index.html
As we mentioned earlier the websericie by default look at the /var/www/html looking for index.html

```
(pytorch_env) (base) C02Z69GALVCG:Downloads hniakan$ chmod 400 hniakan.pem
(pytorch_env) (base) C02Z69GALVCG:Downloads hniakan$ ssh -i "hniakan.pem" ec2-user@ec2-3-18-101-84.us-east-2.compute.amazonaws.com

       __|  __|_  )
       _|  (     /   Amazon Linux 2 AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-2/
[ec2-user@ip-172-31-41-222 ~]$ ls
[ec2-user@ip-172-31-41-222 ~]$ sudo su
[root@ip-172-31-41-222 ec2-user]# yum update -y
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
amzn2-core
No packages marked for update
[root@ip-172-31-41-222 ec2-user]# yum install httpd
Complete!
[[root@ip-172-31-41-222 ec2-user]# ls
[[root@ip-172-31-41-222 ec2-user]# service httpd start
Redirecting to /bin/systemctl start httpd.service
[[root@ip-172-31-41-222 ec2-user]# ls
[[root@ip-172-31-41-222 ec2-user]# cd /var/www/html
[[root@ip-172-31-41-222 html]# ls
[[root@ip-172-31-41-222 html]# cd ~
[[root@ip-172-31-41-222 ~]# ls
[[root@ip-172-31-41-222 ~]# sudo su
[[root@ip-172-31-41-222 ~]# cd /var/www/html
[[root@ip-172-31-41-222 html]# nano index.html
[[root@ip-172-31-41-222 html]# ls
index.html
```

TIPS



Application load balancer making intelligent routing decisions
When you designing load balancer we need to have the multiple instances in different availability zones

RDS

Multi az vs replica

Multi az is for disaster recovery and it is for when one of your Az is down and you have to rely on the other one
You always read and write from the primary one but you have always a back up on secondary as well
But multiple replica is for performance
Your ec2 is able to write on your database and you can have up to 5 replica of it , so if it fails you (your ec2) are not able to write or read on your database. However it can be set uo to read from the replicas … so it is optimized for performance so it can be set uyo that your ec2 instance write to your primary data base and read from the replicas
Each availability zone can have it is own replica (I guess , we ll see)

RDS :

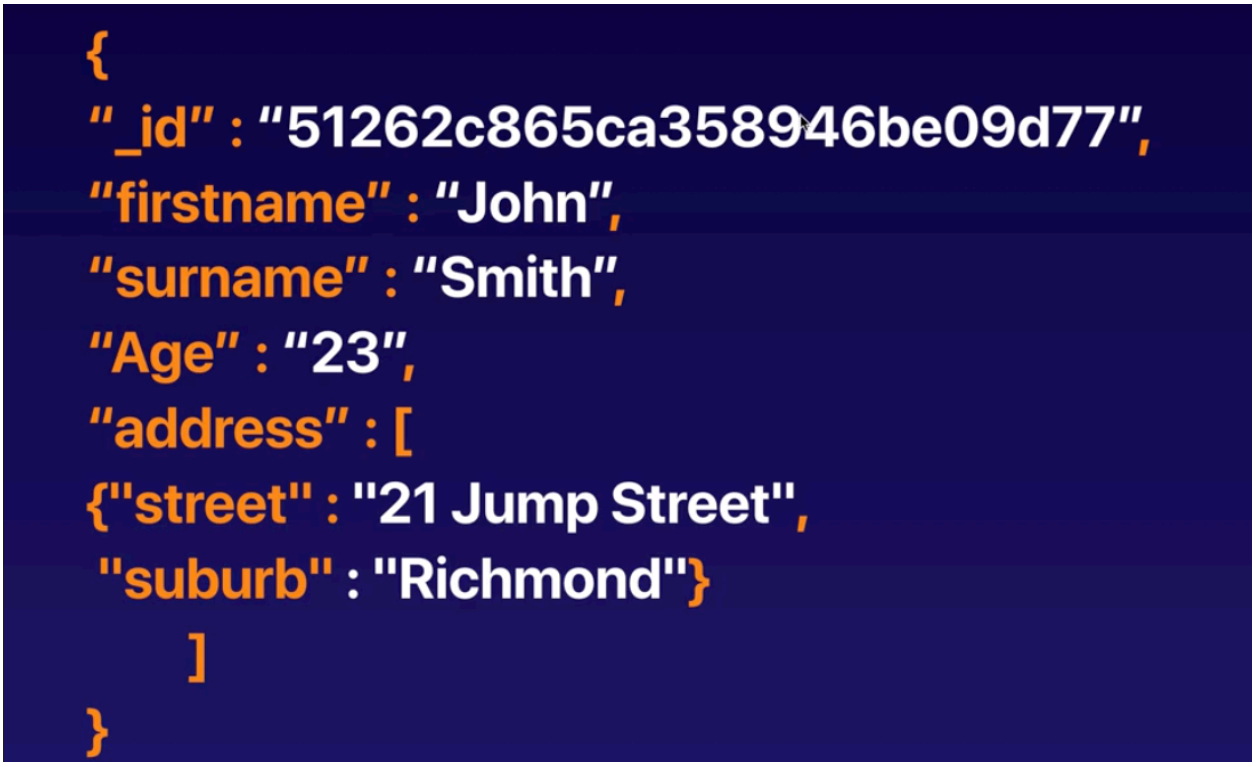
- SQL Servers
- Oracle
- Mysql server
- PostgreSQL
- Aurora (AMAZON SQL)
- Maria DB

RDS:

- Multiple AZ for disaster recovery
- Replica for performance

NOSQL :

- Collection ==Table
- Document == each row
- Key – value pairs = columns which could be nested (fields)



Fieldes can be nested or flat
The columns can be varied == each record can have different number of fields
NOSQL :

- DynamoDB is the amazon solution

Online Transaction Processing VS Online Analytics Processing

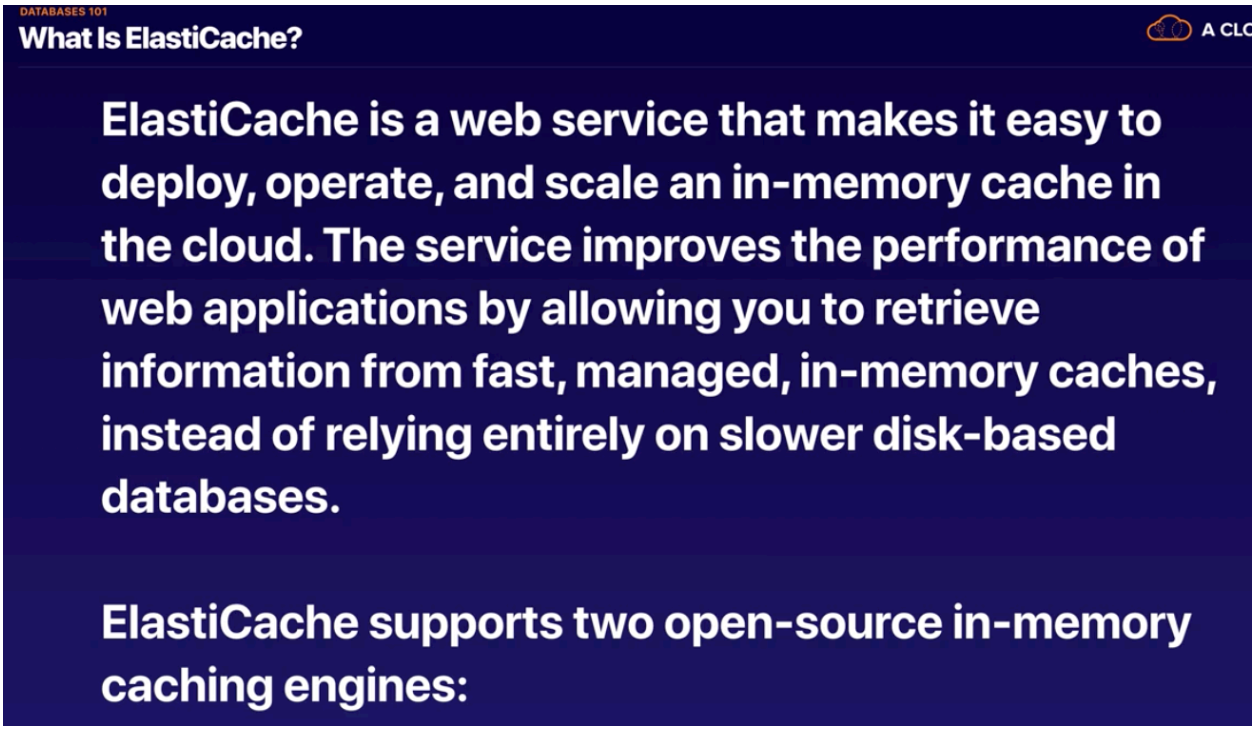
- Looking at each transaction vs analyzing the revenue , profit , business insight

For the purpose of Online Analytics since a massive load can hit the databases , datawarehouse solution comes to play . Creating different copy of different databases (no always allthe tables) in different servers for different purposes , so for instance the online analytics does not affect the production or customer services

Amazin Data Warehouse solution is

- Redshift

ElasticCache



So imagine a scenario where in each second we have many people using amazon for shopping. Amazon always wants to suggest the popular products in each department; kitchen , bay, hardware . So, this is the most common queries for those department which is pulled and held in your elasticcache and uncommon queries goes to databases . So basically there is a copy of data related to popular ones always in elasticcache and for those products it hits the elastic cache for anything other than this it goes to databases.
Elastic Cache /:

- Memcahched
- Redis

Tips :

RDS:

- SQL
- MySQL
- PostgreSQL
- Oracle
- Aurora
- MariaDB

DynamoDB: solution for no sql
Red Shift OLAP: solution for Data Warehouse

- Having different databases for different purposes to take off the unnecessary load from the primary one and each will be serving for some different purposes (if the business wants to run the heavy analytical queries they need to query redshift)

ElasticCache :

- In memory caching soluton in the clouse and it takes off some heavy loads from your production servers
- Memcahched
- Redis

Business intelligence go for data warehouse solution or redshift
Elastic speed up performance of existing databases for frequent identical queries

LAB (not tested in the exam)

- Provisioning an RDS instance
- Open My SQL port to the WEB_DMZ SG
    - Let our instance to talk (receive) request from our web server (the one has WEB_DMZ SG (security group))
- Create a we bserver (ec2 instance)
- Install wordpress using boot strap scripting
- Register the EC2 to the target group
- Upload the DNS (loadbalancer) named ALB
- Take a snapshot

Important note :
After creating our instance in RDS (under Databases) we have to open up the port to web server sg

- Open the database , under connecertivity and security , click on security ,
- We can see also the end point to the database
- Under the sg , we have to open ports for it
- We can add mysql and auro port 3306 and the source gonna be any instance with sg webDMZ

Boot strap script

```
#!/bin/bash
yum install httpd php php-mysql -y
amazon-linux-extras install -y php7.2
cd /var/www/html
wget https://wordpress.org/wordpress-5.4.1.tar.gz
tar -xzf wordpress-5.4.1.tar.gz
cp -r wordpress/* /var/www/html/
rm -rf wordpress
rm -rf wordpress-5.4.1.tar.gz
chmod -R 755 wp-content
chown -R apache:apache wp-content
service httpd start
chkconfig httpd on
```

we can have sql servers on our local ec2 but it wont be replicated unless we replicate the ec2 as well

we can take an image from our instance and then replicate it
AMI : Amazon Machine Image
So
In ec2 , we can take an image from our machine and then terminated it
In autoscaling

- Launch configuration
    - Using the AMI instead of booting a machine with bott starp or manually
    - So in the configure details we can just put yum update -y to make sure the machine update itself immediately after it launches
- Auto scaling group
    - Select the name
    - Select the config name (from previous step)
    - Add all the availability zone
        - It knows if an instance is initiated somewhere the next one should be in another availability zone
        - When we create the auto scaling , we attach it to our target group in load balancer

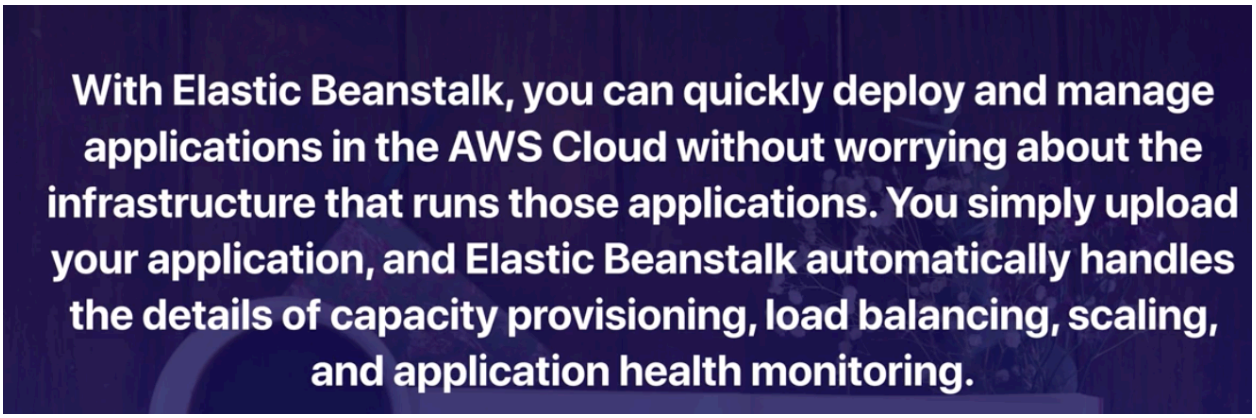
How we can buy a domain ?
DNS : Domain Name system , amp a name to the IP address

- Using Amazon route 53 , amazon DNS service
- For that make sure the s3 bucket with that name you need to created and that s3 bucket shouldn't have been taken !
-

Elastic Beanstalk

So we create instance with all boost starp script , security group , load balancer , target …
It will do that all by one click.

Deploying your application on the cloud and we don’t need to set up instance and install php or anything else depending on our application on it. It takes care of it all by itself.

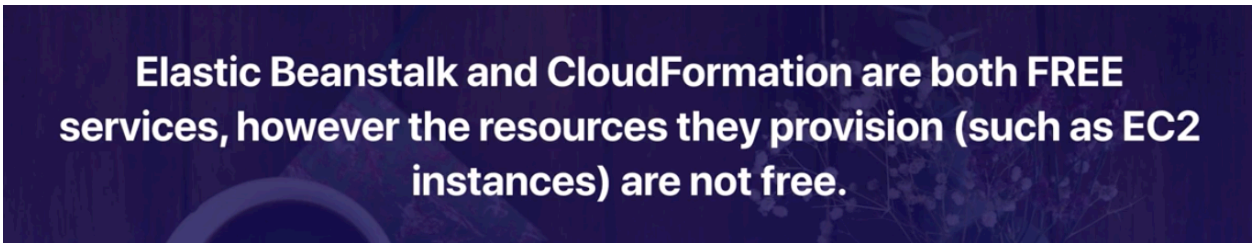


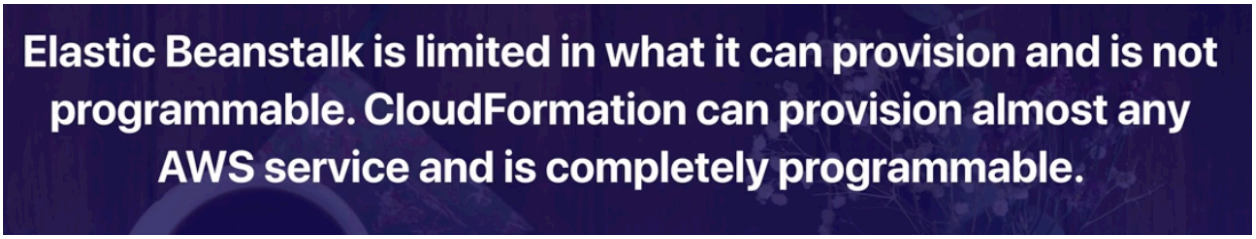
CloudFromation :

Under Management and governance in console
It contains stacks maybe

- An ec2 instance
- As well as RDS
- Secutity groups
- Lambda
- Etc .
-
- It has a stcak designer that design the stack for us all about the connectivity and different instances we need

-





Global AWS services

- IAM
- Route 53 : register domain name
- Cloud front : setting up a cloud front CDN is a global service
- roles
- SNS & SES

Some services gives global views but they are regional

- S3 : they are physically located somewhere but they have a global view

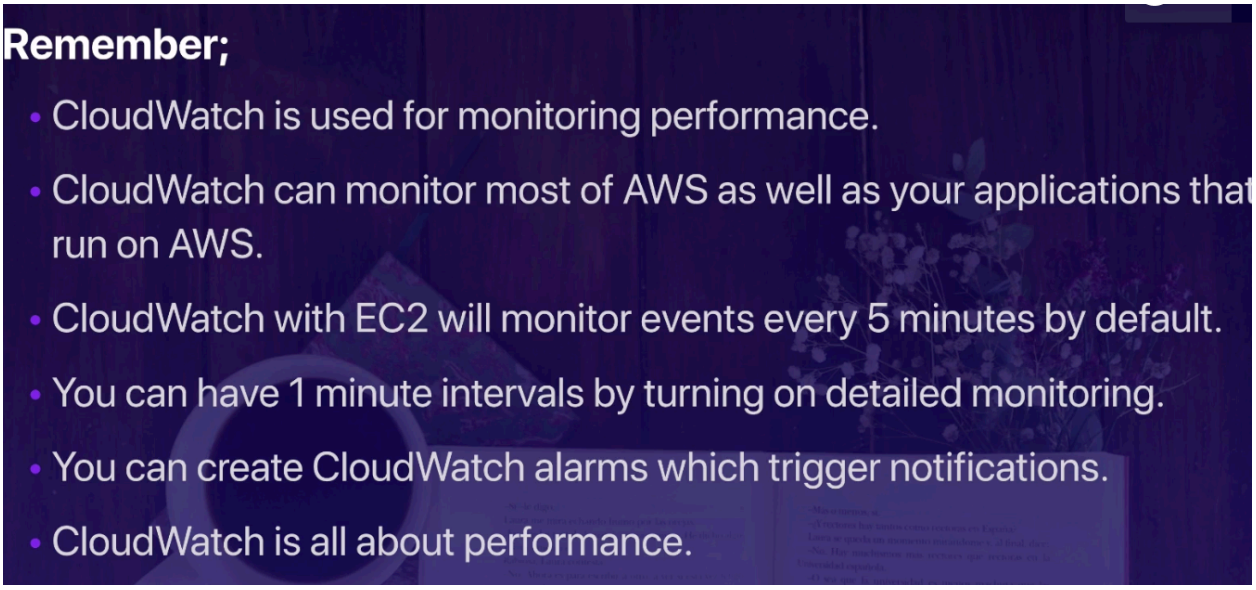
What services can be used on Premise ?

