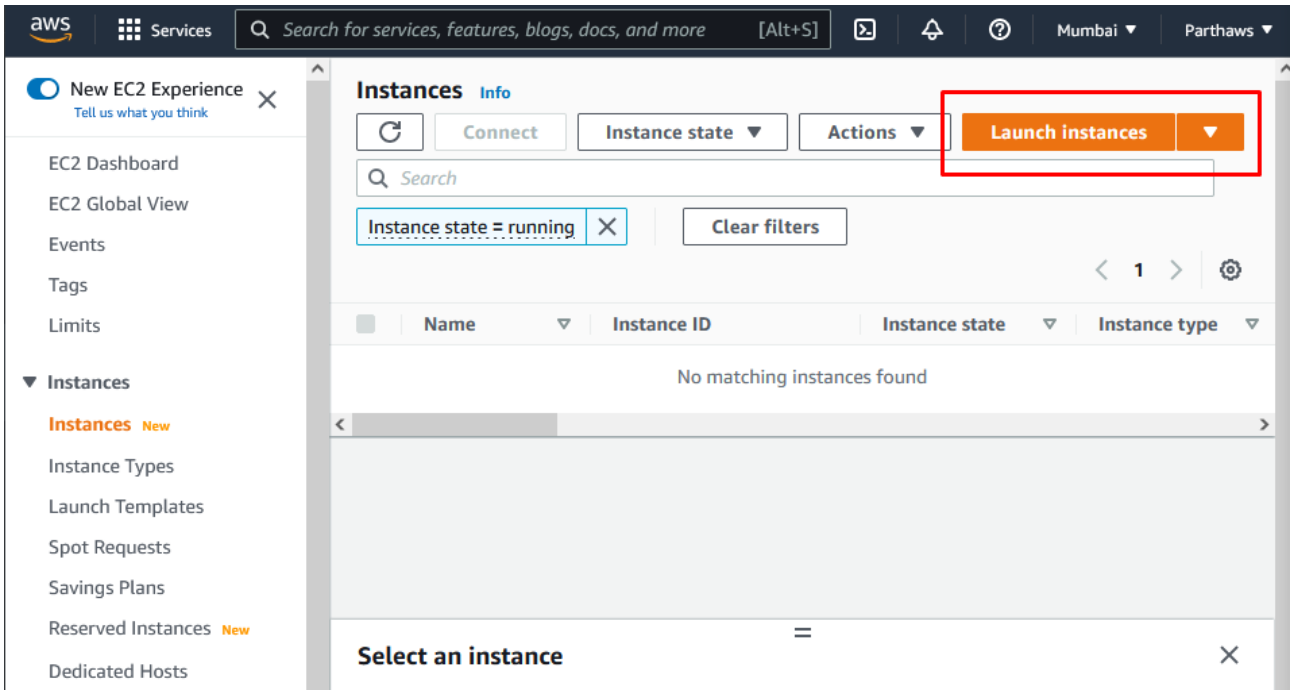
Q1. Working and Implementation of Infrastructure as a service.

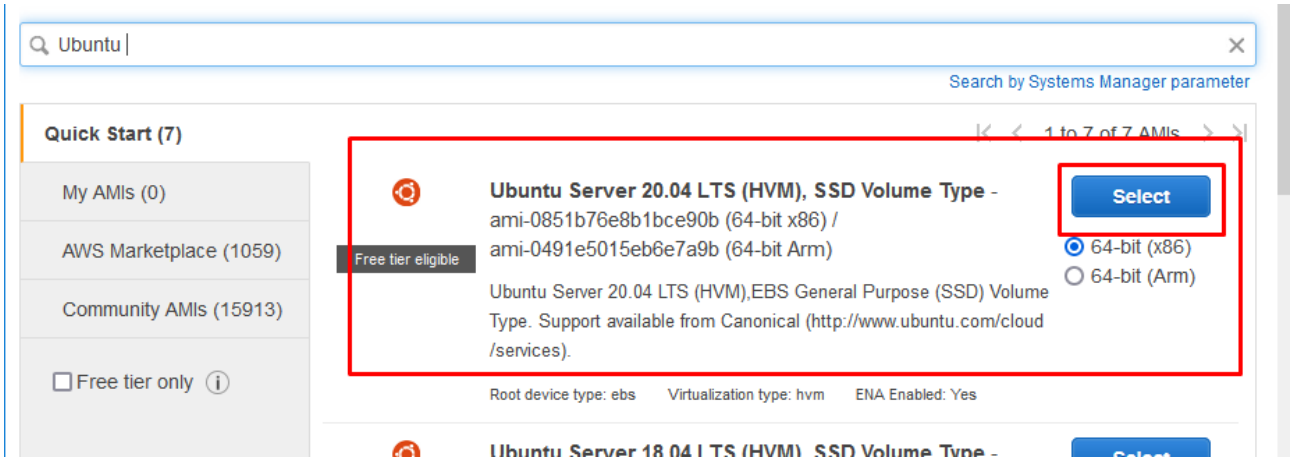
- VM (GCP)
- EC2 (AWS)
- Share screenshots of each step
- Detail out what are pros and cons of it

Answer using AWS

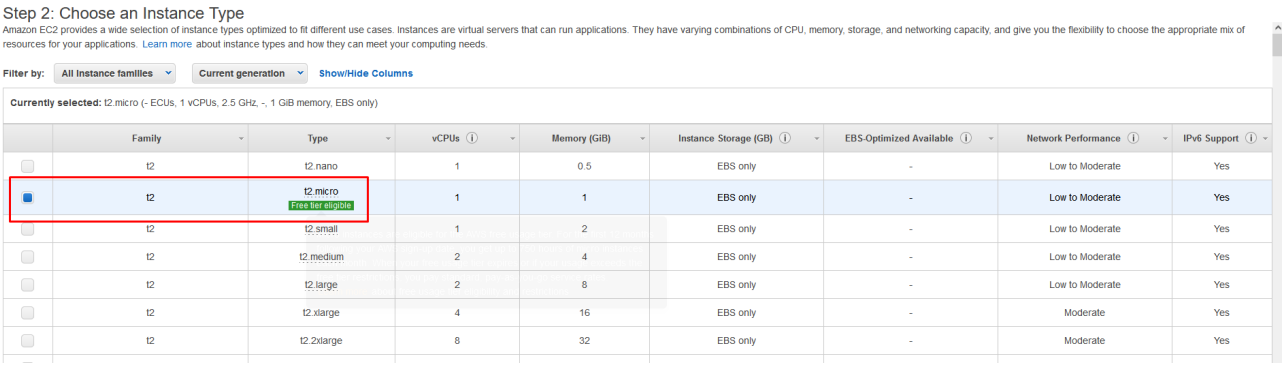
> Search for EC2 or Elastic Compute Cloud service on AWS and click on Launch Instance



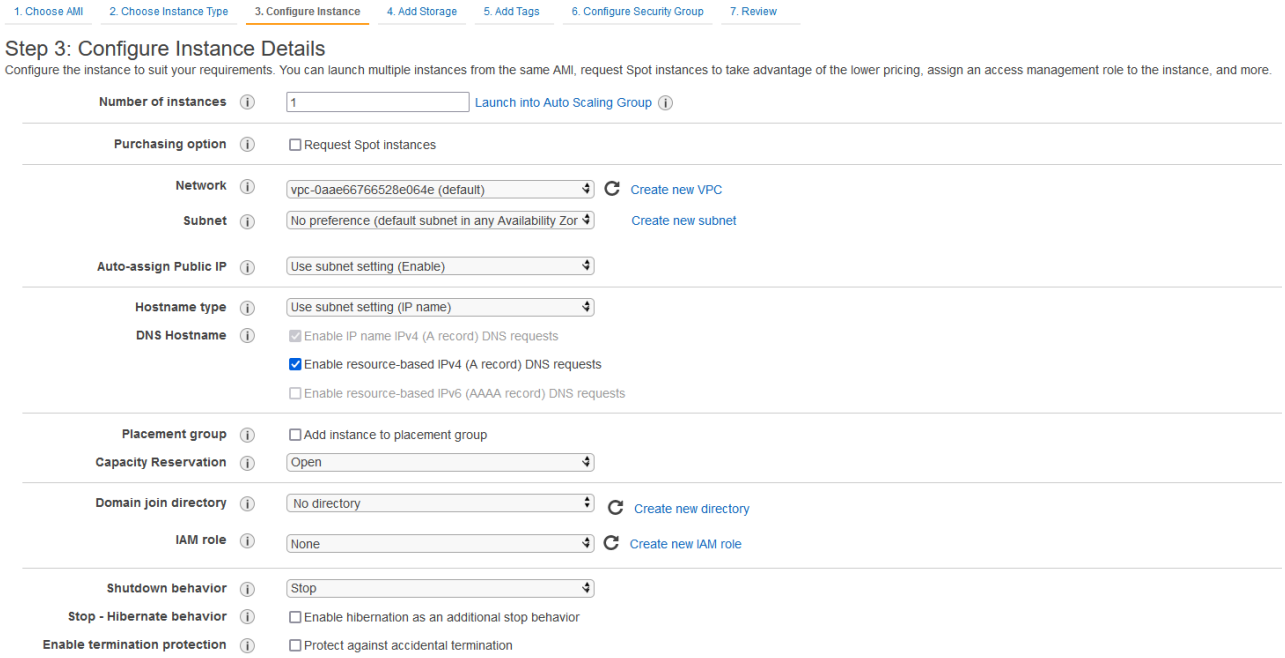
> Select the OS you want the instance to be created in (Ubuntu 20.04 in this example) and select the instance



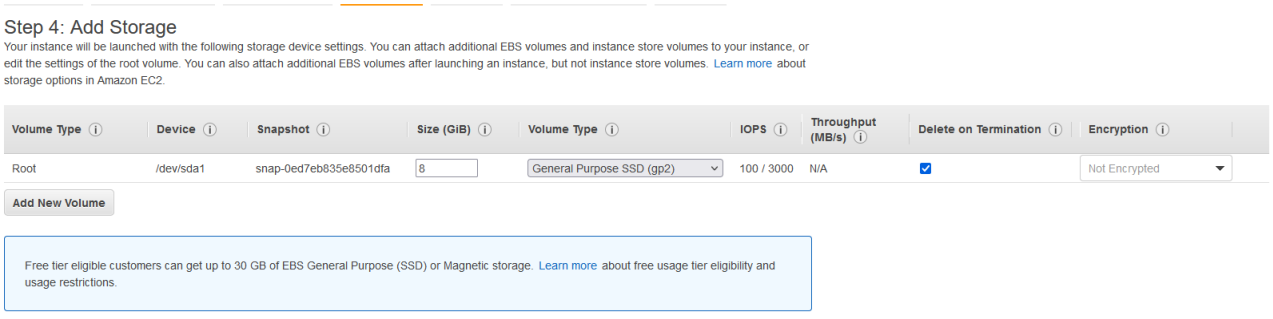
> We will be selecting free tier as of now for the VM instance type and go ahead with Instance Configuration



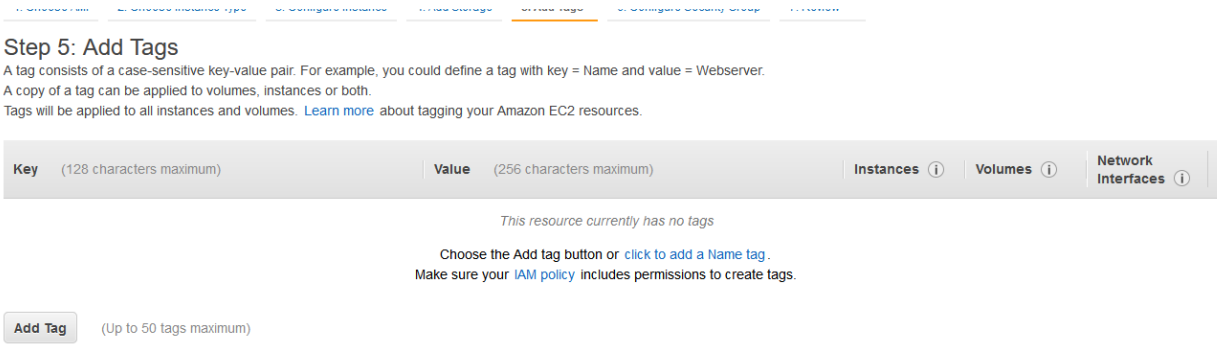
> Configure any of the specifications required in this step



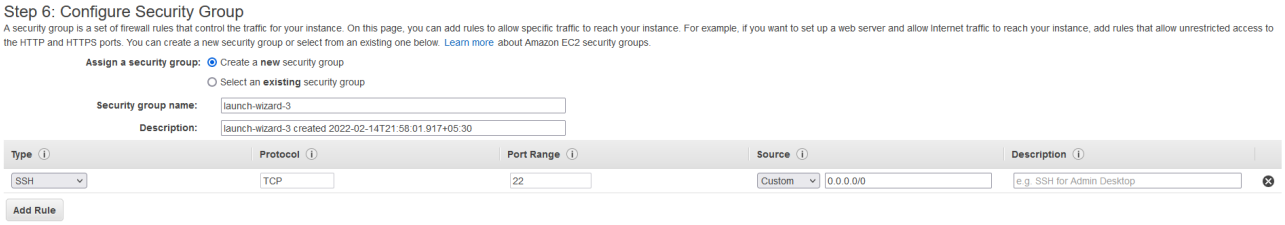
> In the next step configuration Add any storage requirements you required



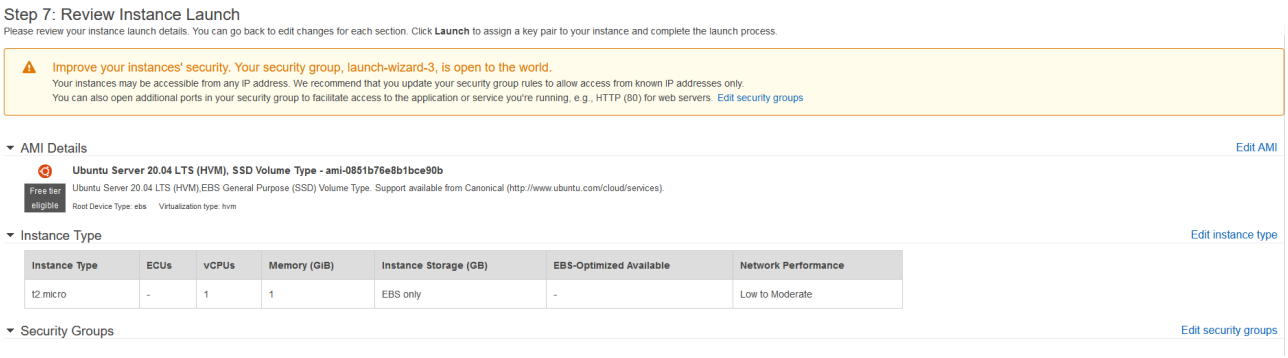
> Add any tags you require in the next step which will help you distinguish between VMs