- Snowball : gigantic disk and they are shipped to your co , you upload everything there and send it back and amazon load it to s3

- Snowbell edge : using lambda faction on your premise ,
    - When you don’t have aws connectivity , somewher in antarctica
    -
- Storage Gateway :
    - Stays on premise all time it could be storage or ec2 or can be virtual
    - Caching your files in your data center and replicate them in s3
    - If you were to loose internet connection your data still is available
- Code deploy
    - You can deploy code in your aws or on premise
- Opsworks
    - Is for deployment and automating your application code
- IoT Greengrass

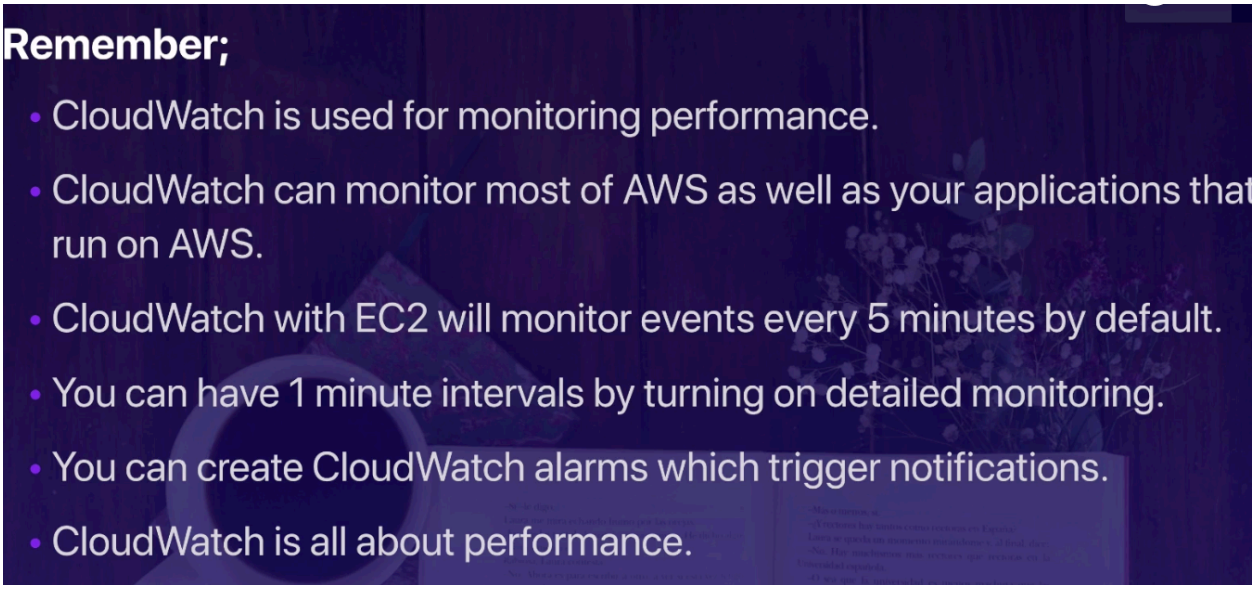
Cloud watch :

- Monitoring services to monitor resources and your application
- Compute
    - EC2 instances
    - Autoscaling load balancer
    - Route 53 heath check
- Storage and conetent delivery
    - EBS volume
    - Storage gateway
    - Cloud Front
- Hose Level metrics
    - CPU
    - Network
    - Disk
    - Status Check
    - We can create costume metrics



AWS System manager :

- Allows you to manage your EC2 instances at scale
- What if instead of two instance we have a fleet of ec2 and we want to update them all by Yum update -y or shh into eachj of them and odeing something them
- What we can do is when we deploy our instances , we install a software on it that it connects the instance to AWS system manager
- AWS system manager can run commands and it would be deployed on every instance
-



Service Health Dashboard :

- Checking the health of each services in each region
- So it deos not talk about the services you are using , it s about all the services on AWS in each region
- Just google it
- Don’t confuse with personal health dashboard

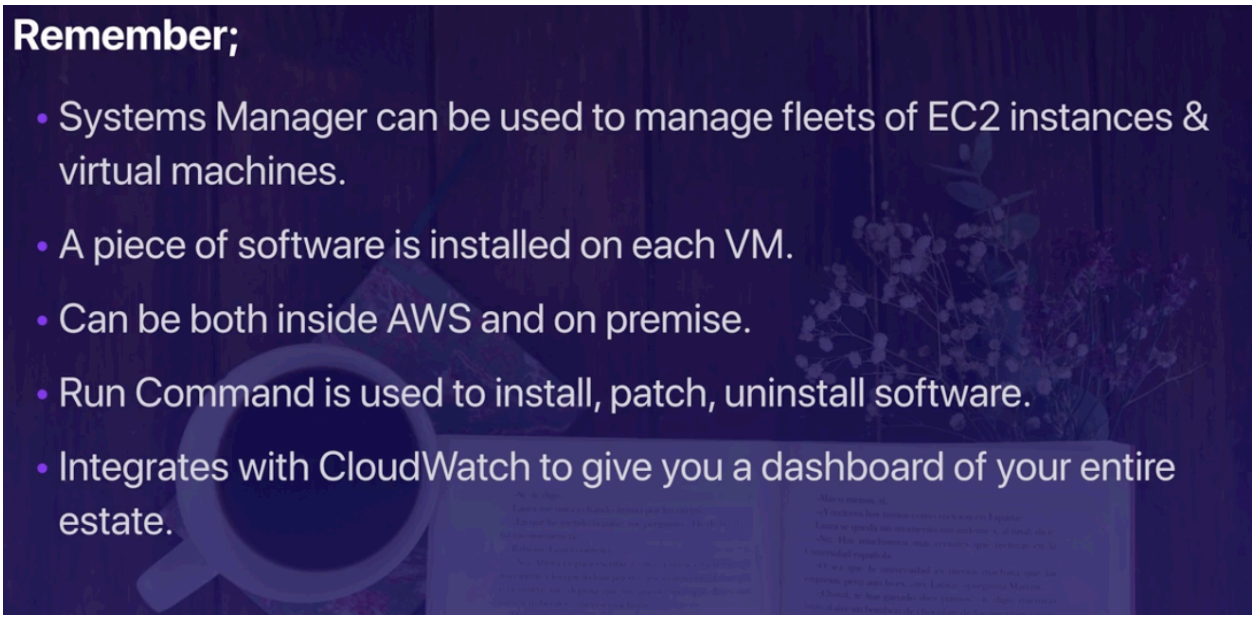
Personal Health dashboard :

- Which services I am using and what is the heath status of them
- Relevenat and up-to date info
- Provide prtoactive notification if any activity is scheduled
- You can make rules to notify you

S3 vs EBS vs EFS :

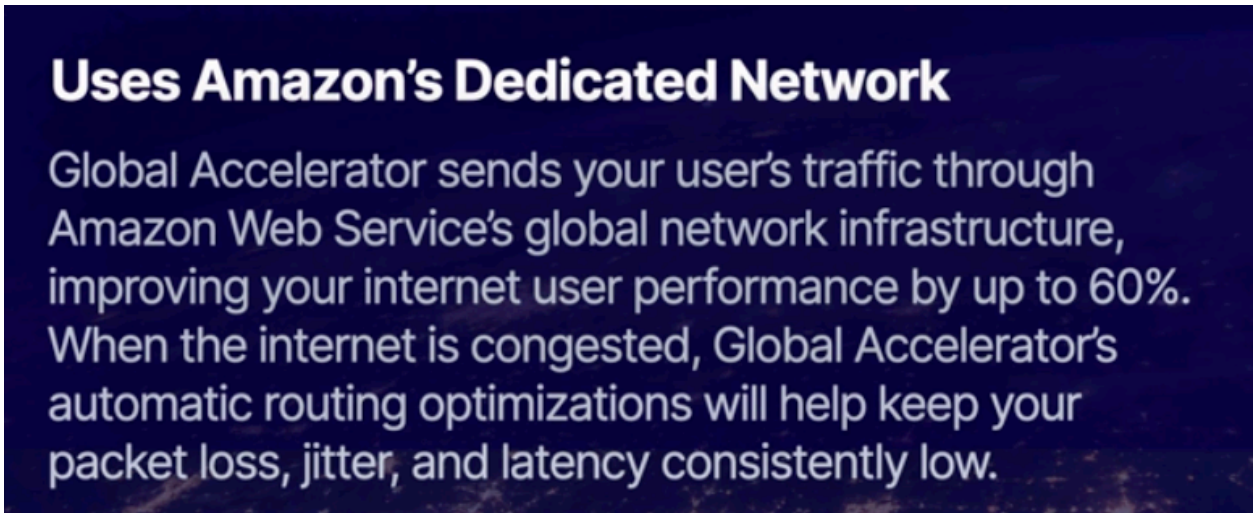
- S3 :
    - Secure , durable and highly scalable object storage and stored across multiple Az
- EBS :
    - Block Storage on the Cloud

    - Elastic Block Store (EBS)
    - Good for OS
    - The data can be saved there but hard to make it public
    - Still we get some replication and availability but in the same AZ
    - Can be attached to multiple instances
- EFS :
    - Elastic File System
    - It grows as the seize of data grow
    - Centralize file sysyrem , content management system , data bases (it is not recommeneded)
    - Can be attached to multiple instances
    - Differenec with EBS : EFS is elastic and the size is not fixed

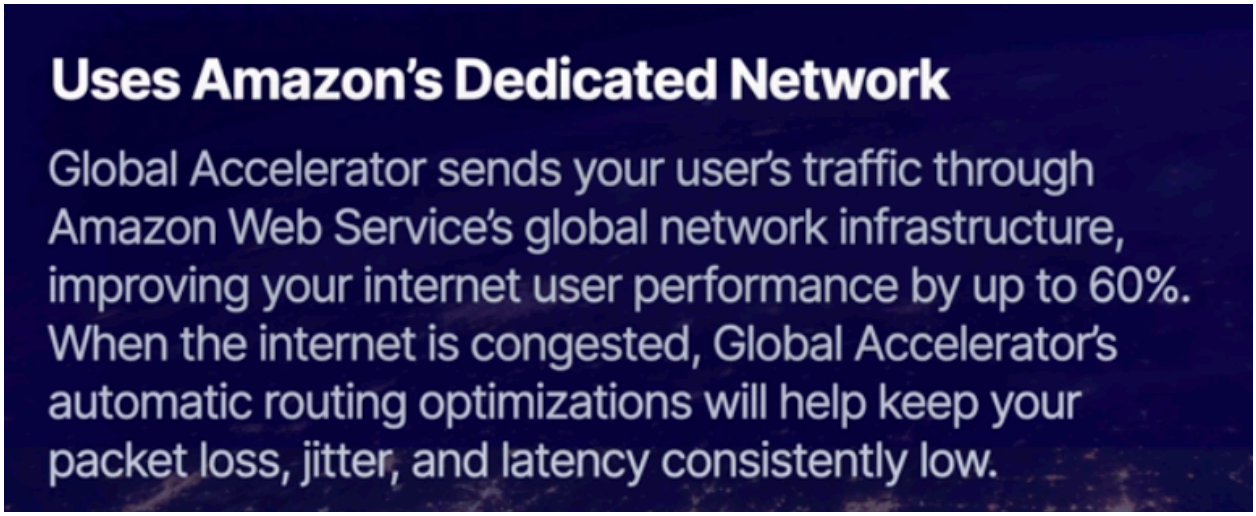


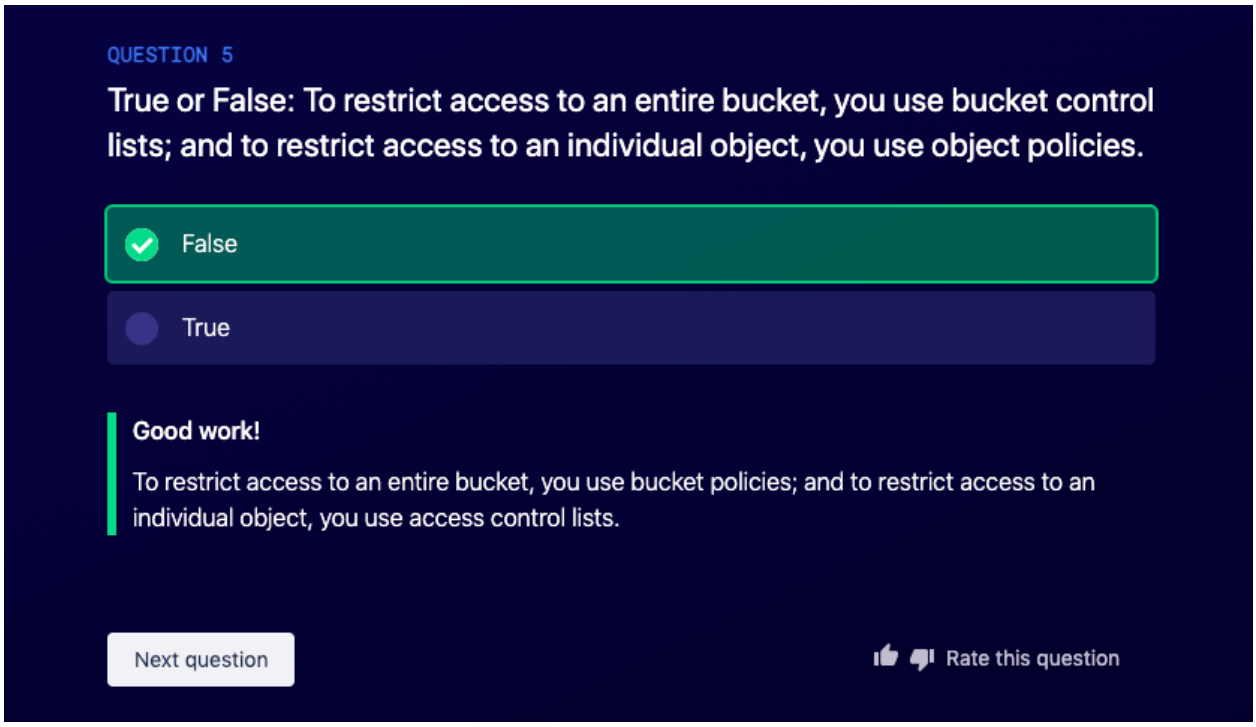
AWS Accelerator:

- Service that creates accelerators to improve the performance, scalability and availability of your applications



It uses the amazon network as backbone !





Amazon S3 access control lists (ACLs) enable you to manage access to buckets and objects. Each bucket and object has an ACL attached to it as a subresource. It defines which AWS accounts or groups are granted access and the type of access. When a request is received against a resource, Amazon S3 checks the corresponding ACL to verify that the requester has the necessary access permissions.

QUESTION 9

Which of the following Route 53 policies allow you to a) route data to a second resource if the first is unhealthy, and b) route data to resources that have better performance?

- ✓ Failover Routing and Latency-based Routing
- ✗ Geolocation Routing and Latency-based Routing
- Geoproximity Routing and Geolocation Routing
- Failover Routing and Simple Routing

Sorry!

Correct Answer

Failover Routing and Latency-based Routing are the only two correct options, as they consider routing data based on whether the resource is healthy or whether one set of resources is more performant than another. Any answer containing location based routing (Geoproximity and Geolocation) cannot be correct in this case, as these types only consider where the client or resources are located before routing the data. They do not take into account whether a resource is online or slow. Simple Routing can also be discounted as it does not take into account the state of the resources.

Next question

Rate this question

QUESTION 10

Amazon Lightsail is an example of which of the following?

- ✗ Software as a Service
- ✓ Platform as a Service
- Functions as a Service
- Infrastructure as a Service

Sorry!

Correct Answer

Lightsail is AWS' Platform-as-a-Service offering.

Next question

Rate this question

QUESTION 19

Which of the following are Support Levels offered by AWS?

Choose 3

- ✗ Start-up
- ✓ Developer
- ☐ Individual
- ✓ Basic
- ✓ Business

Sorry!

Correct Answer

The AWS Support levels are Basic, Developer, Business, and Enterprise.

Next question

Rate this question

QUESTION 22

Which of the following are characteristics of cloud computing?