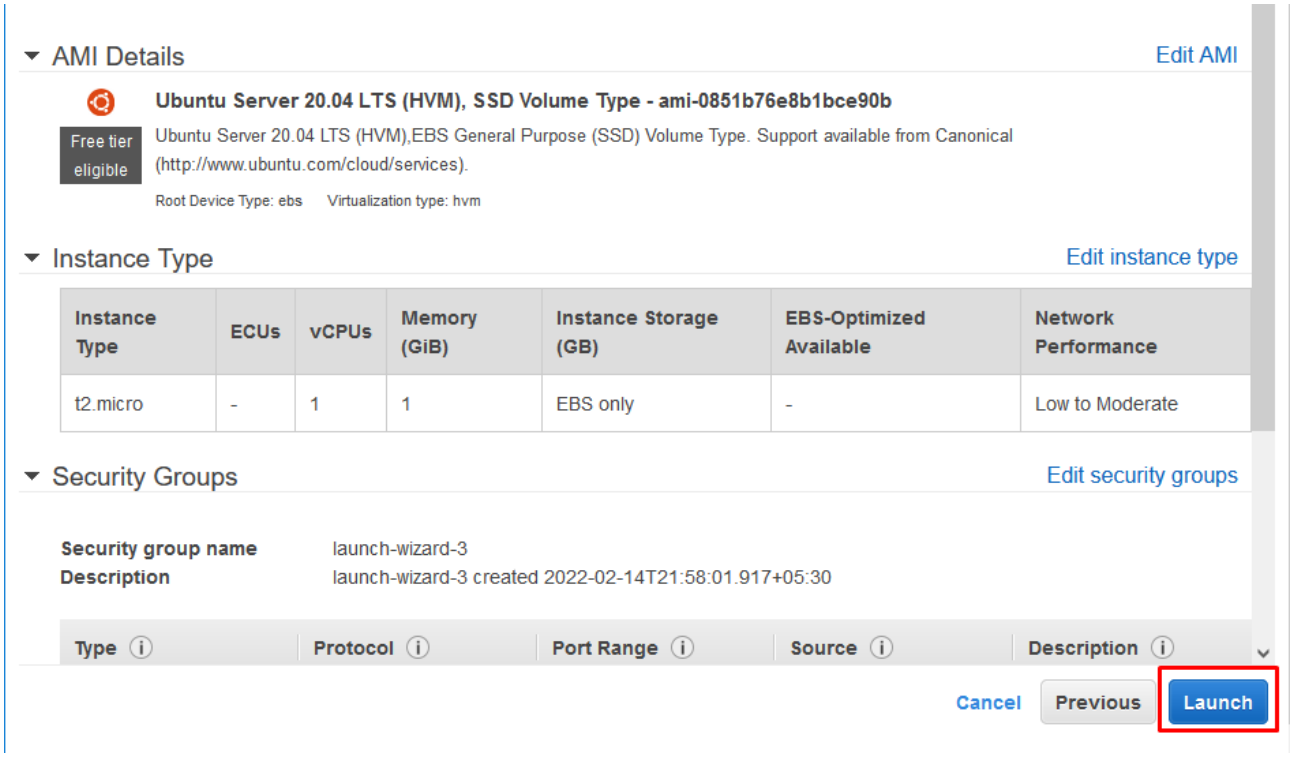
> In the next step Configure the security groups which you wish to set



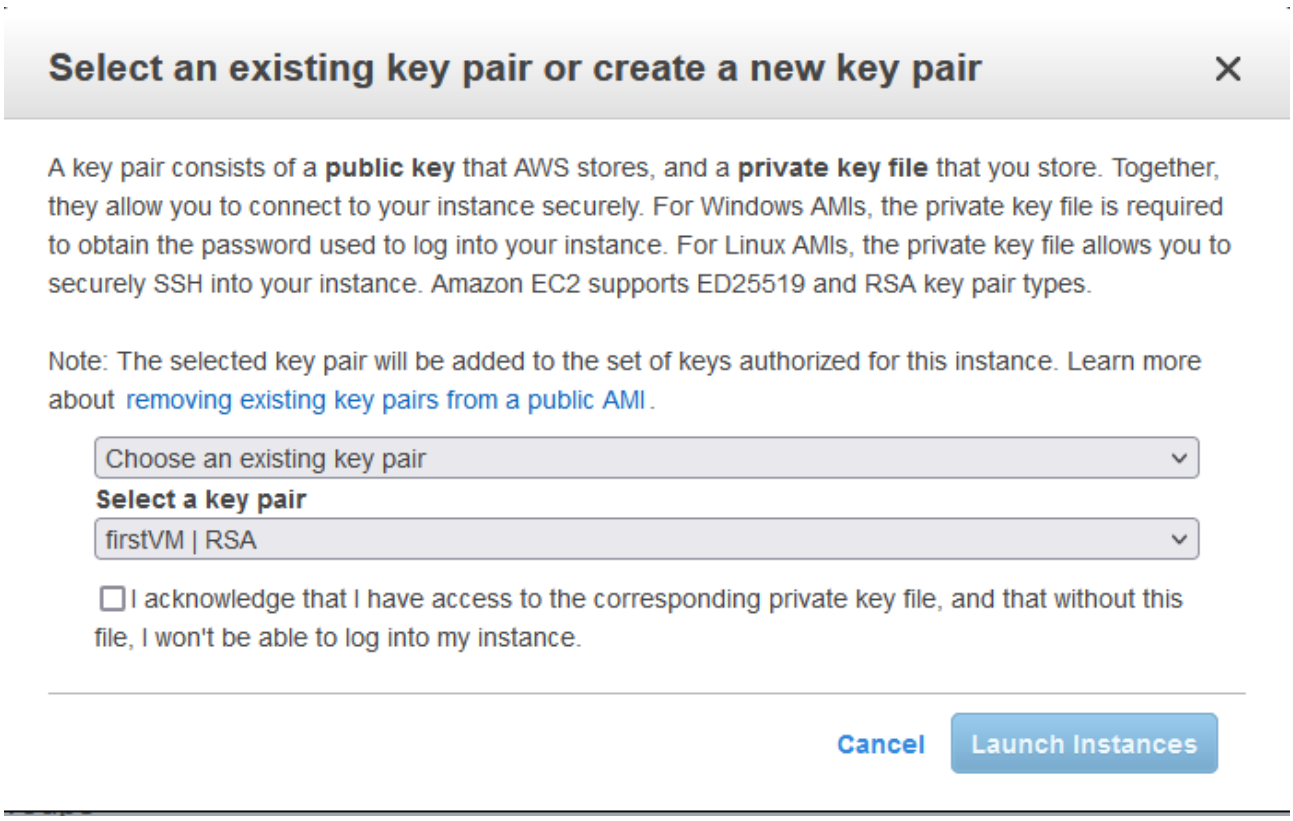
> In the next and last step review any settings you wish to change



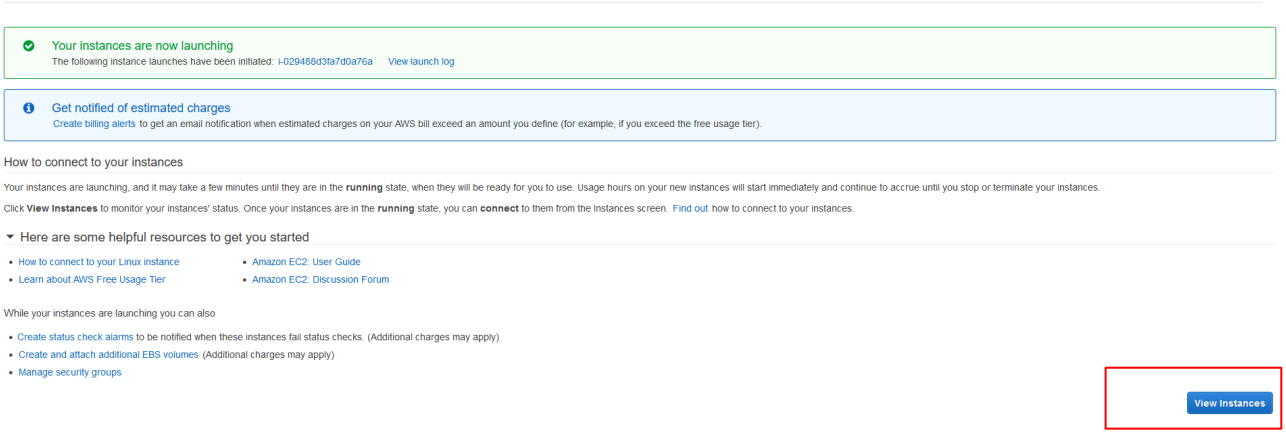
> Click on Launch when you wish to launch your VM



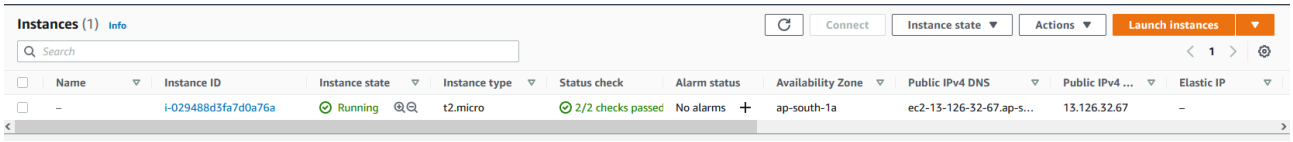
> Create key pair or use existing key pairs which will help login to your VM



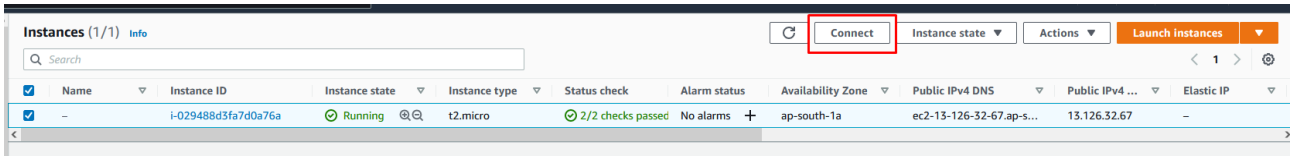
> Click on View Instance



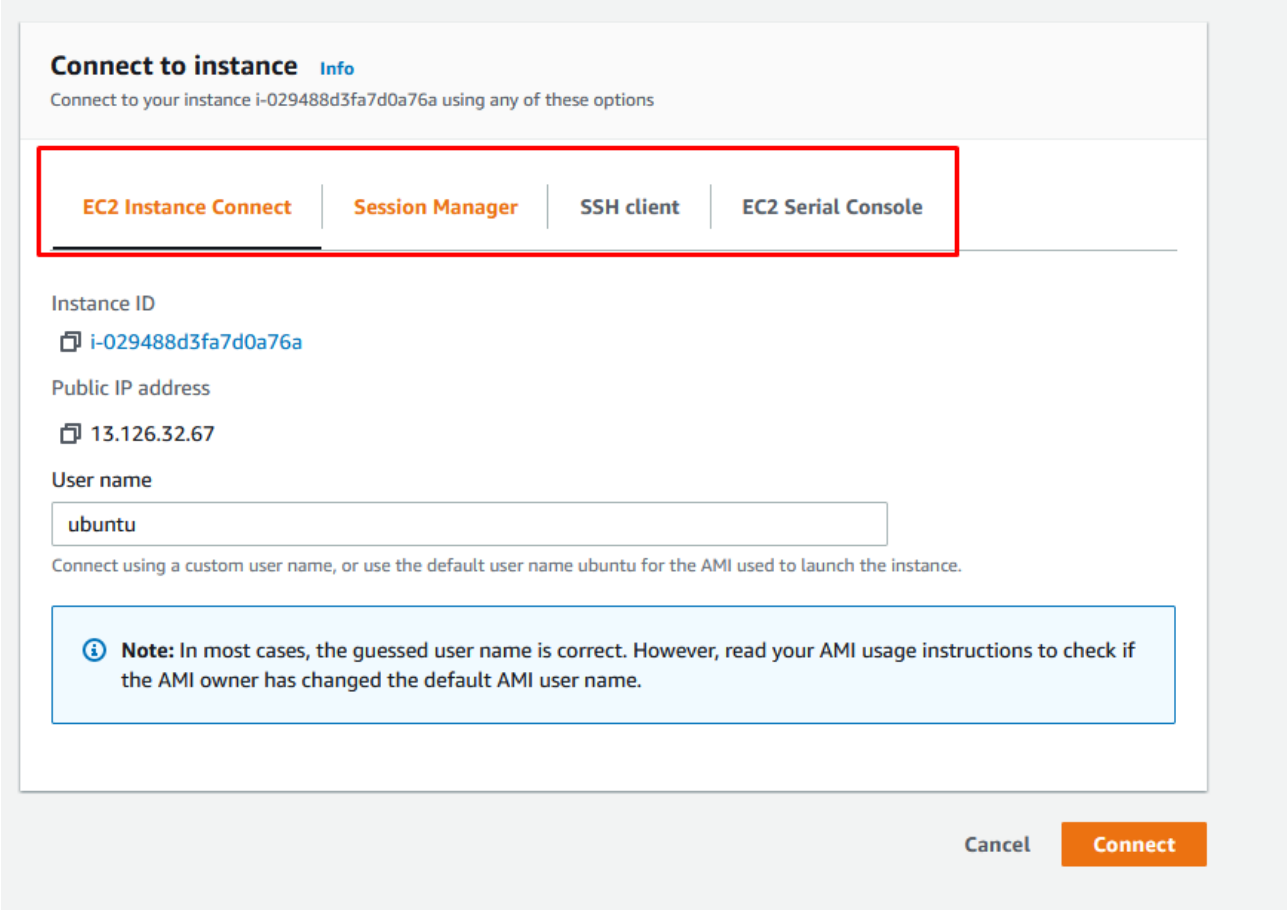
> We can see our Instance here in the list



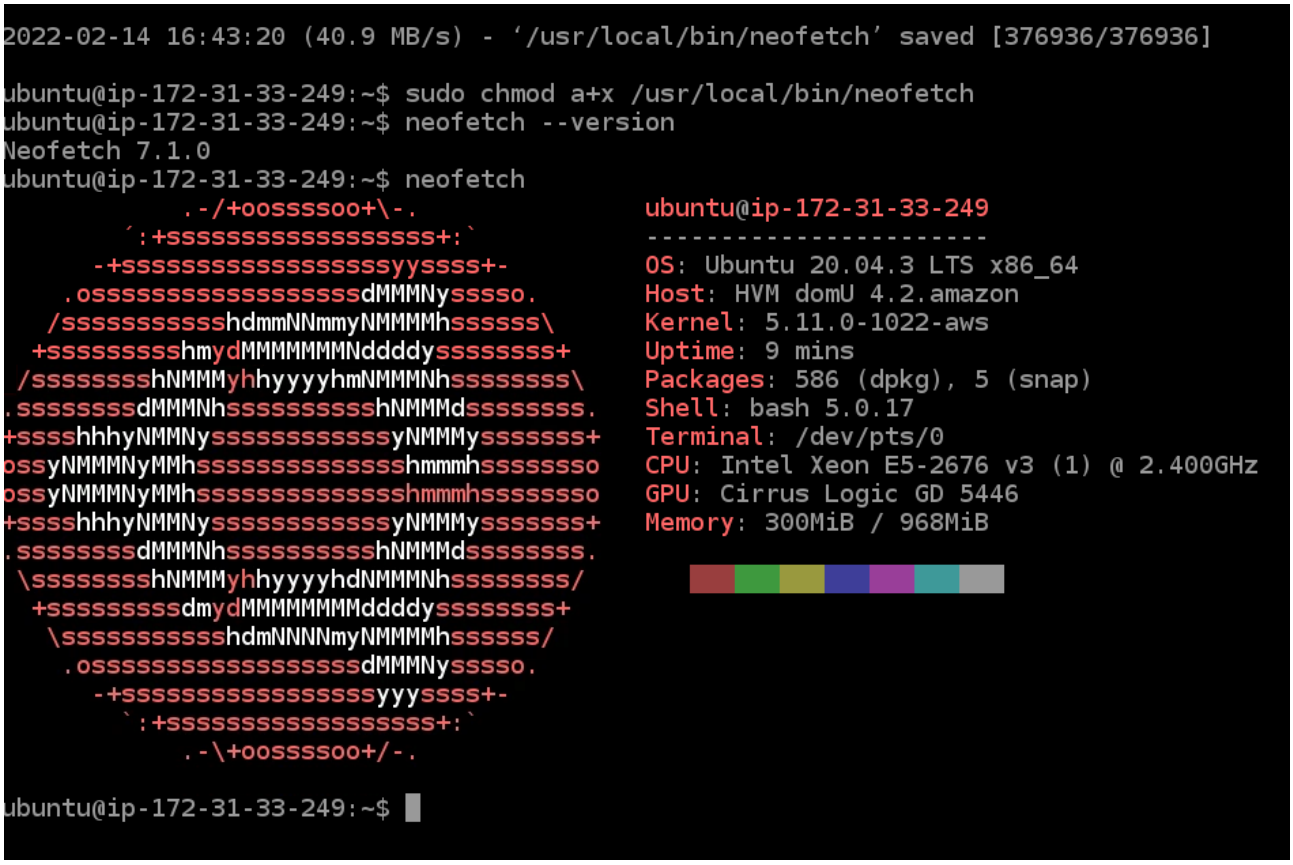
> Select the instance and click connect to connect to the instance