Choose 3

- ✓ Services are delivered via the Internet.
- ✓ On-demand delivery
- ✓ Pay-as-you-go pricing
- ✗ Cloud charges are capital expenditures.

Sorry!

Correct Answer

Services incurred from a cloud services provider are operating expenses, not capital expenses. The other answers are correct.

Next question

Rate this question

QUESTION 24

True or False: Access Control Lists are used to make entire buckets (like one hosting an S3 website) public.

- ✗ True
- ✓ False

Sorry!

Correct Answer

Bucket Policies are used to make entire buckets (like one hosting an S3 website) public.

Next question

Rate this question

QUESTION 27

True or False: A Distribution is what we call a series of Edge Locations that make up CDN.

- ✓ True
- ✗ False

Sorry!

Correct Answer

The collection of a CDN's Edge Locations is called a Distribution.

Next question

Rate this question

QUESTION 28

Mark which statements are true regarding Lambda.

Choose 3

- [x] The resources section is the only required field in Lambda templates.
- [x] You can use JSON or YAML for Lambda templates.
- [x] Lambda can be used for Infrastructure as Code.
- [ ] Lambda functions have a timeout of 5 minutes.

Good work!

True. The resources section is the only required field in Lambda templates.
True. You can use JSON or YAML for Lambda templates.
True. Lambda can be used for Infrastructure as Code.

Next question

Rate this question

QUESTION 29

Which of the following are advantages of cloud computing?

Choose 4

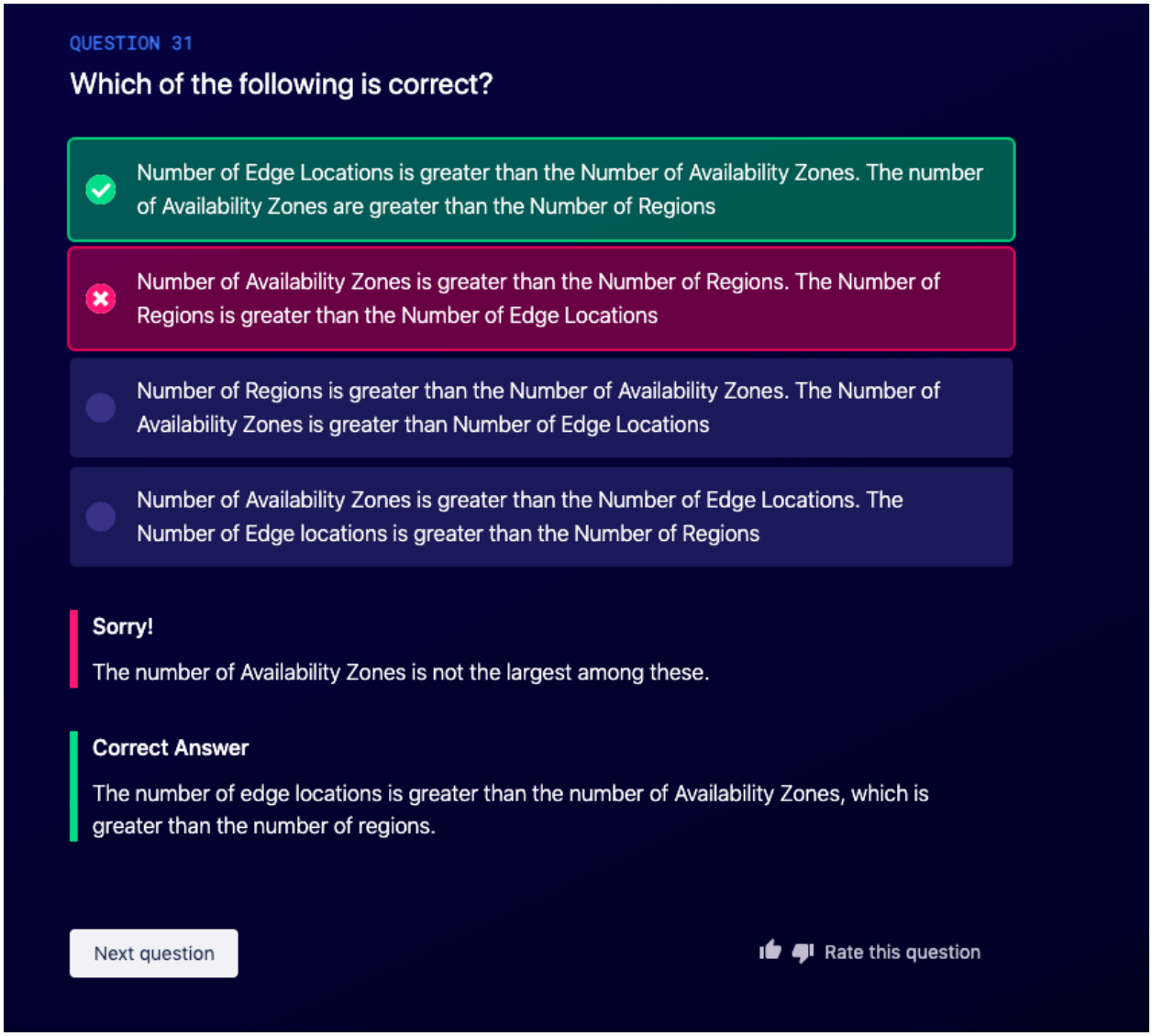
- [x] The ability to 'go global' in minutes
- [x] Increased speed and agility
- [x] Variable expense
- [x] Elasticity - you need not worry about capacity.
- [ ] The capital expenditure (CapEx) funding model

Good work!

The 'pay-as-you-go' nature of cloud computing ensures that a large up-front capital expense is not required.

Next question

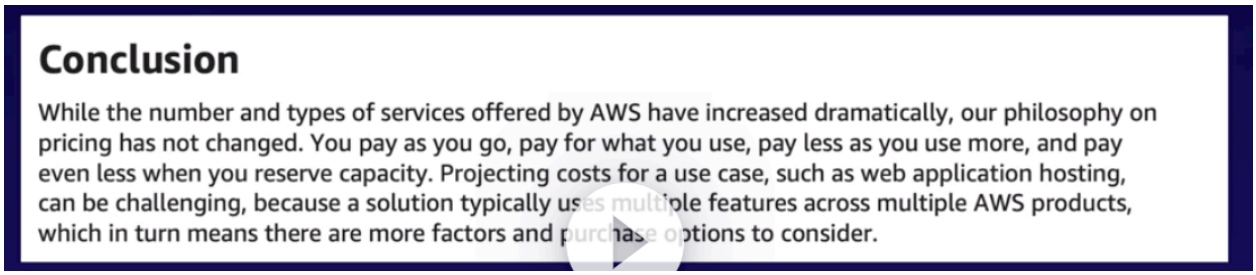
Rate this question



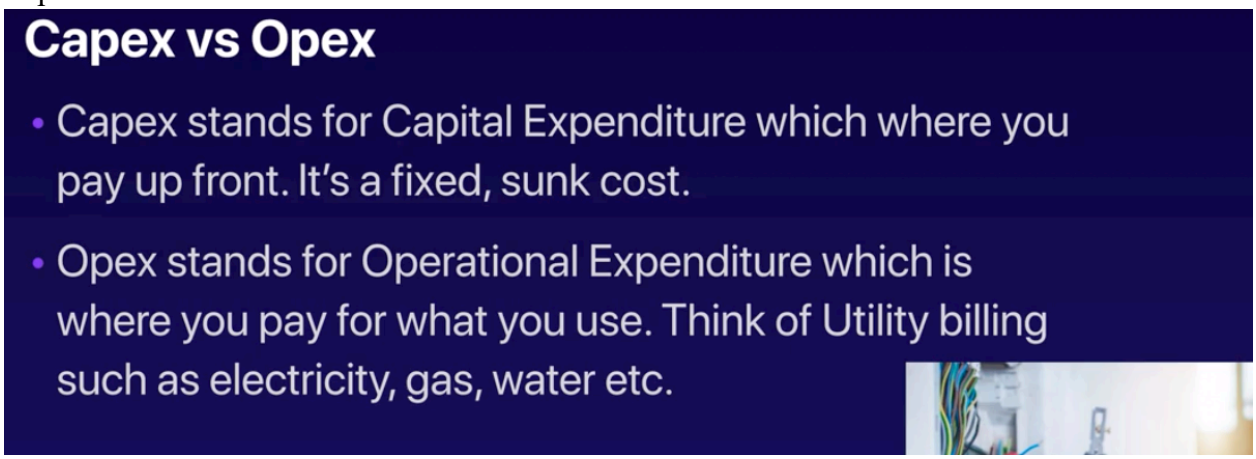
Pricing:

White paper is a must read .

https://d0.awsstatic.com/whitepapers/aws_pricing_overview.pdf



Capex vs OPex :



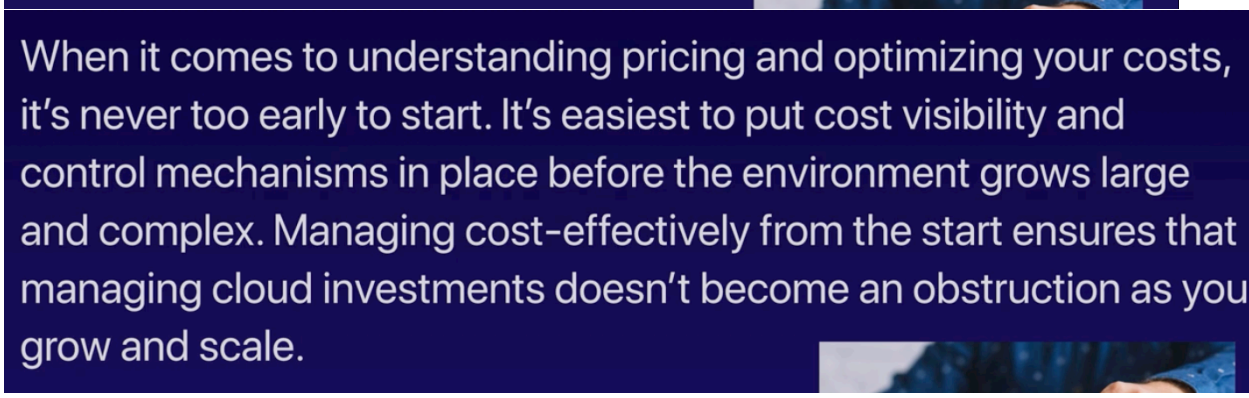
The basic pricing policies are as follows :

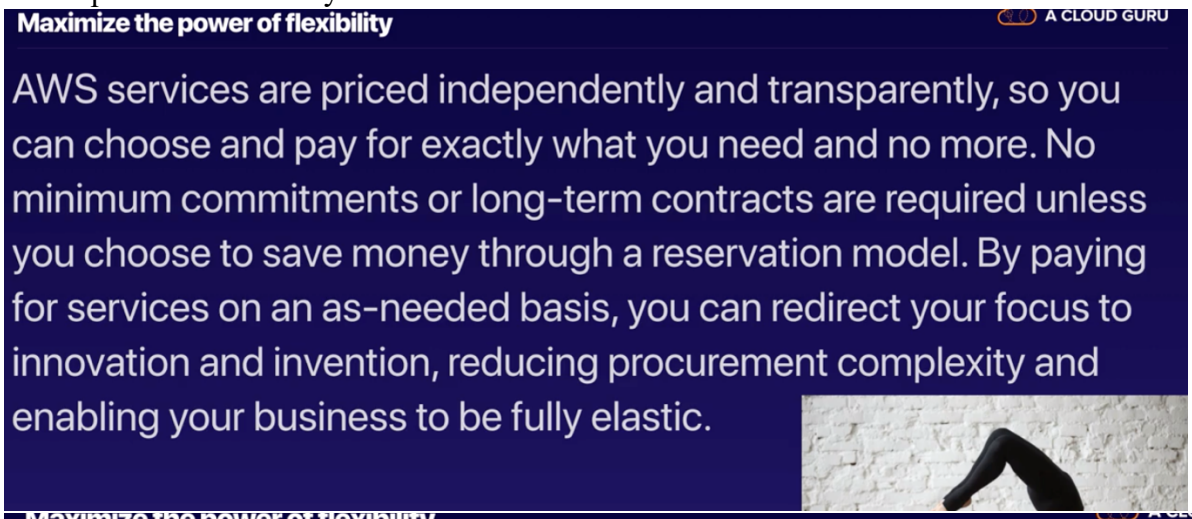
- Pay as you go
- Pay less when you reserve
- Pay even less per unit by using more services
- Pay even less as AWS grows

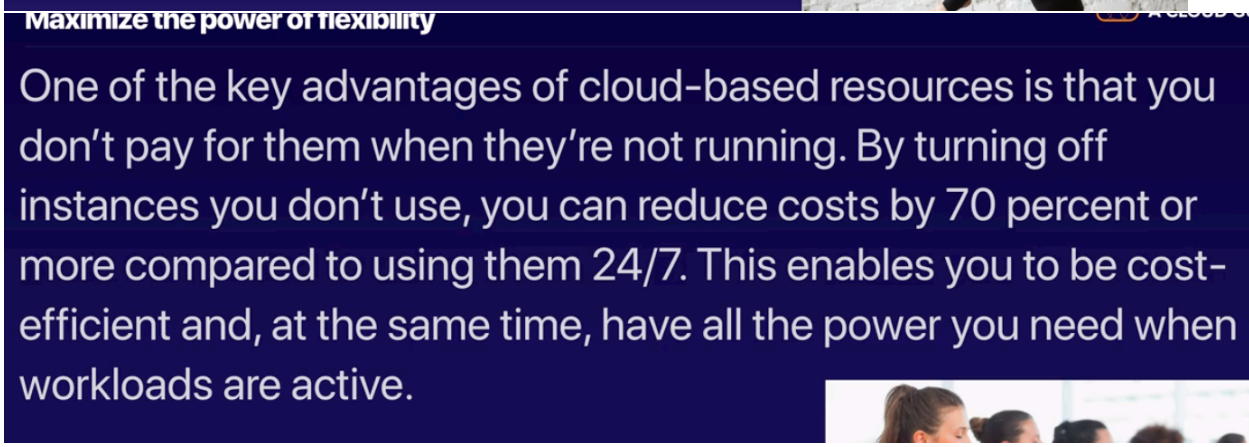
To the best practice of pricing:

- Understand the fundamental of pricing
  - Compute
  - Storage
  - Data Outbound: data leaving your aws env
- Start early with cost optimization
  -
  -

- 

- 

- Maximize the power of flexibility
  - 

  - 

- Use the right pricing principal model for the job
    - On demand / dedicated / spot / reservations; seems it is applicable to all instances not just EC2
    - **To help new AWS customers get started in the cloud, AWS offers a free usage tier. If you're a new AWS customer, you can run a free Amazon EC2 Micro Instance for a year while also leveraging a free usage tier for Amazon S3, Amazon Elastic Block Store, Amazon Elastic Load Balancing, AWS data transfer and other AWS services.**
    - 100 % free :
        - AMAZON VPC: virtual data center in the cloud
            - That s where the little virtual machines live
            - Amazon VPC is the networking layer for Amazon EC2
            - Amazon Virtual Private Cloud (Amazon VPC) enables you to launch AWS resources into a virtual network that you've defined. This virtual network closely resembles a traditional network that you'd operate in your own data center, with the benefits of using the scalable infrastructure of AWS.
        - Elastic Beanstalk:
            - If you don't know about the aws architecture, you don't need to be worry about the infrastructure just submit your application and it takes care of instances needed itself.
        - Cloud formation
            - If you are aware of the architecture, model it schematically and it creates everything for you
        - IAM
        - Auto Scaling
        - OPSworks
            - ???
        - Consolidating billing
    - What determines price?
        - Clock hours of instance
        - Instance type
        - Pricing model
            - Spot. /reserved/ etc.
        - Number of instances
        - Load balancing
            - Network load balancing vs instance load balancing
        - Detailed monitoring
        - Auto Scaling
        - ELASTIC IP Address
        - Operating systems and software packages
            - Windows is slightly more expensive than Linux
    - EC2 pricing model

        - On demand
        - RESERVED
            - The more you pay upfront or longer contract the more discount
        - Spot
        - Dedicated

Lambda Pricing:

- Serverless
- It is like s3
- You pay for the execution time
- Request Pricing:
    - Free tier: 1 million free request per month
    - 20 cents per million request there after
- Duration pricing :

400 1865868

    - ,000GB second per month free up to 3.2 million seconds of compute time
    - 0.000016 for every gb-second used ther after
- Additionla charges :
    - If lambda uses the other instances
    - Or transfer data : read / write data to s3 for instance

EBS pricing :

- Elastic Block Storage
- Volumme (per GB)
- Snapshots (GB)
- Data transfers

S3 pricing :

- Standarad/ IA , 1 ZA IA etc
- Storage
- Request (get ., put , copy)
- Data Transfer

Glaciers pricing

- Storage
- Data retrieval time (the longer retrieval time th eles price)

Snowball :

- A large PB-Scale data transport solution usues to securely transfer data in and out of the cloud
- Gigantic disk
- Service fee per job
    - 50 tb
    - 80 tb
- Daily charge
    - First 10 days is free after that 15 per day
- Data transfer in to s3 is free. But out is not .
    - They want to encourage you to stay on AWS .