> Choose the method you want to connect to your VM with



> After connecting you are inside your configured VM



Pros and Cons of EC2

Pros

- It has the ability to expand resources for the deployment of your cloud according to demand makes it extremely likeable.
- Cloud hosting offers excellent backup capabilities, so it's a breeze to go back to the previous version.
- The cloud infrastructure prevents us from maintaining local hardware resources.
- Amazon EC2 is highly scalable.

Cons

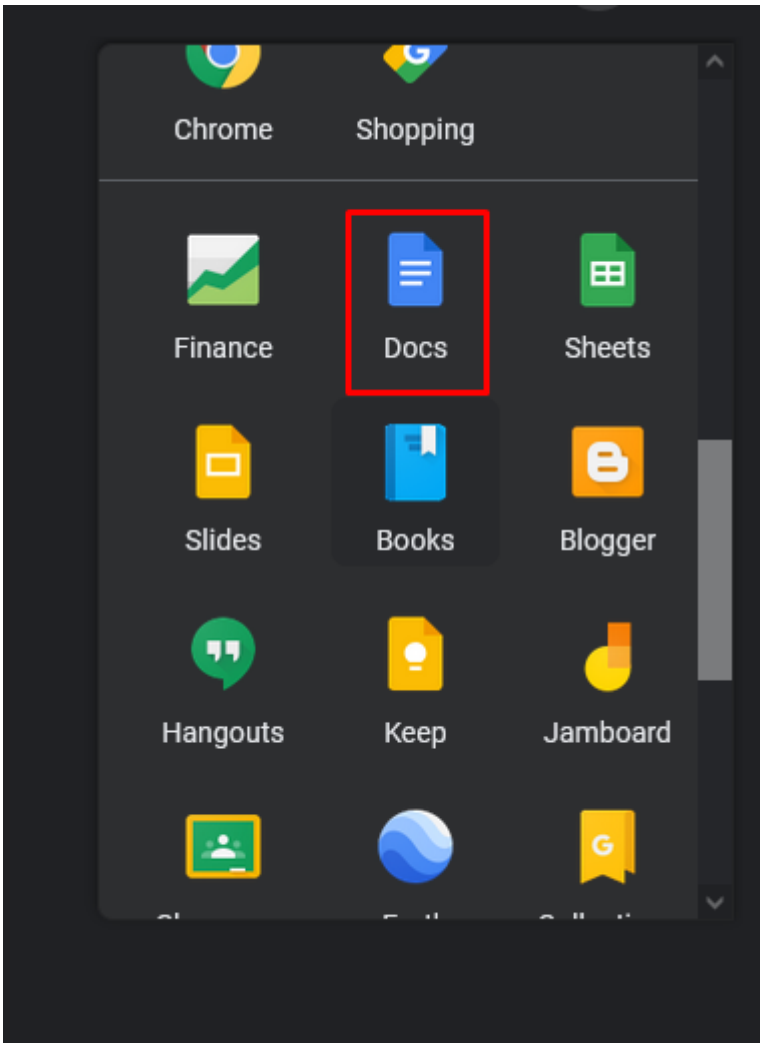
- The entire configuration and spin-up process require comprehensive technical knowledge.
- It has a little lack of training documentation and support.

Q2.Working and Implementation of Software as a service.

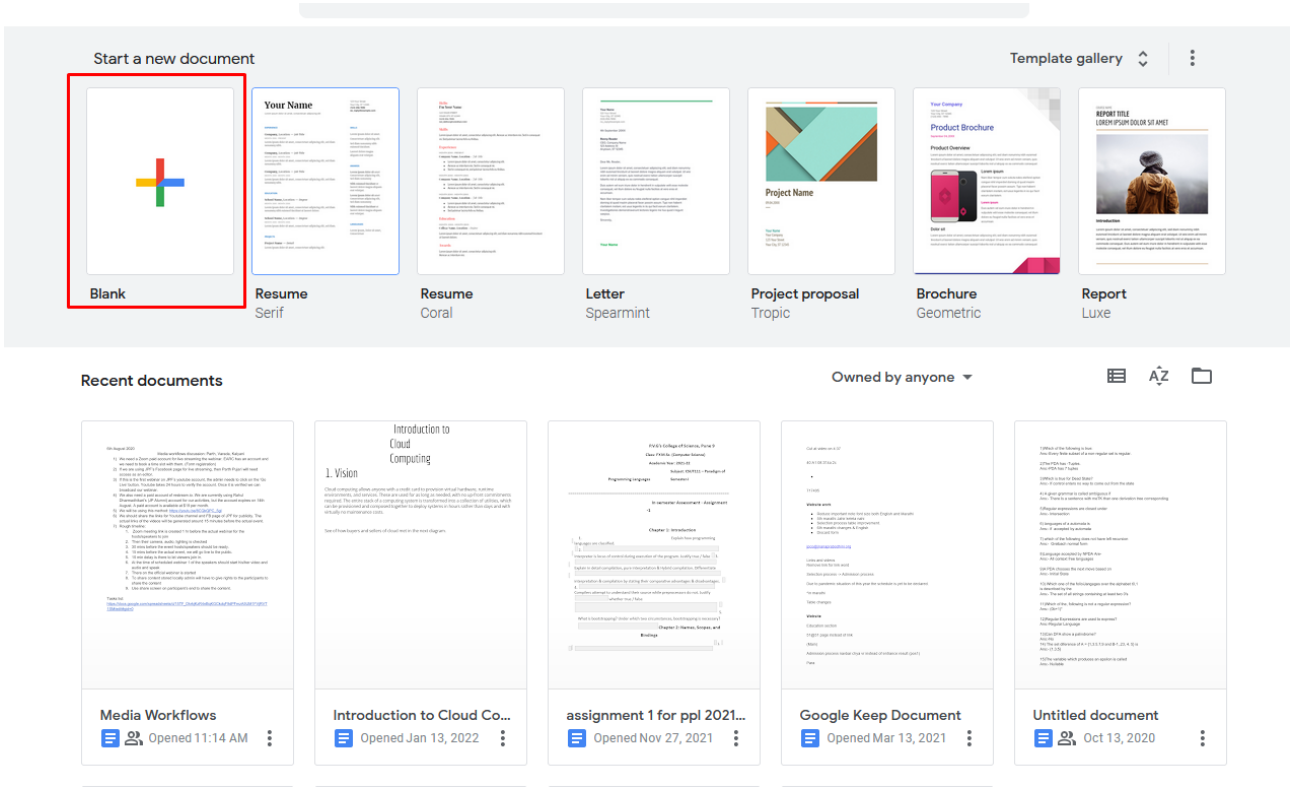
Software as a Service

- Google Drive/ Google Doc/ Google Presentations
- Share screenshots of each step
- Detail out what are pros and cons of it

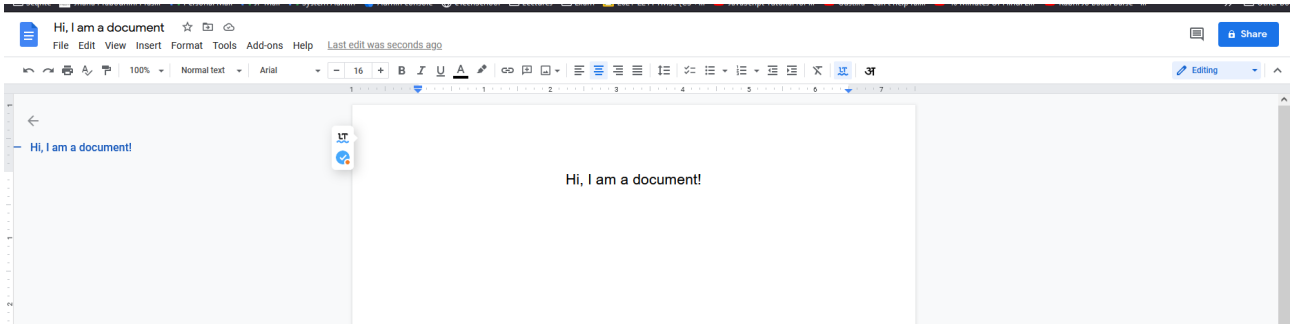
> Sign in your Google Account on any browser & navigate to Docs feature.



> Once inside we can create, view or delete any documents. We will create one by clicking on the blank option.



> You have successfully created a document with Google Doc which is Saas (Software as a service).



SaaS Pros and Cons

Pros

- No Need to Install and Run Applications
- Easy or Instant Updates
- Remote Access
- Scalable Opportunities

Cons

- A lack of control
- Forced Upgrades
- Web Access Necessity
- Varying functionality

Q3. Working and Implementation of Platform as a services.

- Platform as a Service
- Google App Engine
- Lambda Functions on AWS
- Create one of the two above
- Share screenshots of each step
- Detail out what are pros and cons of it

Solved using AWS

Refer answer to Q7

Pros and Cons of Platform as a services

Pros

- Cost Savings
- Streamline Production
- Fast and Flexible Tools
- Access from anywhere
- Reduction of in-house IT resources

Cons

- Incompatibilities with current systems
- Poor access to support
- Necessary third-party services incongruous with current business model
- No way to manage security in-house
- Limitations based on product functionality
- Challenges in transition from one platform to another

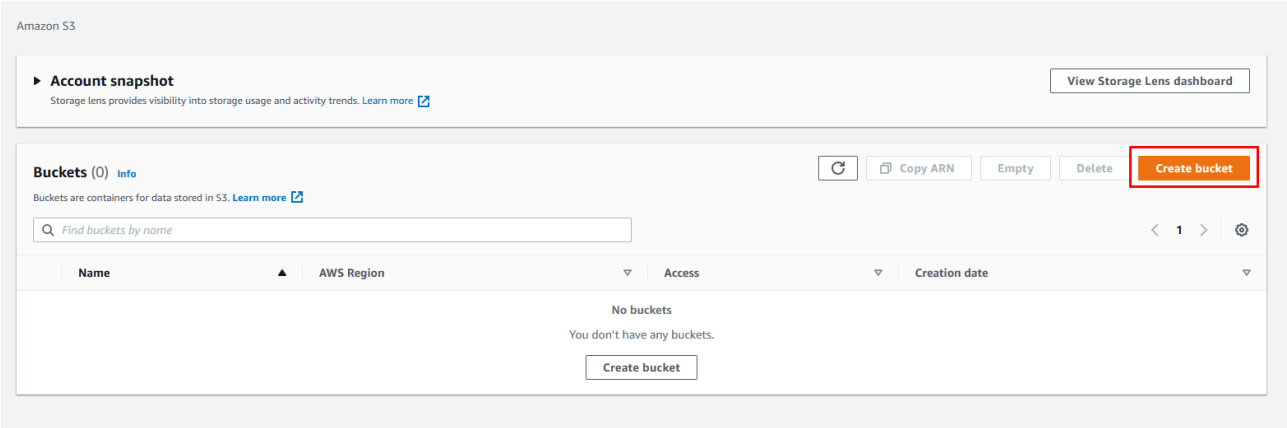
Q4. Practical Implementation of Storage as a Service.

Instructions

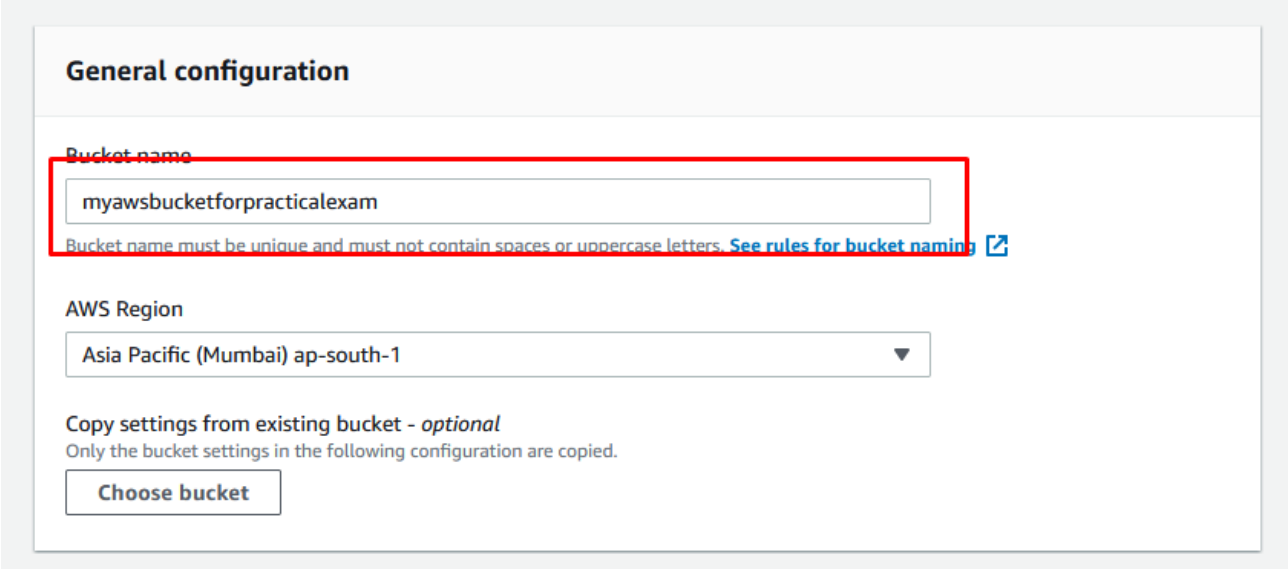
- S3 (AWS)
- Buckets (GCP)
- Share screenshot of each step

Solving with AWS

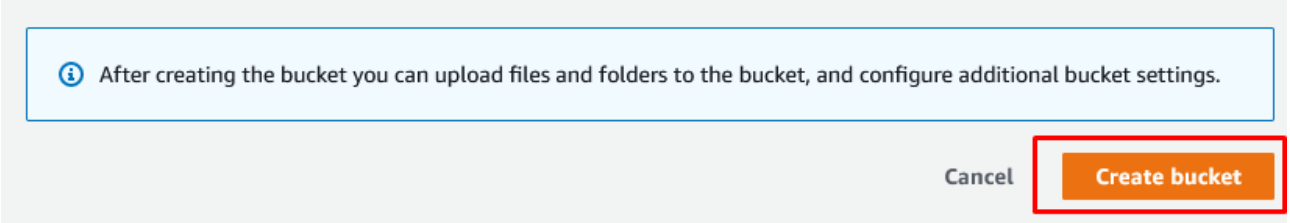
> Login to AWS account > Search for S3 Service > Create Bucket