RDS PRICING

- CLOCK HOURS OF server run: how many hours it runs
- Data Base Characteristics :
    - Sql , my sql , aurora
- DataBase purchase type
    - How large
- The number of database instances
- Provision storage
    - How big data bases are
- Additional instances
- Request
- Deployment type
- Data transfers

No sql (Dynamo Db) pricing :

- Provisioned through put write
- Provisioned through put read
- Data storage

Cloud Front : (CDN for AWS)

- Traffic distribution
- # of requests
- Data transfer out

Conclusion

While the number and types of services offered by AWS have increased dramatically, our philosophy on pricing has not changed. You pay as you go, pay for what you use, pay less as you use more, and pay even less when you reserve capacity. Projecting costs for a use case, such as web application hosting, can be challenging, because a solution typically uses multiple features across multiple AWS products, which in turn means there are more factors and purchase options to consider.

Tips :

Exam Tips

Capex vs Opex

- Capex stands for Capital Expenditure which where you pay up front. It's a fixed, sunk cost.
- Opex stands for Operational Expenditure which is where you pay for what you use. Think of Utility billing such as electricity, gas, water etc.

1

On Demand

Allows you to pay a fixed rate by the hour (or by the second) with no commitment.

2

Reserved

Provides you with a capacity reservation, and offer a significant discount on the hourly charge for an instance. Contract Terms are 1 Year or 3 Year Terms.

3

Spot

Enables you to bid whatever price you want for instance capacity, providing for even greater savings if your applications have flexible start and end times.

4

Dedicated Hosts

Physical EC2 server dedicated for your use. Dedicated Hosts can help you reduce costs by allowing you to use your existing server-bound software licenses.

Serveless service :

- S3
- Lambda

Different support level plan :

- basic
- Developer
- Business
- Enterprise

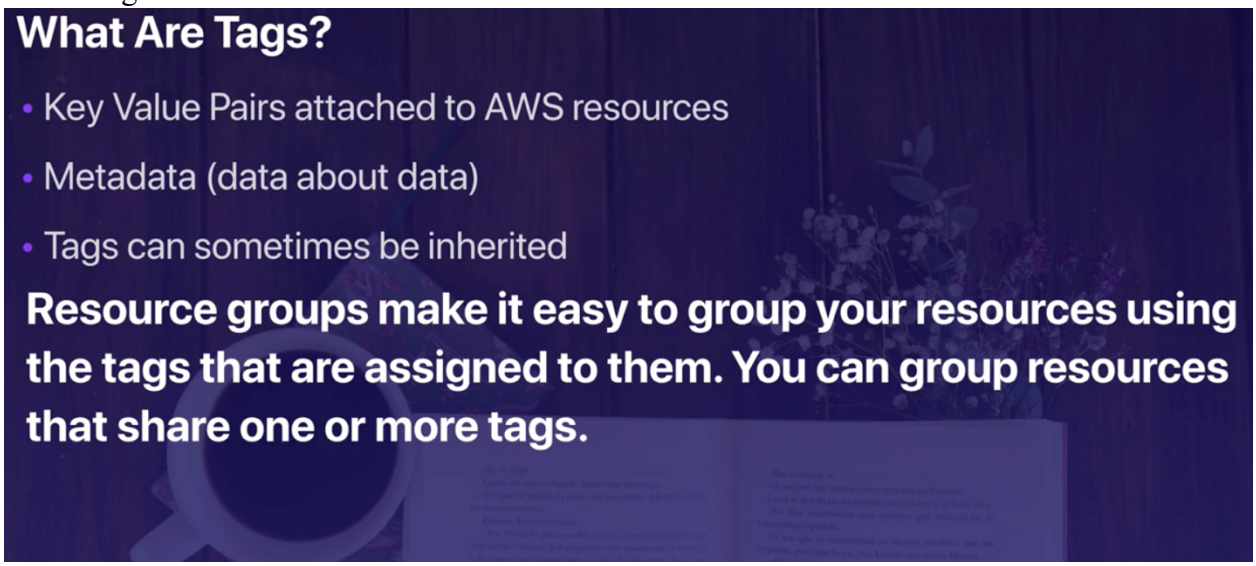
	BASIC	DEVELOPER	BUSINESS	ENTERPRISE
COST	FREE	$29 A MONTH	$100 A MONTH	$15,000 A MONTH
Tech Support		Business hour access via email	24 x 7, email, chat & phone	24 x 7, email, chat & phone
TAM	NO	NO	NO	YES
Who can open cases?	None	1 Person / Unlimited Cases	Unlimited Contacts/ Unlimited Cases	Unlimited Contacts/ Unlimited Cases

	BASIC	DEVELOPER	BUSINESS	ENTERPRISE
Case Severity / Response Times		General guidance: < 24 business hours System impaired: < 12 business hours	General guidance: < 24 hours System impaired: < 12 hours Production system impaired: < 4 hours Production system down: < 1 hour	General guidance: < 24 hours System impaired: < 12 hours Production system impaired: < 4 hours Production system down: < 1 hour Business-critical system down: < 15 minutes

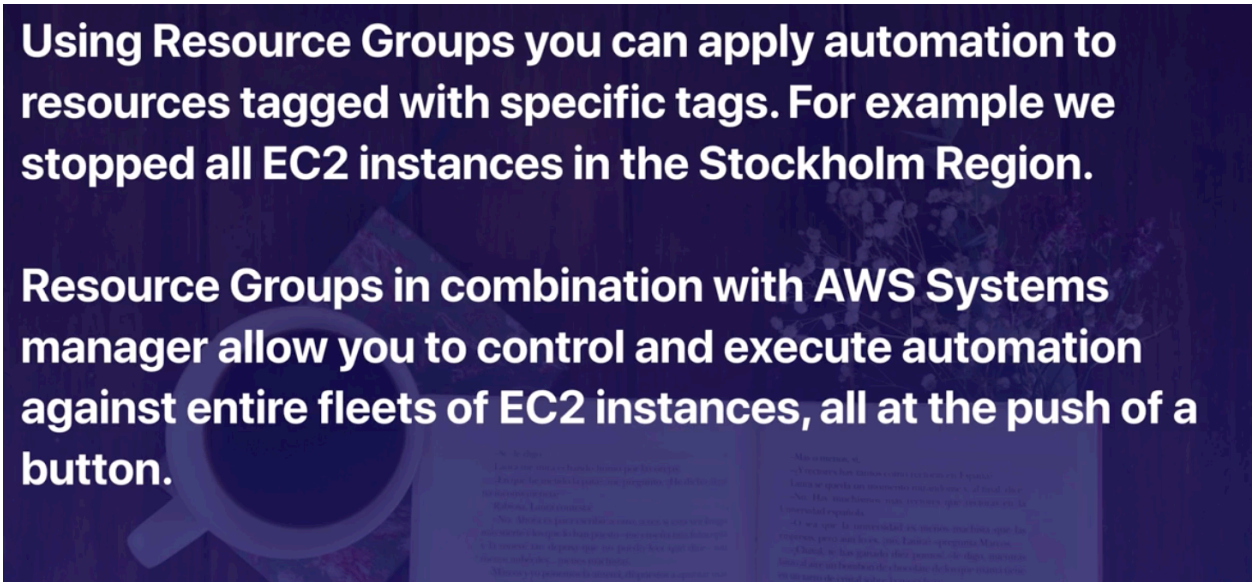
Resource groups and Tags :

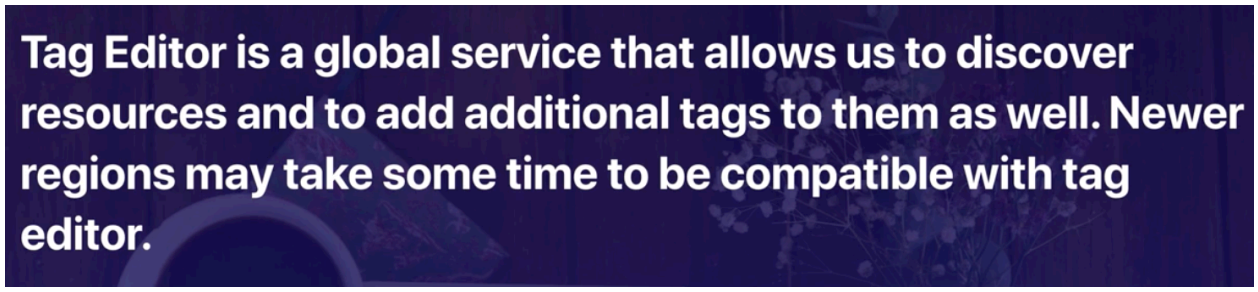
- Tag editor
  - It s a global service
  - So , in the find our instances based on their region , type of instances and the tag they have
  - For the tag they have it can be just a key or key – value
  - And then search and find all the instances and we can create new tags or modified the existing
  -
- Create a group
  - So it can query based on tag ; cerate query based group !

- It does that for just a region
- Again we can query them based on their tags
  - It can be either key
  - Or key-value
- We named them and we can create a group
- For instance, if we query all ec2 instances in N. Virginian and all the ones that have the department tag …
- Actually it goes through AWS system manger and it can run a command and execute through whole bunch of instances using that group we created using their tags



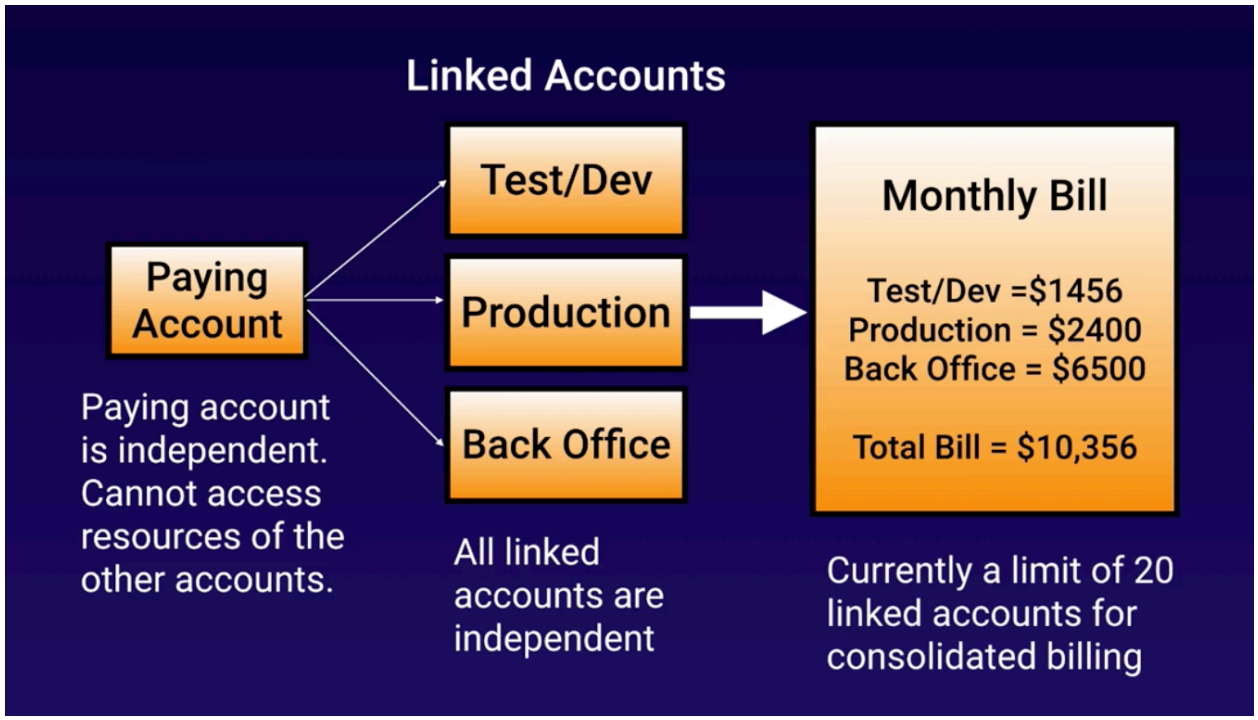
Tags can be inherited, for instance using cloud formation if you create an architecture using cloud formation whatever tags the formation is given it will be inherited by its instances.





AWS Organiztion :

- Is an account management service that enables you to consolidate multiple AWS accounts into an organization that you created and centrally manage?
- We can have multiple account for different organizations and each of them has it s own policy



Paying account is independent; it cannot create or turn off some instances from the other accounts.

What is cloud Trail ?
Cloud trail VS cloud watch :

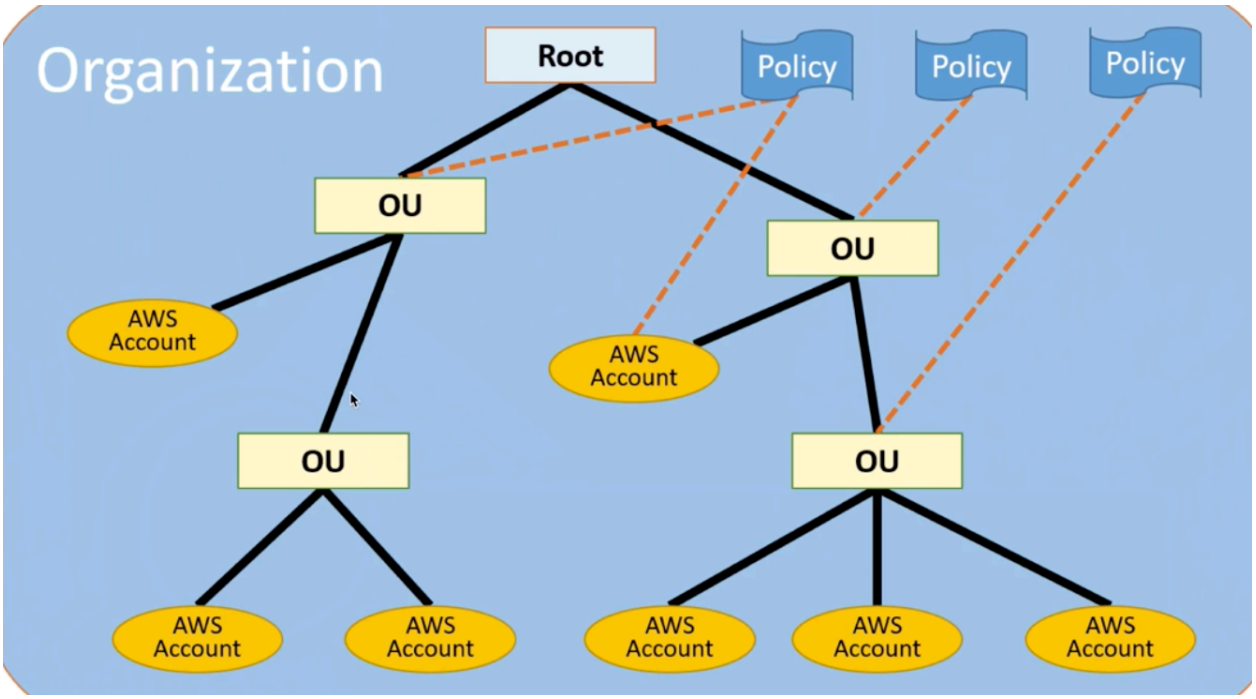
- Cloud watch is all about performance
    - Monitor the respurces and cpu and rams
- Cloud trail monitors API calls in AWS platforms; auditing tool .

Cloud Trail :

- PER AWS account and is enabled per region.
- Can consolidates logs using s3 bucket:
    - Turn cloud tarin in paying account
    - Create a bucket policy that allows a cross-account access
    - Turn on Cloud Trail in the other accounts and use the bucket in the paying account : so technically we turn it in the other accounts but saved the logs in the paying account !

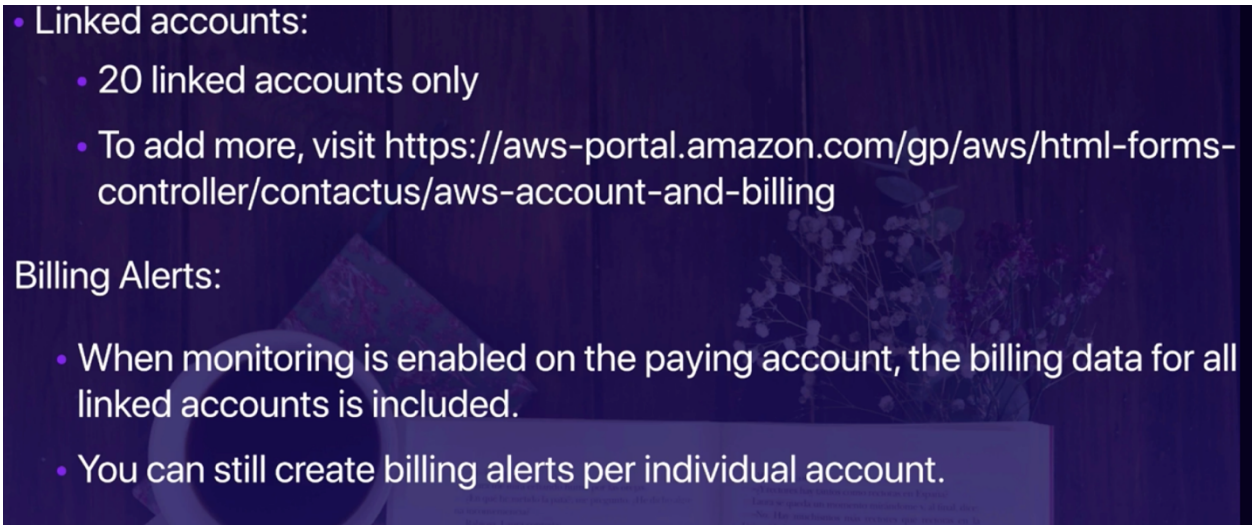
Tips:
AWS organization:

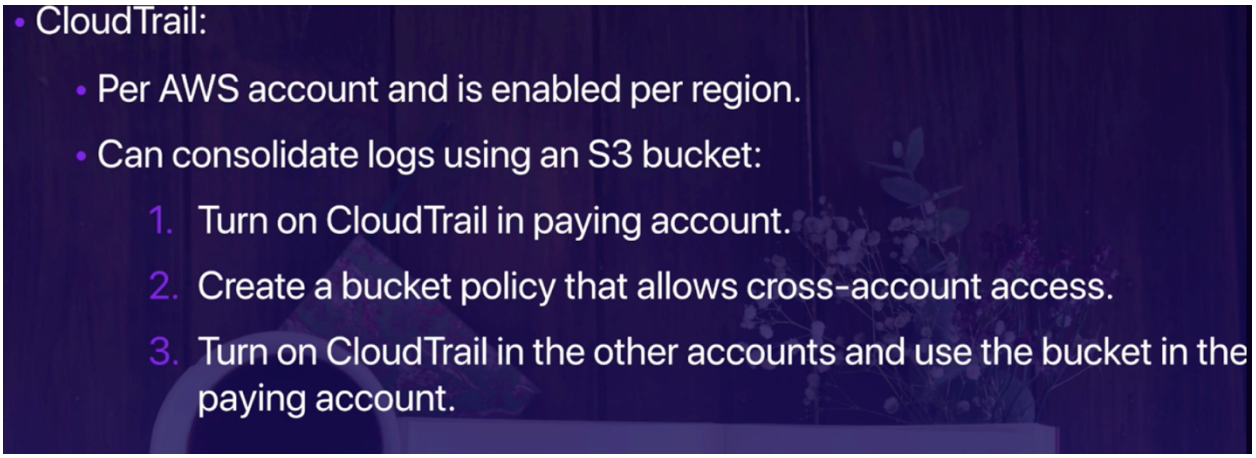
- Full access
- Billing

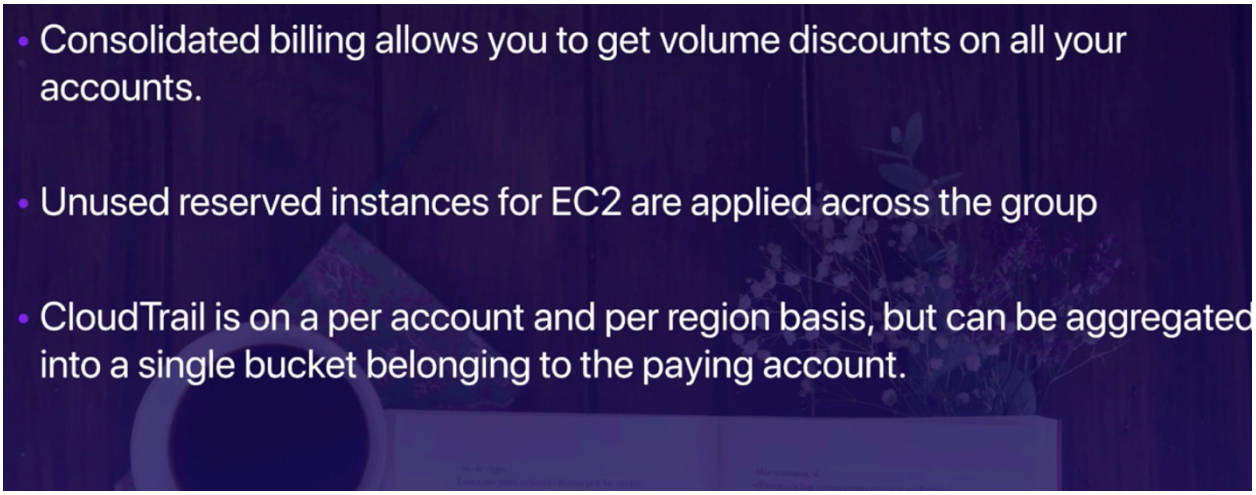


OU is full access (meaning that the root has access to do anything but it should not be used for deployment and instances provisions, etc) and each has an account behind it and policies could apply either to OU or AWS accounts.
On top of all them, there is a root that can be billing account

Billing monitoring (cloud watch) is for account
Cloud Trail: monitor APIs over the accounts







AWS organization :

- In console where your profile exists , click on my organization s
- It goes to gloabal as it s gloabla service

- Create a organization
- Verify the action by the email
- Then we can either invite the account or create accounts
- We can see there is no organizational unit at the beginning and we can create Organizational Units
- Apply policies to the organizational units
    - Allow to do something
    - Deny to do something
- Attach the account to each OU
- Apply the proper policy to each of which

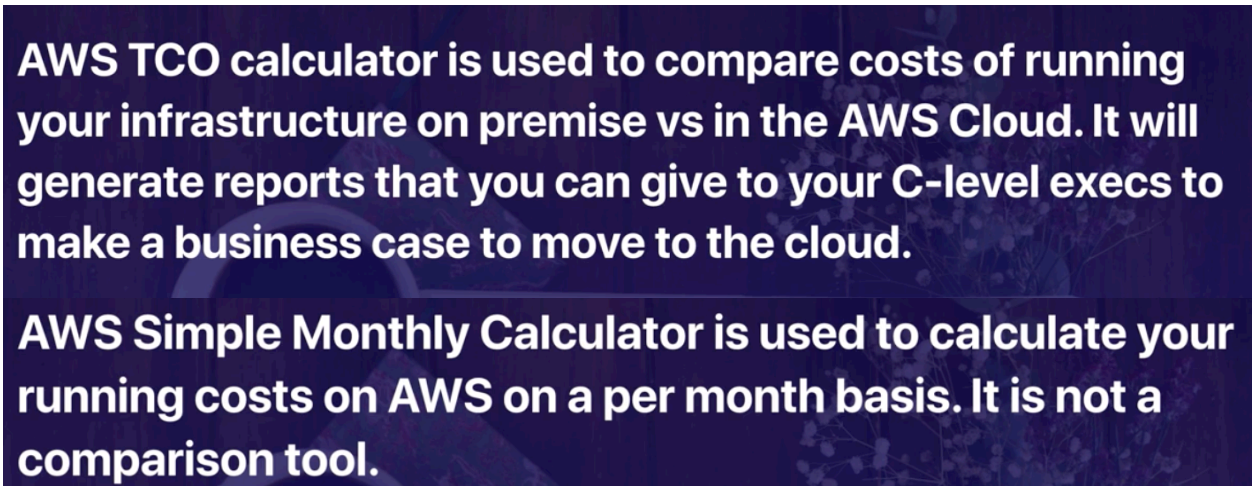
AWS quick start and AWS Landing zone

AWS Partner Network:
- Consulting
    - These partner design, architect, build, Migrate and manage customer workloads and application on AWS
- Technologies
    - Provides hardware, connectivity services, software solutions that are either hosted or integrated with the AWS cloud.

Partner	Practitioner Certs	Associate Certs	Professional/ Specialty Certs
Select	2	2	2
Advanced	4	4	6
Premier	10	10	10

Amazon Calculators :

- Aws helps you to calculate your coasts using a couple if different calculators
- Available in two different features :
    - Aws Simple monthly calculator
        - Located in S3 and it s static website
        - AWS Total cost of ownership Calculator



Summary :

https://d0.awsstatic.com/whitepapaers/

AWS organization:

- Full access
- Billing consolidation

Capex vs Opex

- Capex stands for Capital Expenditure which where you pay up front. It's a fixed, sunk cost.
- Opex stands for Operational Expenditure which is where you pay for what you use. Think of Utility billing such as electricity, gas, water etc.

1

On Demand

Allows you to pay a fixed rate by the hour (or by the second) with no commitment.

2

Reserved

Provides you with a capacity reservation, and offer a significant discount on the hourly charge for an instance. Contract Terms are 1 Year or 3 Year Terms.

3

Spot

Enables you to bid whatever price you want for instance capacity, providing for even greater savings if your applications have flexible start and end times.

4

Dedicated Hosts

Physical EC2 server dedicated for your use. Dedicated Hosts can help you reduce costs by allowing you to use your existing server-bound software licenses.

Remember The Free Services

- Amazon VPC
- Elastic Beanstalk
- CloudFormation
- Identity Access Management (IAM)
- Auto Scaling
- Opsworks
- Consolidated Billing

Remember the difference between Budgets & Cost Explorer

- Budgets is used to budget (or predict) costs **BEFORE** they are incurred.
- Cost Explorer is used to explore costs **AFTER** they have been incurred.

	BASIC	DEVELOPER	BUSINESS	ENTERPRISE
COST	FREE	$29 A MONTH	$100 A MONTH	$15,000 A MONTH
Tech Support		Business hour access via email	24 x 7, email, chat & phone	24 x 7, email, chat & phone
TAM	NO	NO	NO	YES
Who can open cases?	None	1 Person / Unlimited Cases	Unlimited Contacts/ Unlimited Cases	Unlimited Contacts/ Unlimited Cases

	BASIC	DEVELOPER	BUSINESS	ENTERPRISE
Case Severity / Response Times		General guidance: < 24 business hours System impaired: < 12 business hours	General guidance: < 24 hours System impaired: < 12 hours Production system impaired: < 4 hours Production system down: < 1 hour	General guidance: < 24 hours System impaired: < 12 hours Production system impaired: < 4 hours Production system down: < 1 hour Business-critical system down: < 15 minutes

What Are Tags?

- Key Value Pairs attached to AWS resources
- Metadata (data about data)
- Tags can sometimes be inherited

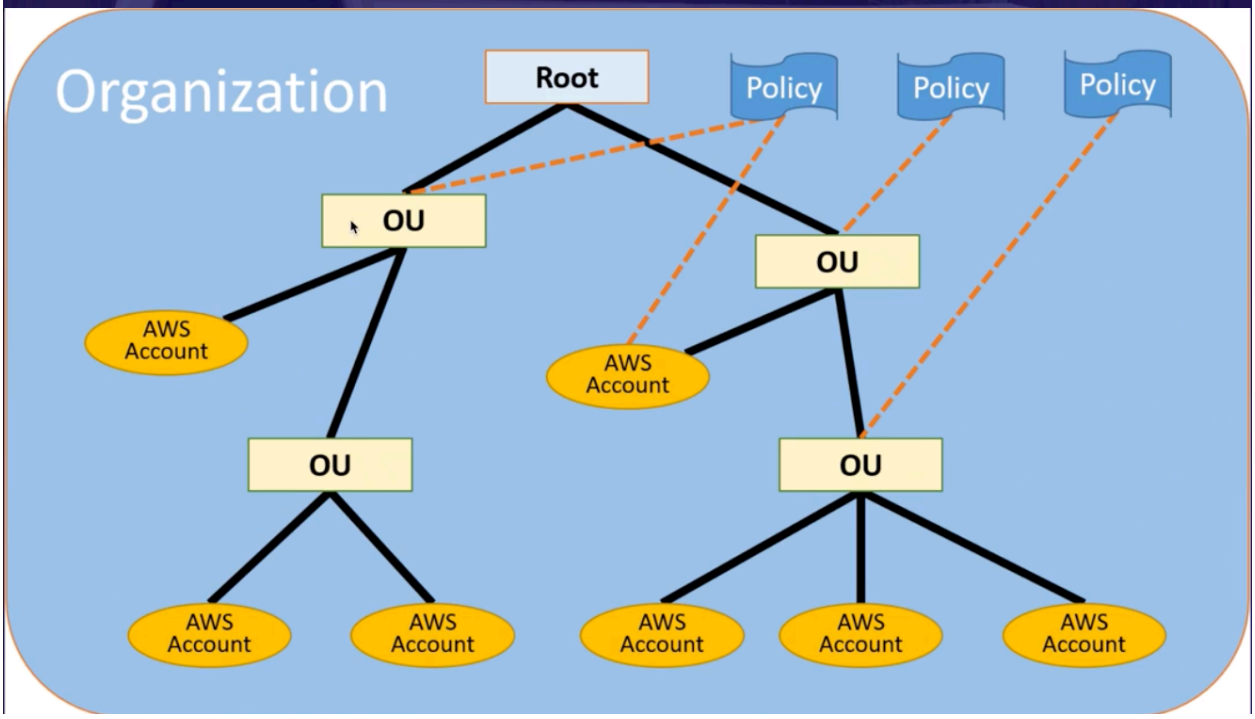
Resource groups make it easy to group your resources using the tags that are assigned to them. You can group resources that share one or more tags.

- Region
- Name
- Health Checks

Using Resource Groups you can apply automation to resources tagged with specific tags. For example we stopped all EC2 instances in the Stockholm Region.

Resource Groups in combination with AWS Systems manager allow you to control and execute automation against entire fleets of EC2 instances, all at the push of a button.

Tag Editor is a global service that allows us to discover resources and to add additional tags to them as well. Newer regions may take some time to be compatible with tag editor.



- Linked accounts:
  - 20 linked accounts only
  - To add more, visit https://aws-portal.amazon.com/gp/aws/html-forms-controller/contactus/aws-account-and-billing
- Billing Alerts:
  - When monitoring is enabled on the paying account, the billing data for all linked accounts is included.
  - You can still create billing alerts per individual account.

- Consolidated billing allows you to get volume discounts on all your accounts.
- Unused reserved instances for EC2 are applied across the group
- CloudTrail is on a per account and per region basis, but can be aggregated into a single bucket belonging to the paying account.

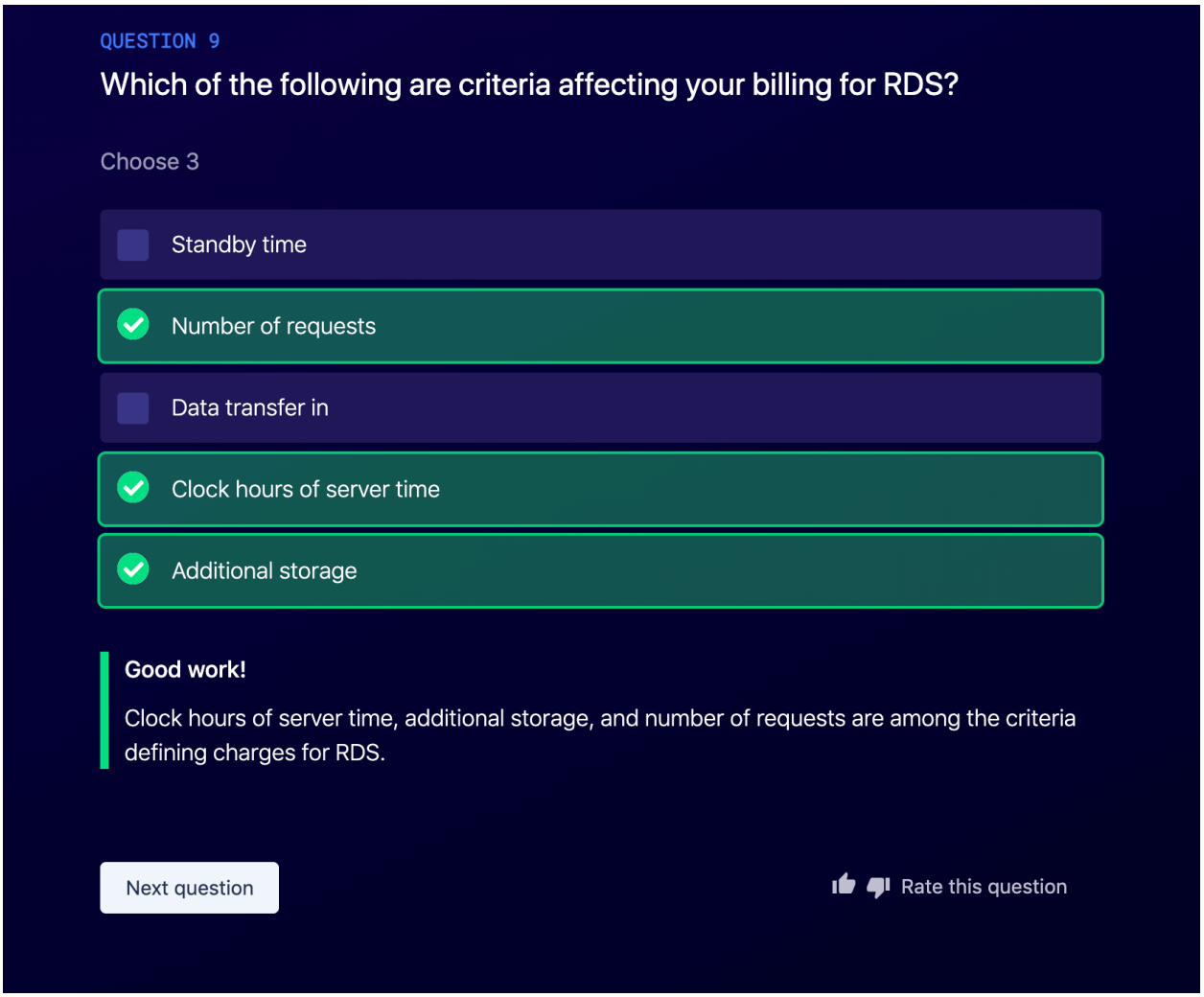
- CloudTrail:
  - Per AWS account and is enabled per region.
  - Can consolidate logs using an S3 bucket:
    1. Turn on CloudTrail in paying account.
    2. Create a bucket policy that allows cross-account access.
    3. Turn on CloudTrail in the other accounts and use the bucket in the paying account.

AWS Quick Start is a way of deploying environments quickly, using CloudFormation templates built by AWS Solutions Architects who are experts in that particular technology.

AWS Landing Zone is a solution that helps customers more quickly set up a secure, multi-account AWS environment based on AWS best practices.