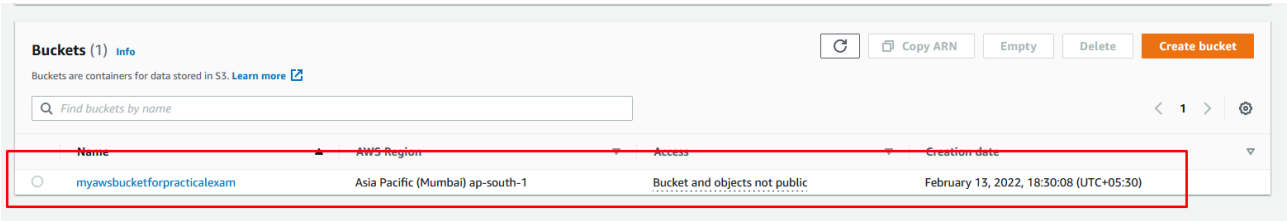
> Give a unique name to the bucket & configure other settings (Optional)



> And then click on create bucket



> You should be greeted with a success message



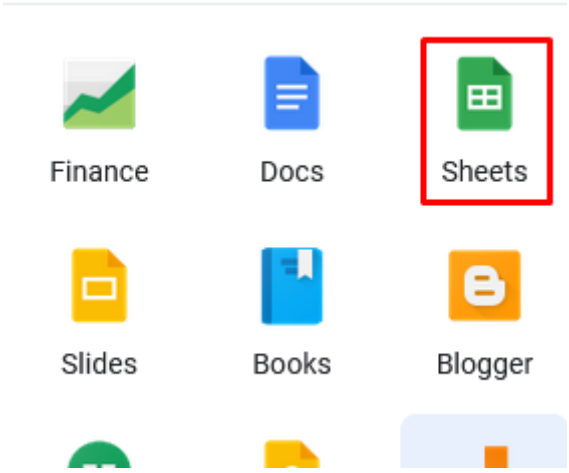
Q5. Working of Google Drive to make spreadsheets and notes

Instructions

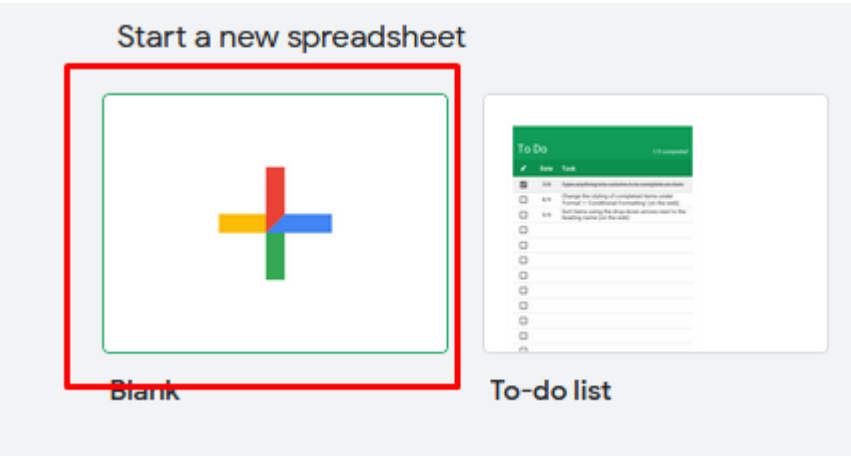
- Goto google drive -> create a spreadsheet or google doc
- Explain which type of example this service is of (SaaS/ PaaS/ IaaS) and why
- Share the details with me

Answer:-

> Login your google account and access the “Sheets” service from the services menu



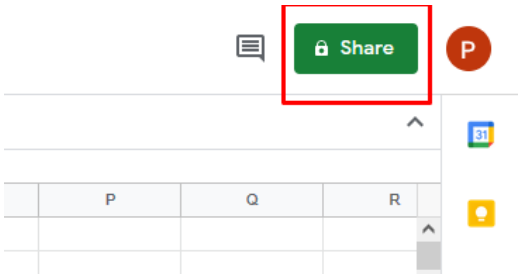
> Click on “Blank” option to simply create a new spreadsheet

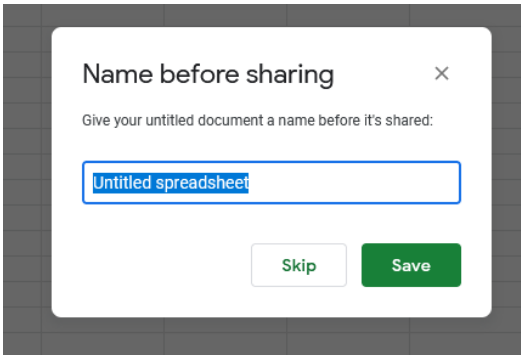


> Your spreadsheet should be created

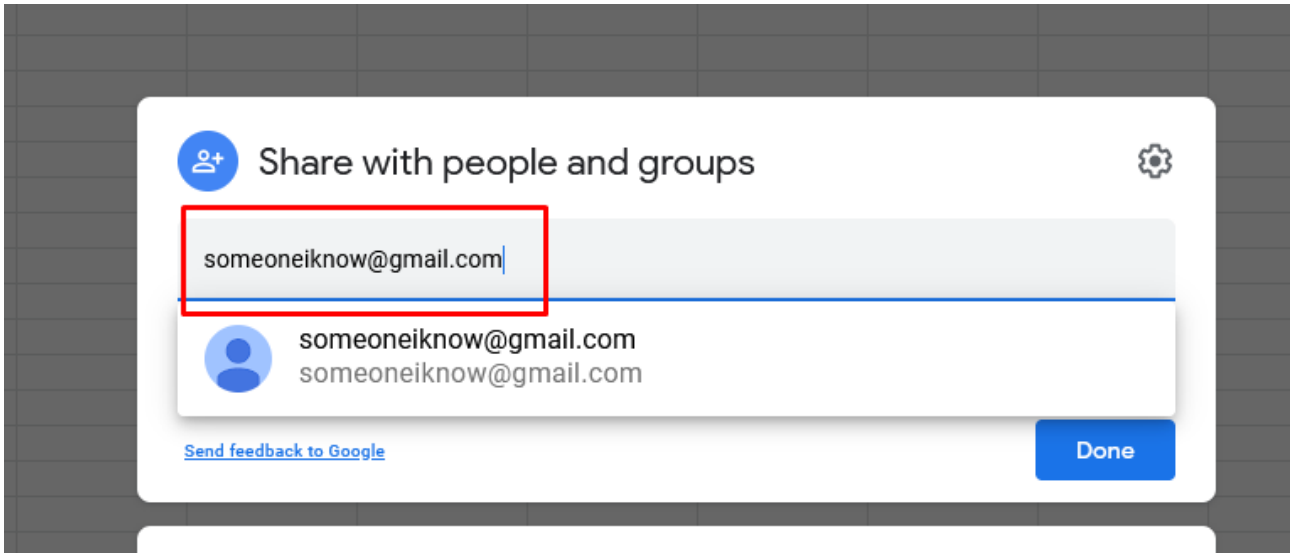
Hi, I am a spreadsheet	
Yes	No
4	5

> To share the spreadsheet simple click on share & provide the spreadsheet a name





> Add emails of people you want to share it with & click on done, it will be shared now.



Google Sheets is a type of SaaS or software as a service provided by Google for it’s users to create, modify and share data over the internet.