AWS Simple Monthly Calculator is used to calculate your running costs on AWS on a per month basis. It is not a comparison tool.

AWS TCO calculator is used to compare costs of running your infrastructure on premise vs in the AWS Cloud. It will generate reports that you can give to your C-level execs to make a business case to move to the cloud.



Security & Complinace :

How do you know it saved to store your credit card, heath record, etc in AWS ?

AWS shared Responsibility Model:

- AWS is responsible for something ; like datacenter , facilities , RDS , S3
    - RDS and S3 would be AWS responsibility since you don't have access to their Operating systems
- You are responsible for EC2 security
    - Security patch
    - Data into and out from EC2
    -

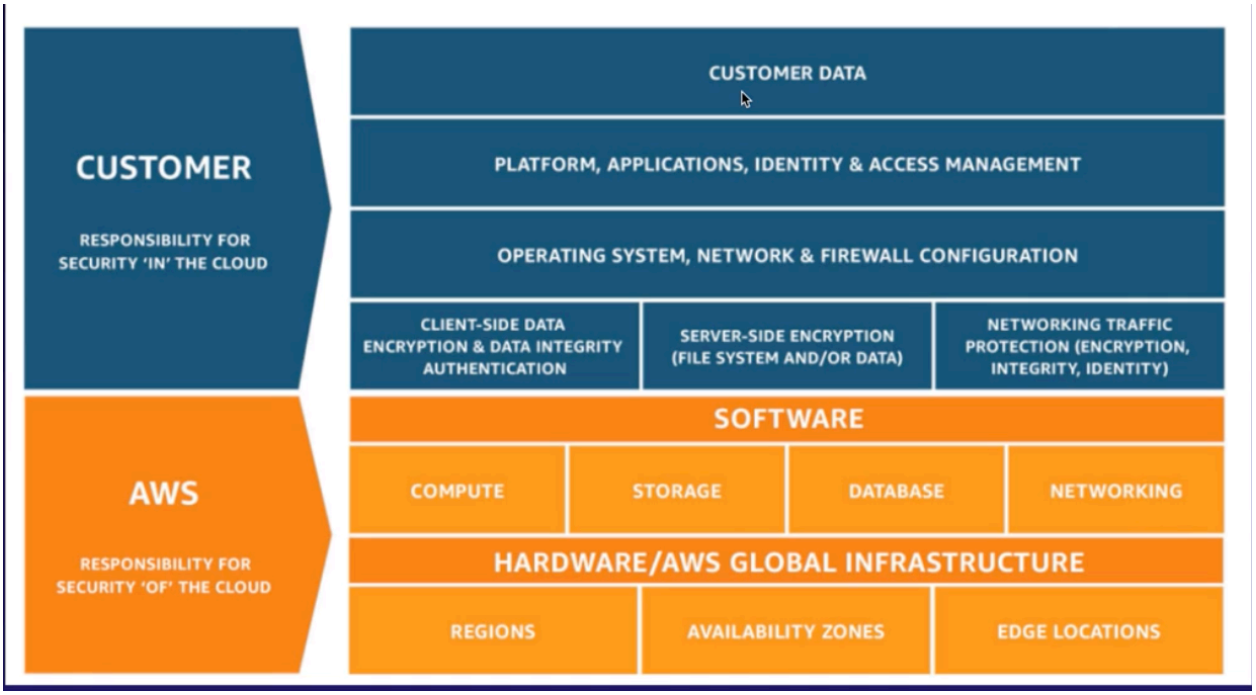
or abstracted services, such as Amazon S3 and Amazon DynamoDB, AWS operates the infrastructure layer, the operating system, and platforms, and customers access the endpoints to store and retrieve data

AWS responsibility is security of the cloud
Users responsibility is security in the cloud

Encryption is a shared responsibility:

- You need to use http
- You need to encrypte the data into the cloud
- You need to turn encryption on and aws will encrypt the martial for you and save it in s3 .

While AWS manages security of the cloud, security in the cloud is the responsibility of the customer. Customers retain control of what security they choose to implement to protect their own content, platform, applications, systems and networks, no differently than they would in an on-site datacenter.



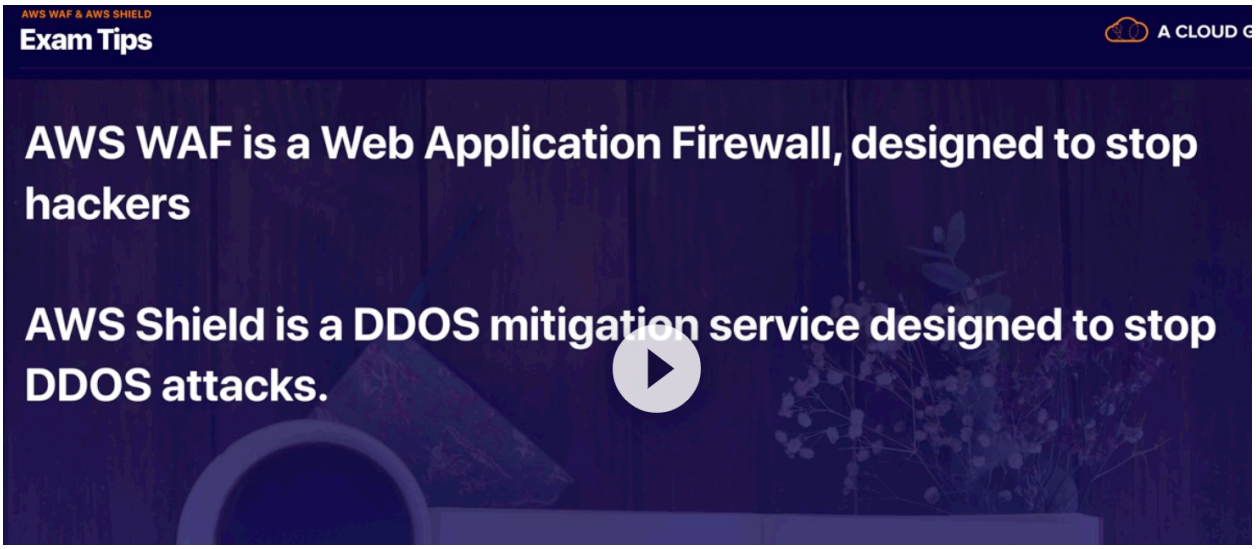
AWS WAF & AWS shield
WAF : Web Application Firewall (layer 7firewall)

- Helps you protect your web app from common web exploits that could affect application availaibility , compromise security or consume excessive resources
- Seven layer security from the hardware phisycal layer all the way up to app layer
- Inspect the web traffic

What s AWS shield ?

- Is a managed Distributed Denial of Service (DDoS) protection service safeguard web application running on aws.
- How is that different from WAF ?
    - WAF protect you against hack and data ingestion and malicious activities
    - Shield protects against sending too much of traffic and making your app down

Standard comes with all aws accounts by default.
Advances : 3000 / month



AWS inspector vs AWS Trusted Advisor vs Cloud Trail

Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. Amazon Inspector automatically assesses applications for vulnerabilities or deviations from best practices. After performing an assessment, Amazon Inspector produces a detailed list of security findings prioritized by level of severity. These findings can be reviewed directly or as part of detailed assessment reports which are available via the Amazon Inspector console or API.

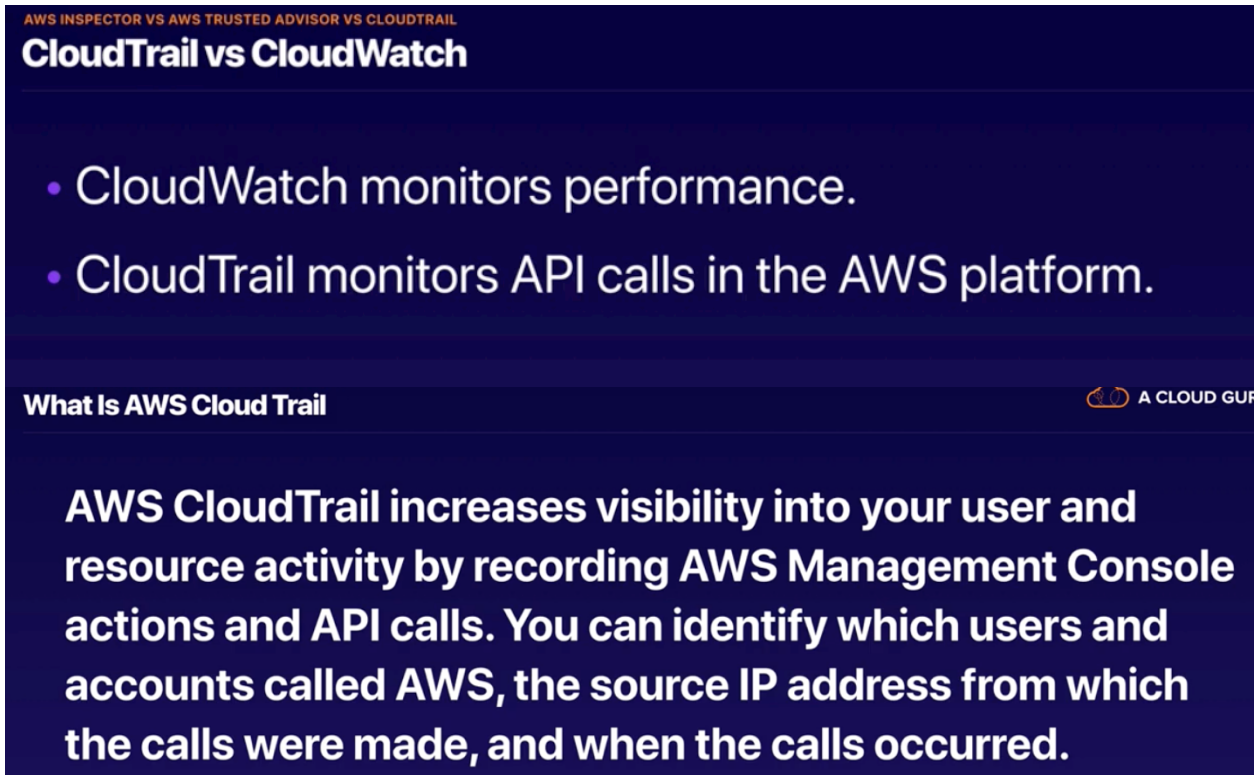
Amazon Inspector operates on your EC2 instances , it is like a software check all the patch and compliance on that ec2 for you .

AWS Inspector, is used for inspecting EC2 instances for vulnerabilities.

AWS Trusted advisor inspects your AWS account as a whole (not just EC2). It does more than just security checks. It also does Cost Optimization, Performance, & Fault Tolerance

AWS CloudTrail increases visibility into your user and resource activity by recording AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from which the calls were made, and when the calls occurred.

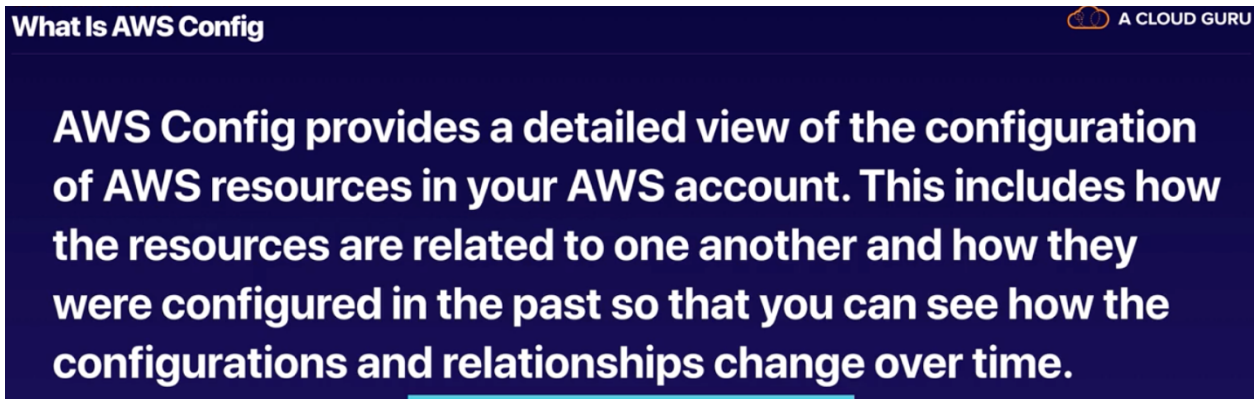
Trusted advisor : looking at your entire eco system



AWS cloud watch vs AWS Config :

Host level of metrics consist of :

- CPU
- Network
- Disk
- Status Check
- Custom metrics using scrips



So if the security group changes … it will be shown in AWS config !

- Not only to see the config of the all instances and their relation ship
- If something change it can show that to us as well

AWS inspector : inspect the 7 layer security level of each instance
AWS trusted advisor : monitor and advise the whole aws eco system on security , cost optimization

- Cost optimization (you need to upgrade it to business package)
- Performance
- Security (provided fro free)
- Fault tolerance
- Service limit
- The default services is open to you but in order to use all thrusted advisor module we need to upgrade it to the business support level

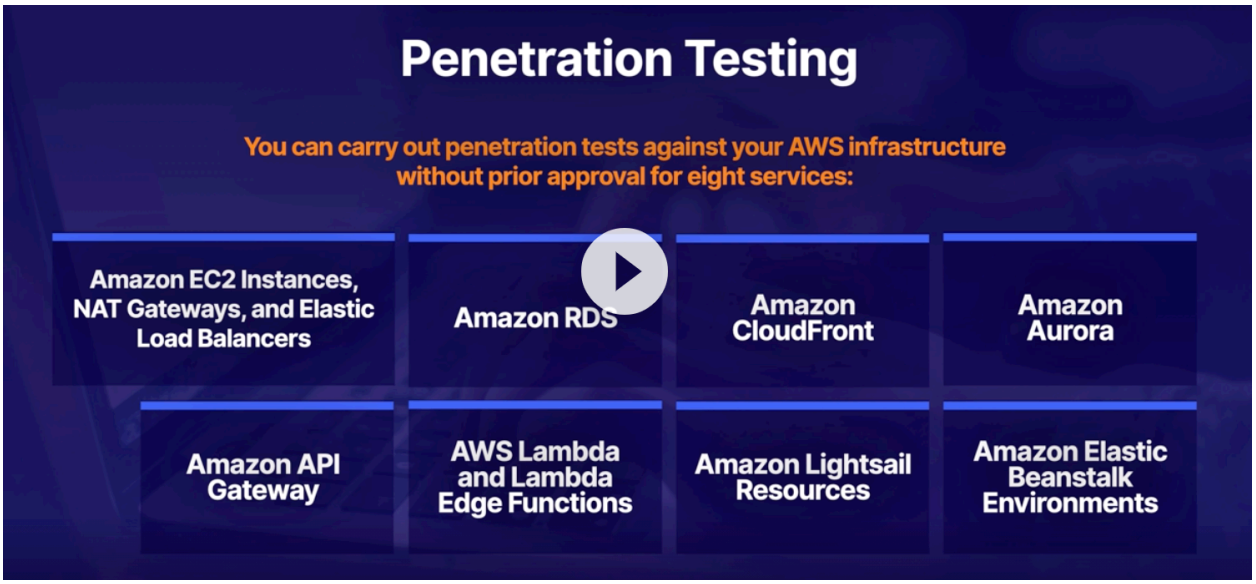
Cloud trail: monitor all the apis calls and log them
Cloud watch: monitor performance & metrics of the instance
AWS config: monitor services config and their relationship and log them

Aws config vs AWS trusted advisor:

- AWS config is logging the relationship between aws resources
- AWS trusted advisor: other than monitoring and advising on performance and cost
    - It checks the security as well
-

Penetration testing :

- What ? pen test : simulated cyber attack to check
- Which services without prior approval : EC2, Lambda , RDS , Beanstalk , Aurora , cloud front , api
-



- There are a bunch of things that you cannot do that
- For any simulated we need to contact them

AWS KMS : key management services

- Regional bases : keys generated in virgina cannot be used in the other regions
- Manages customer master keys (use for encryption and decryption)
- Good for s3 objects , database passwords , PAI keys stored in the systems manager parameters
- Encrypt and decrypt up to 4gb integrated with any services == S3
- KMS is on shared hardware … with other KMS cutomers ,
    - Like ec2s which is a shared hardware , KMS is also located on shared hardware not on a hardware dedicated to you.

AWS HSM :

- Does every thing KMs does and more
- It is a dedicated hardware security module (HSM) == more expensive
- It complies with FIPS 140 level 3 : fed information process standards : governmental security
- It is single tenant since it is dedicated. But you can deploy it to multiple availability zone as well.

Parameter store vs secret manager:
- Both store your password

Param store:
- Part of System manager (SSM)
- Secure serverless storage for configuration and secret
    - Passwords
    - Database connection strings
    - Values can be encrypted using KMS
    - Can set TTL ; time to live
    - Free , 10,000 parameters per account

Secret manager :
- Like para store
- It is not free
- Some more advantages:
    - Rotate secretes
    - Apply the new key / password in RDS for you
        - Can store secrete in cloud formation
    - Generate random secretes

AWS guard duty :
- Using machine learning for anomaly detection
- One click , 30 day trail
- Inputs :
    - Cloud trail logs
    - VPC logs
    - DNS logs
- Control tower vs guradduty : gurad duty just runs across one accont

Control tower:
- The easiest way to set up and govern a new , secure , multi account AWS environment
- Allow you to provision multiple aws accounts in just few minutes
- Those account will conform the company policy
- Used for large enterprises with multiple aws accounts

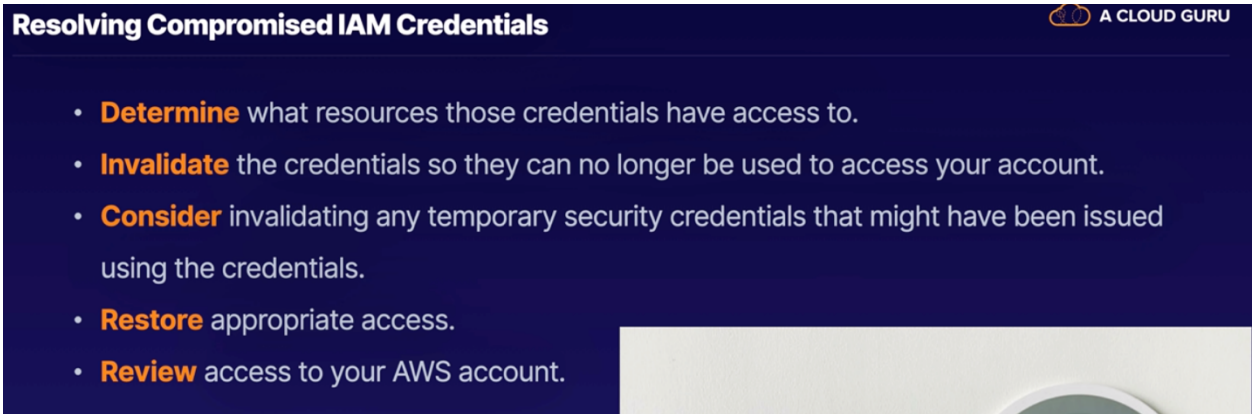
Security hub :
- A comprehensive view of your security alerts across multiple AWS accounts
- Security hub is a single place that aggregates , organize , prioritizes your security alert or find bugs from multiple aws services such as Amzon guard duty amazon inspector ,

amazon macies , amazon Identity abd access management , analyzer , aws firwall manager across multiple account s

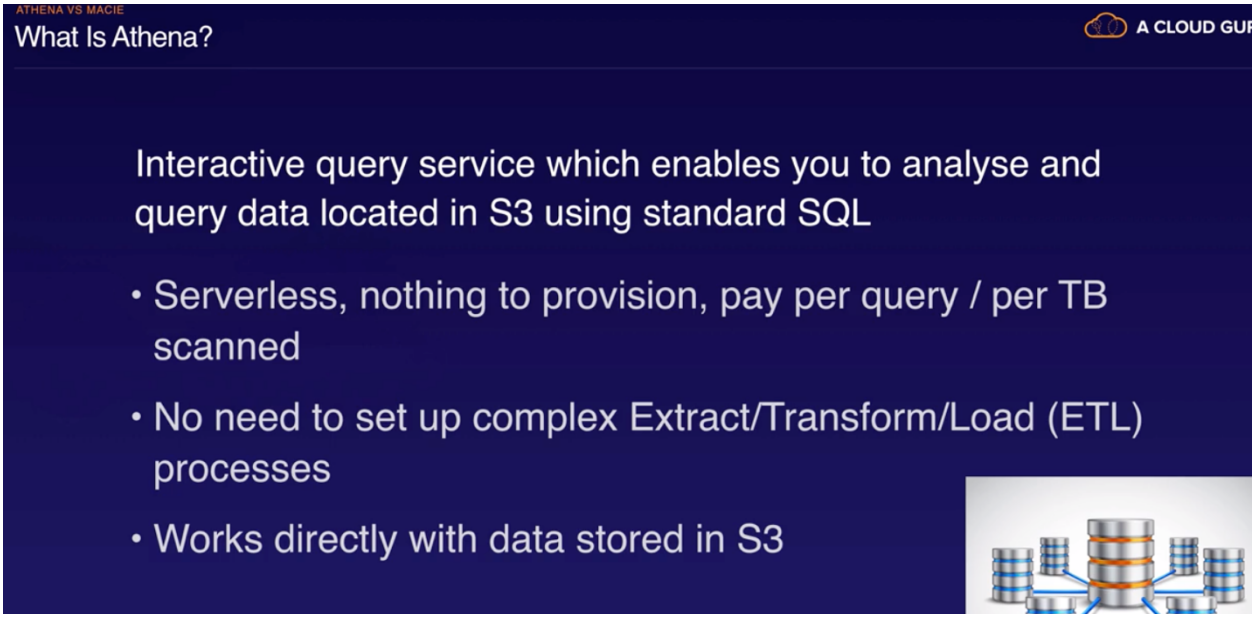
- From different services
- Across multiple accounts

Compromised IMA credential :

- Stolen credential
- Determine what resources do these credential have access to to ?
  - Invalidate those credentials
  - Invalidating temporary security credentials that might have been issued
  - Restore appropriate access
  - Review access in your aws accounts



Athena vs Macies :



Athena Use Cases

A CLOUD GURU

What Can Athena Be Used For?

- Can be used to query log files stored in S3, e.g. ELB logs, S3 access logs etc
- Generate business reports on data stored in S3
- Analyse AWS cost and Usage reports
- Run queries on click-stream data

ATHENA VS MACIE

What is Macie?

A CLOUD GU

What is PII? (Personally Identifiable Information)

- Personal data used to establish an individual's identity
- This data could be exploited by criminals, used in identity theft and financial fraud
  - Home address, email address, SSN
  - Passport number, Drivers license number
  - D.O.B, phone number, bank account, credit card number

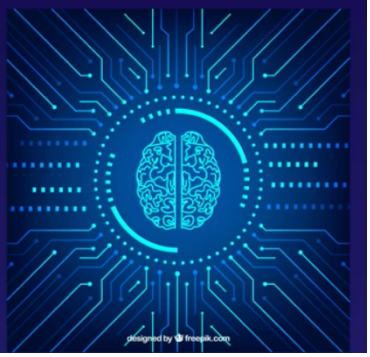
ATHENA VS MACIE

What Is Macie?

A CLOUD GU

Security service which uses Machine Learning and NLP (Natural Language Processing) to discover, classify and protect sensitive data stored in S3

- Uses AI to recognise if your S3 objects contain sensitive data such as PII
- Dashboards, reporting and alerts
- Works directly with data stored in S3
- Can also analyze CloudTrail logs
- Great for PCI-DSS and preventing ID theft

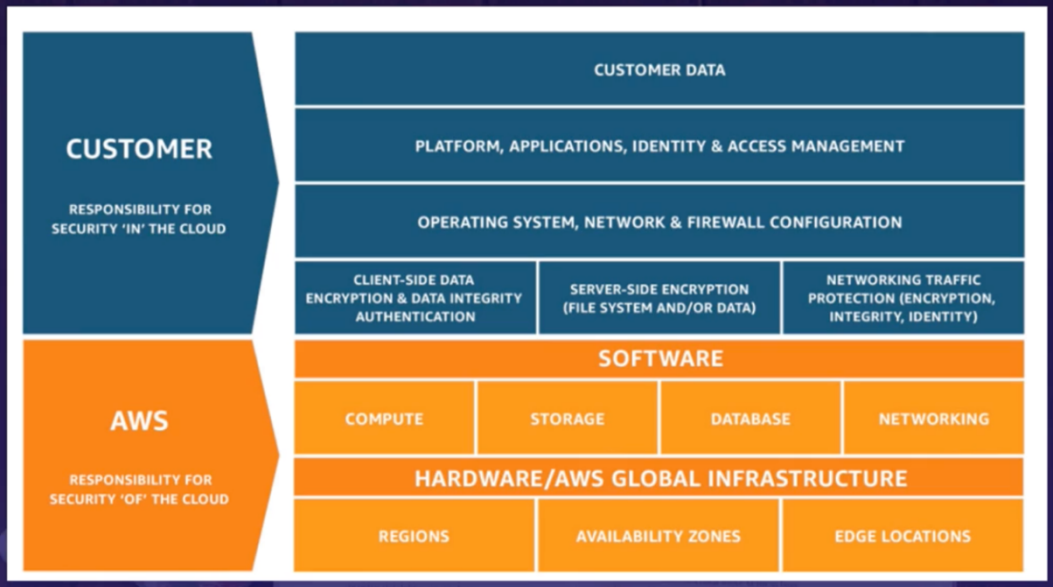


AWS Artifact is used to retrieve compliance reports.

SECURITY SUMMARY

Exam Tips

A CLOUD G



AWS WAF is a Web Application Firewall, designed to stop hackers

AWS Shield is a DDOS mitigation service designed to stop DDOS attacks.

AWS Inspector, is used for inspecting EC2 instances for vulnerabilities.

AWS Trusted advisor inspects your AWS account as a whole (not just EC2). It does more than just security checks. It also does Cost Optimization, Performance, & Fault Tolerance

AWS CloudTrail increases visibility into your user and resource activity by recording AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from which the calls were made, and when the calls occurred.

Athena Exam Tips

- Remember what Athena is and what it allows you to do
- Athena is an interactive query service
- Allows you to query data located in S3 using standard SQL
- Serverless
- Commonly used to analyse log data stored in S3

Macie Exam Tips

- Remember what Macie is and what it allows you to do
- Macie uses AI to analyze data in S3 and helps identify PII
- Can also be used to analyse CloudTrail logs for suspicious API activity
- Includes Dashboards, Reports and Alerting
- Great for PCI-DSS compliance and preventing ID theft

SECURITY SUMMARY
Exam Tips

A CLOU

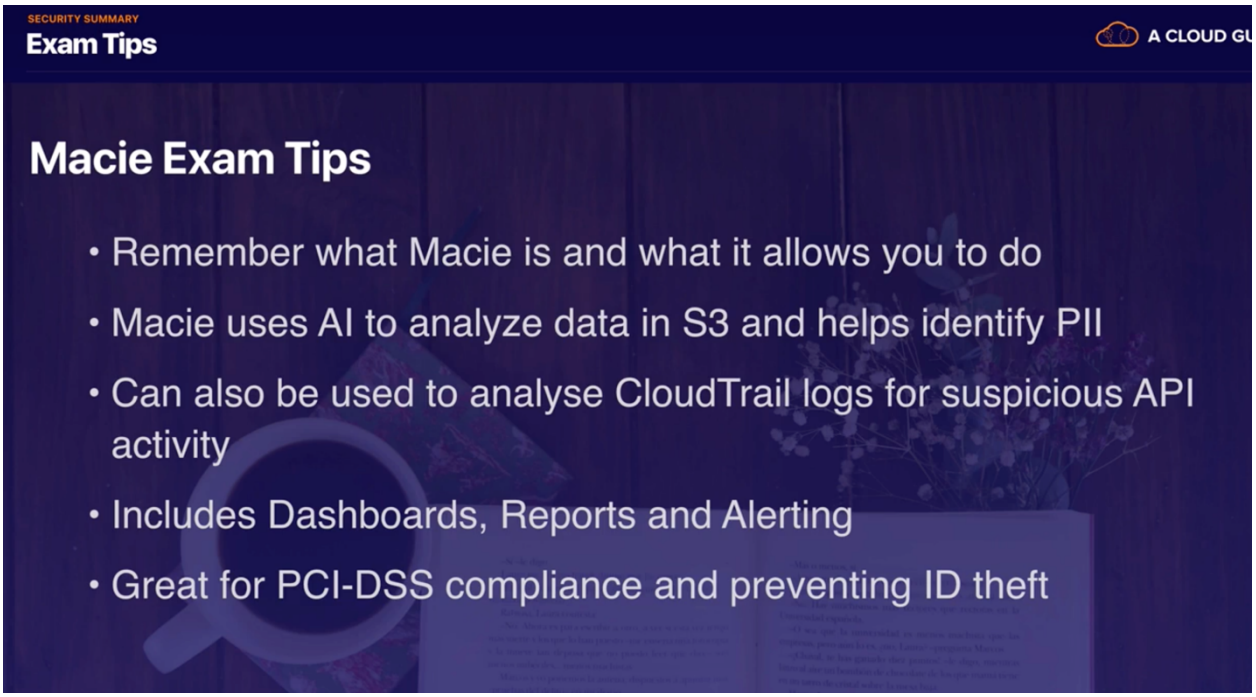
AWS CloudTrail increases visibility into your user and resource activity by recording AWS Management Console actions and API calls. You can identify which users and accounts called AWS, the source IP address from which the calls were made, and when the calls occurred.

SECURITY SUMMARY
Exam Tips

A CLOUD GURU

Athena Exam Tips

- Remember what Athena is and what it allows you to do
- Athena is an interactive query service
- Allows you to query data located in S3 using standard SQL
- Serverless
- Commonly used to analyse log data stored in S3


Macie Exam Tips
• Remember what Macie is and what it allows you to do
• Macie uses AI to analyze data in S3 and helps identify PII
• Can also be used to analyse CloudTrail logs for suspicious API activity
• Includes Dashboards, Reports and Alerting
• Great for PCI-DSS compliance and preventing ID theft

QUESTION 2

Which of the following Compliance guarantees attests to the fact that the AWS Platform has met the standard required for the secure storage of medical records in the US?

- PCI DSS
- FERPA
- GLBA
- HITECH
- HIPAA

Good work!

A HIPAA certification attests to the fact that the AWS Platform has met the standard required for the secure storage of medical records in the US

Next question

Rate this question

QUESTION 6

Which of the following Compliance certifications attests to the security of the AWS platform regarding credit card transactions?

- ISO 27001
- SOC 2
- SOC 1
- PCI DSS Level 1 ✓

Good work!

A PCI DSS Level 1 certification attests to the security of the AWS platform regarding credit card transactions.

Next question

Rate this question

QUESTION 10

True or False: The Standard version of AWS Shield offers automated application (layer 7) traffic monitoring.

- ✓ False
- ✗ True

Sorry!

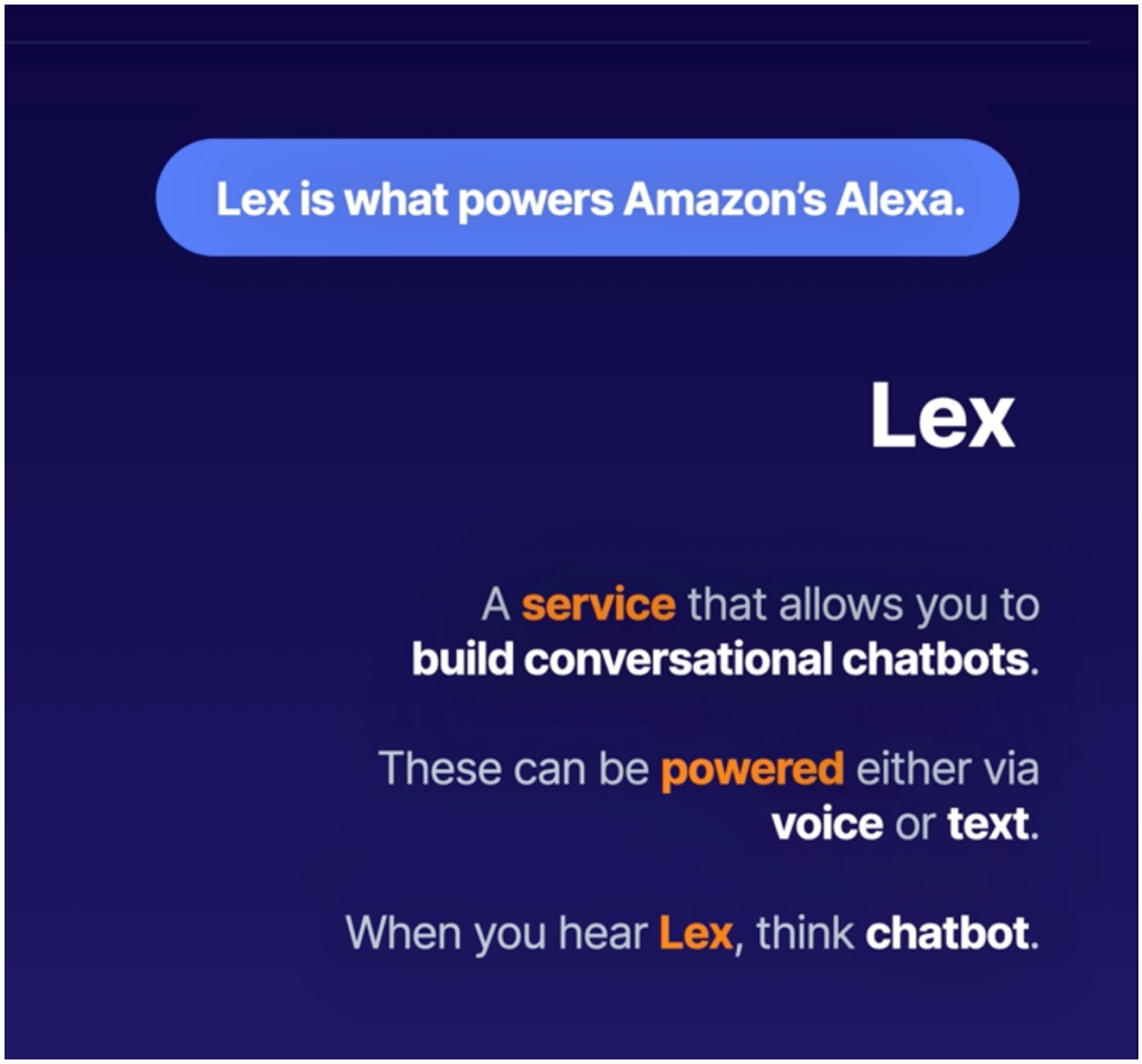
Automated application (layer 7) traffic monitoring is an AWS Shield Advanced feature. Reference: How AWS Shield works.

Correct Answer

AWS Shield Standard defends against most common, frequently occurring network and transport layer DDoS attacks that target your website or applications. For higher levels of protection against attacks, including Automated application (layer 7) traffic monitoring, you can subscribe to AWS Shield Advanced. Reference: How AWS Shield works.

Get my results

Rate this question



Poly use lex to convert text to life-like voice.

Polly converts text to life-like voice.

Amazon Polly

You can choose between a number of different languages, whether the voice is male or female, and even what accent you would like the voice to be rendered in.

AI SERVICES: LEX, POLLY, TRANSCRIBE, AND REKOGNITION

Amazon Transcribe

Transcribe

Converts speech into text.

This can be great for **generating subtitles** or getting transcripts of interviews, speeches, and more.



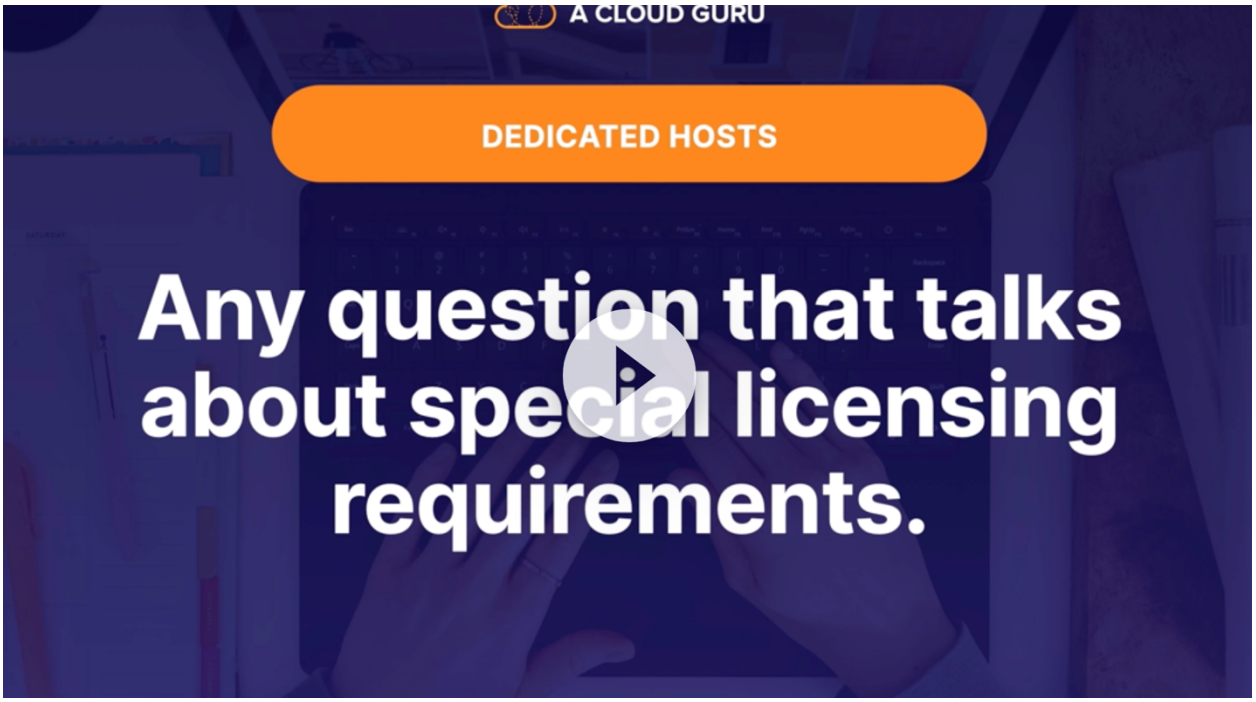
A CLOUD GURU

A way of converting images into tags/text.

Rekognition

Upload an image and Rekognition will tell you what it thinks the image is with a certain **degree of confidence**.

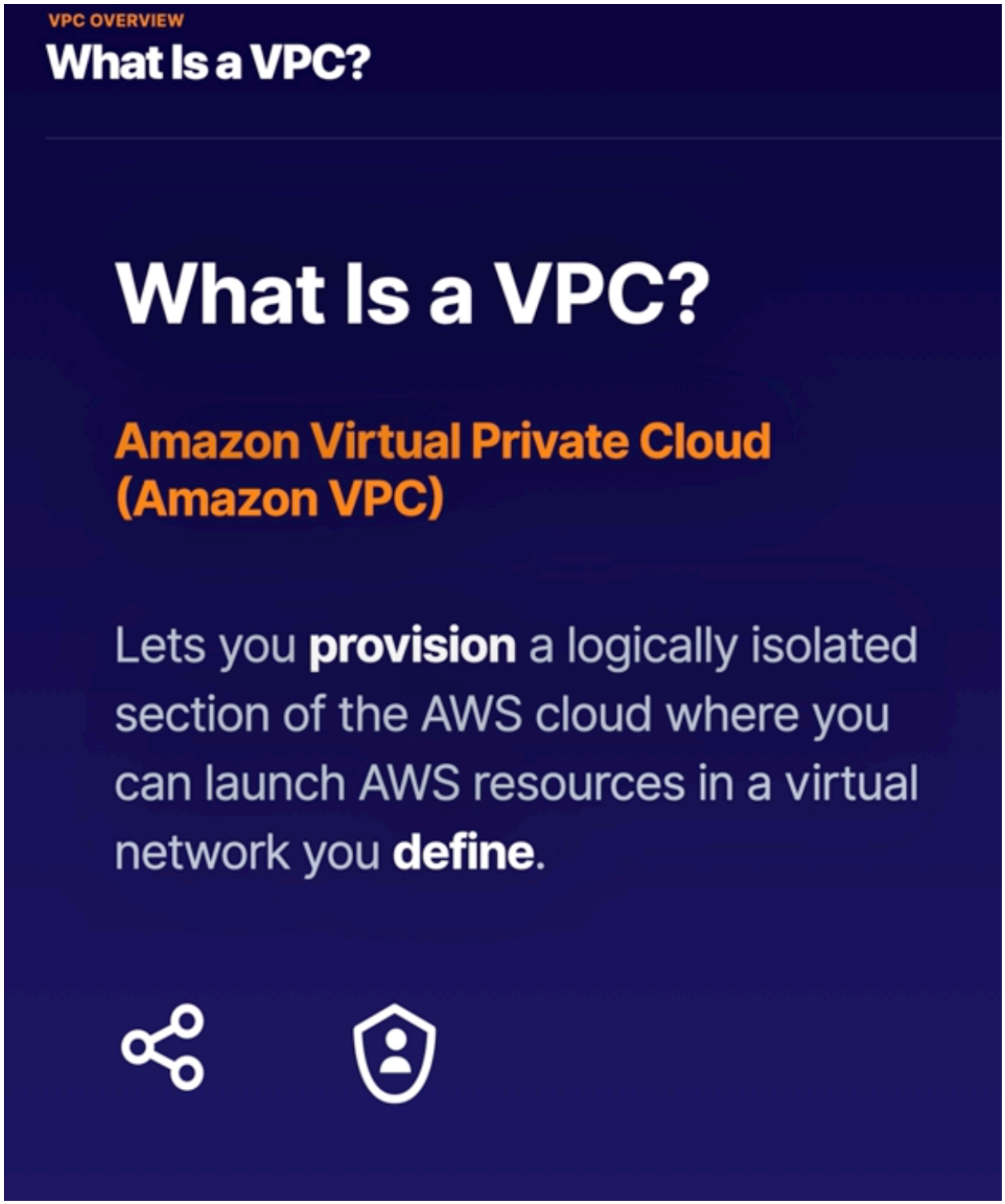
Can be used with lots of apps — for example, an app where you take a photo of a leaf and the app uses Rekognition to **identify** what plant it is based on the picture.



Different compute services :

1- EC2
    a. It is deployment in VPC ; connect all the components in the cloud
2- Lightsail : simple cloud service
    a. You will get just an instance where you can do your shit
    b. It is not in the vpc and it does n't have connectivity with aws services
    c. It is more like a VM
3- Lmbda : serverless in the cloud
4- Batch computing
5- Elastic Beanstalk
    a. Platform as Service
    b. Deploying quickly
6- Serverless application Repository
    a. Allows you to deploy pre-provisioned serverless applications (alexa)
    b. It allows you to deploy prepared code into lambda and modify it
7- AWS outposts
    a. Extending compute to your own data center or on-prem
8- EC2 Image Builder
    a. Help to create instance based your custom ECW images

VPC :



It gives you an virtual cloud where you can have the connectivity between your own instances, like ec2 , lambda , RDS … It is like a virtual data center in the cloud for you! Customizable Configuration.

Customizable Configuration

You can easily **customize** the network configuration for your Amazon VPC.

For example, you can create a **public-facing network zone** for your web servers that has access to the internet, and place your backend systems (such as databases or application servers) in a **private network zone** with no internet access.

Connecting On-premise to AWS :

1. VPN :
    a. you can create a hardware virtual private network (vpn) connection between your and center and your vpc, leveraging the Aws cloud as an extension of your corporate network and data center
2. Direct Connect :
    a. You can establish private connectivity between AWS and your data center, office , or colocation environment which in many cases can reduce your network cost , increase bandwidth throughput and provide a more consistent network experience than internet -base connections.
3. VPN over Direct Connect :
    a. Combined both methods

AWS Lambda :

Supported Languages

What languages does Lambda support?

- Node.js
- Java
- Python
- C#
- Go
- PowerShell

The Basics: Pricing

How Is Lambda Priced?

1

Number of Requests

First **1 million** requests are **free**.
$0.20 per 1 million requests **thereafter**.

AWS LAMBDA

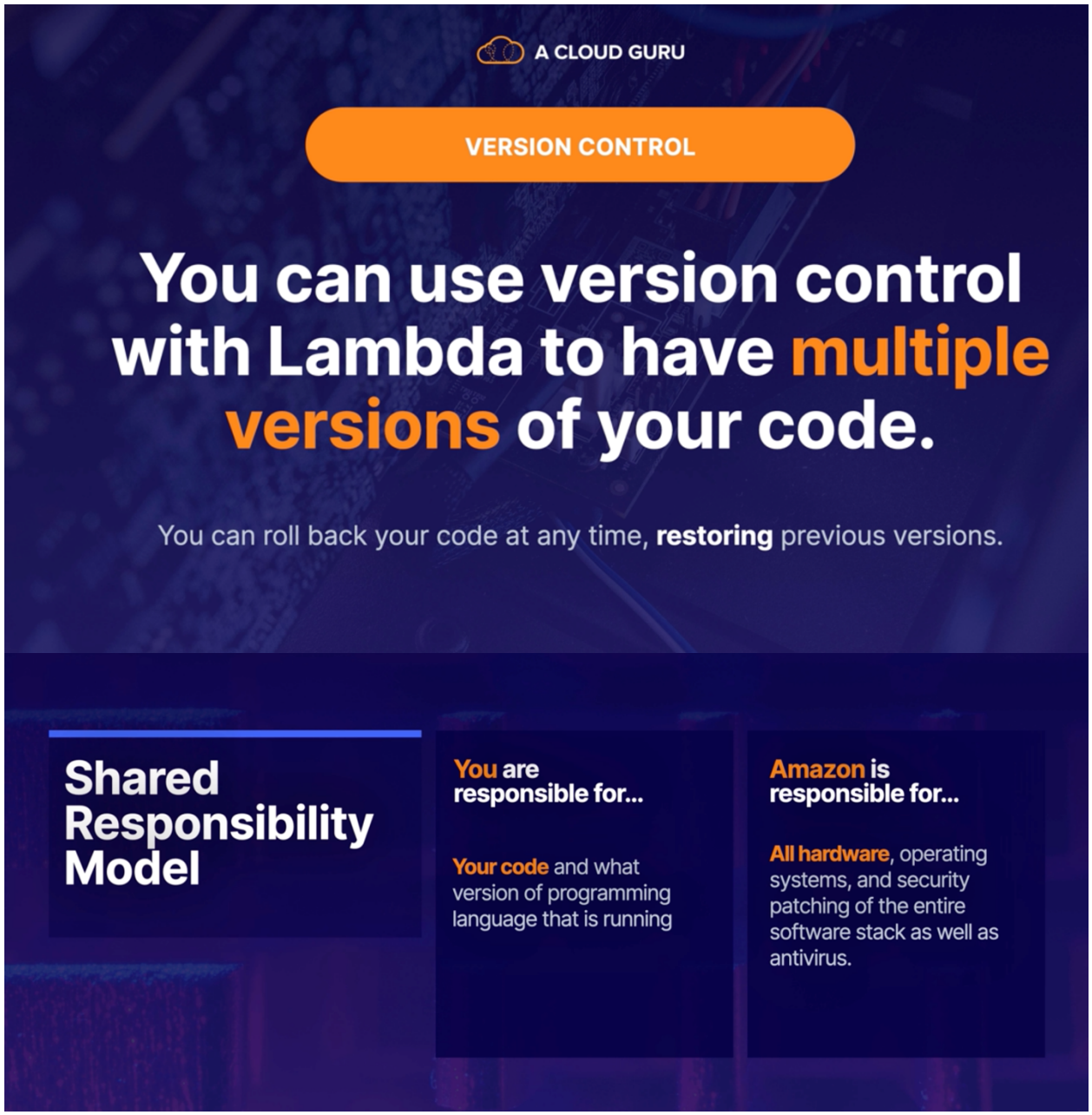
The Basics: Pricing

How Is Lambda Priced?

2

Duration

Duration is calculated from the time your **code begins executing** until it **returns** or otherwise **terminates**, rounded up to the **nearest 100ms**. The price depends on the amount of **memory** you allocate to your function. You are charged $0.00001667 for every GB-second used.


A CLOUD GURU
VERSION CONTROL
You can use version control with Lambda to have multiple versions of your code.
You can roll back your code at any time, restoring previous versions.
Shared Responsibility Model
You are responsible for...
Your code and what version of programming language that is running
Amazon is responsible for...
All hardware, operating systems, and security patching of the entire software stack as well as antivirus.

AWS LAMBDA

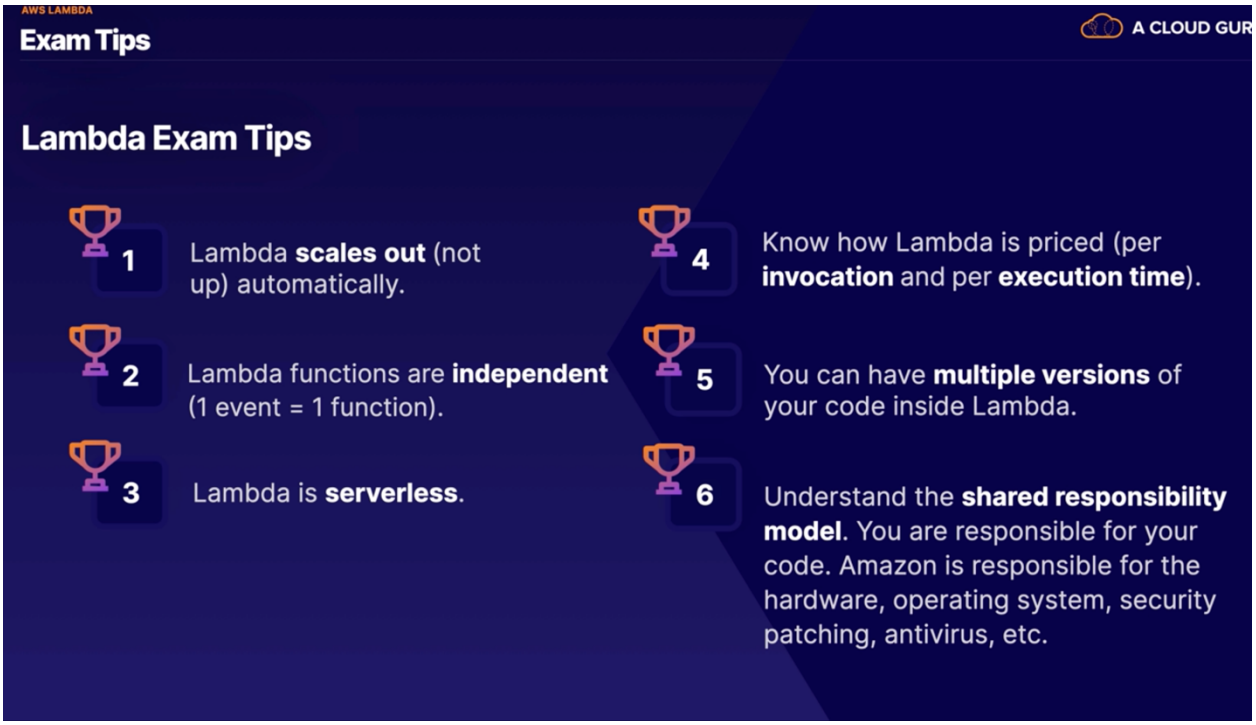
What Sets Lambda Apart?

Why Is Lambda Cool?

No servers!

Continuous scaling

Super cheap!


AWS LAMBDA
Exam Tips
A CLOUD GUR
Lambda Exam Tips
1
Lambda scales out (not up) automatically.
2
Lambda functions are independent (1 event = 1 function).
3
Lambda is serverless.
4
Know how Lambda is priced (per invocation and per execution time).
5
You can have multiple versions of your code inside Lambda.
6
Understand the shared responsibility model. You are responsible for your code. Amazon is responsible for the hardware, operating system, security patching, antivirus, etc.