Q6. Working implementation of Identity Management

- Okta/ Onelogin platform
- Check Onelogin on youtube steps/ read documentation about it
- Identity management on AWS (IAM)
- Identity management on GCP
- Talk about one of these 3
- Students are expected to share screenshot of each and every step they do

---

6th question will not be assigned

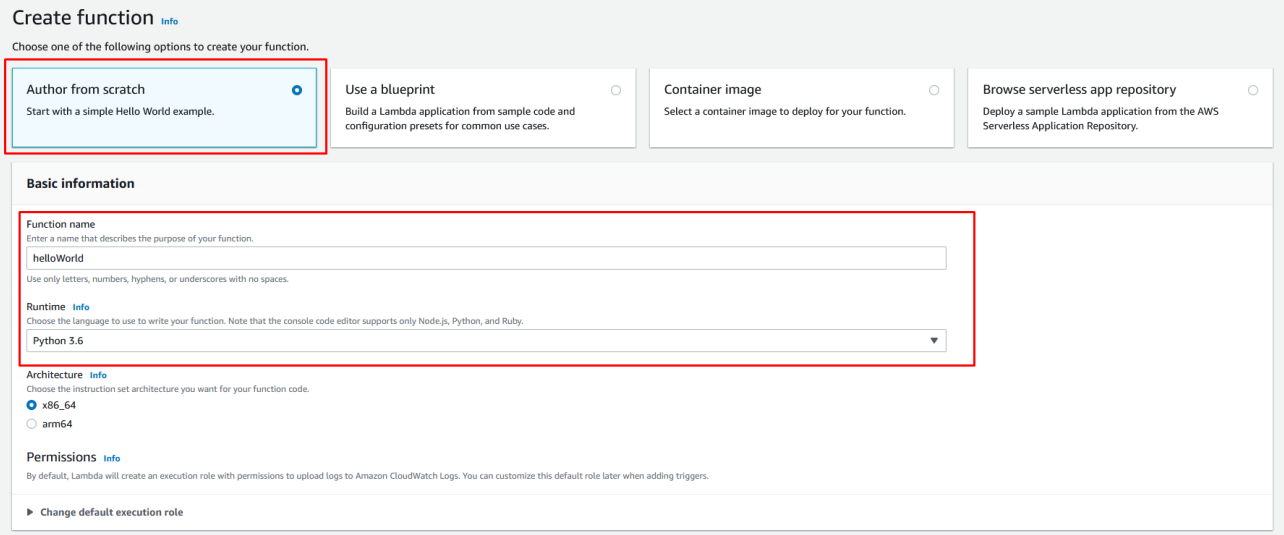
Q7. Program of a web feed

- Specifically talk about IaaS
- On Google Cloud - check cloud functions
- On AWS - check Lambda
- Student should be able to create one of these two and should able to create
- as small program as print “hello world” by creating cloud function/lambda
- Share screenshots of each step

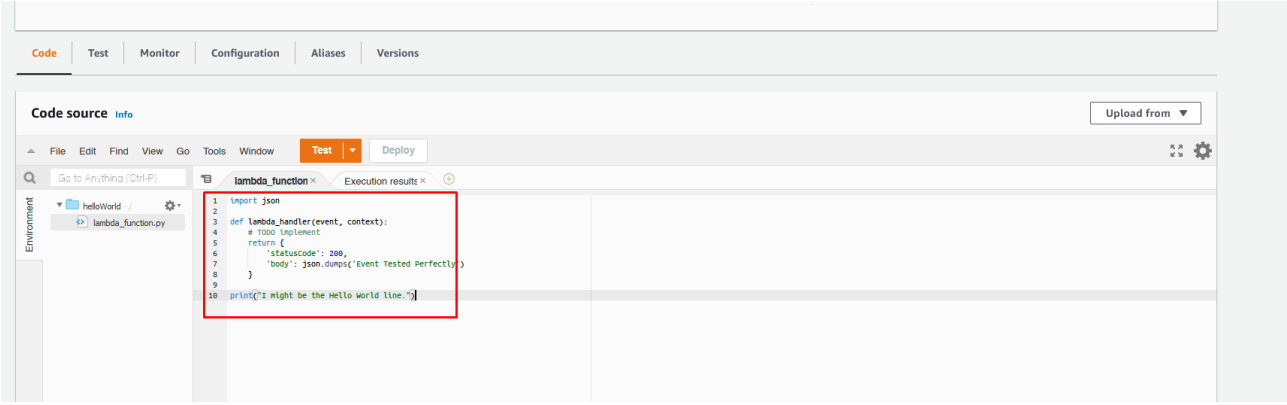
Solving using AWS

> Create a Lambda service instance & choose “From Scratch” option, programming language and other options as required

> Provide a proper name to the function and select “Create Function”.



> Then add the code which is required and select Test
> Provide an event name and then test if the program is working
> Deploy the code and then hit test and check if it is working



Infrastructure-as-a-Service, commonly referred to as simply “IaaS,” is a form of cloud computing that delivers fundamental compute, network, and storage resources to consumers on-demand, over the internet, and on a pay-as-you-go basis. IaaS enables end users to scale and shrink resources on an as-needed basis, reducing the need for high, up-front capital expenditures or unnecessary “owned” infrastructure, especially in the case of “spiky” workloads.

Q8. Execute the step to Demonstrate and implementation of cloud on single sign on.

- Cloud Single Sign on
- Identity management of Google Service - explain it
- Like once you login to Gmail you can access other services of google like
- GDoc/ Google Spreadsheets etc
- So talk about how single sign on is easy to use

Cloud Single Sing-On (SSO)

- Single sign-on (SSO) is a technology which combines several different application login screens into one. With SSO, a user only has to enter their login credentials (username, password, etc.) one time on a single page to access all of their SaaS applications.

SSO is often used in a business context, when user applications are assigned and managed by an internal IT team. Remote workers who use SaaS applications also benefit from using SSO

What are the advantages of SSO?

In addition to being much simpler and more convenient for users, SSO is widely considered to be more secure. This may seem counterintuitive: how can signing in once with one password, instead of multiple times with multiple passwords, be more secure? Proponents of SSO cite the following reasons:

Stronger passwords: Since users only have to use one password, SSO makes it easier for them to create, remember, and use stronger passwords.* In practice, this is typically the case: most users do use stronger passwords with SSO.

*What makes a password "strong"? A strong password is not easily guessed and is random enough that a brute force attack is not likely to succeed. w7:g"5h$G@ is a fairly strong password; password123 is not.

No repeated passwords: When users have to remember passwords for several different apps and services, a condition known as "password fatigue" is likely to set in: users will re-use passwords across services. Using the same password across several services is a huge security risk because it means that all services are only as secure as the service with the weakest password protection: if that service's password database is compromised, attackers can use the password to hack all of the user's other services as well. SSO eliminates this scenario by reducing all logins down to one login.

Better password policy enforcement: With one place for password entry, SSO provides a way for IT teams to easily enforce password security rules. For example, some companies require users to reset their passwords periodically. With SSO, password resets are easier to implement: instead of constant password resets across a number of different apps and services, users only have one password to reset. (While the value of regular password resets has been called into question, some IT teams still consider them an important part of their security strategy.)

Multi-factor authentication: Multi-factor authentication, or MFA, refers to the use of more than one identity factor to authenticate a user. For example, in addition to entering a username and password, a user might have to connect a USB device or enter a code that appears on their smartphone. Possession of this physical object is a second "factor" that establishes the user is who they say they are. MFA is much more secure than relying on a password alone. SSO makes it possible to activate MFA at a single point instead of having to activate it for three, four, or several dozen apps, which may not be feasible.

Single point for enforcing password re-entry: Administrators can enforce re-entering credentials after a certain amount of time to make sure that the same user is still active on the signed-in device. With SSO, they have a central place from which to do this for all internal apps, instead of having to enforce it across multiple different apps, which some apps may not support.

Internal credential management instead of external storage: Usually, user passwords are stored remotely in an unmanaged fashion by applications and services that may or may not follow best security practices. With SSO, however, they are stored internally in an environment that an IT team has more control over.

Less time wasted on password recovery: In addition to the above security benefits, SSO also cuts down on wasted time for internal teams. IT has to spend less time on helping users recover or reset their passwords for dozens of apps, and users spend less time signing into various apps to perform their jobs. This has the potential to increase business productivity.

How does an SSO login work?

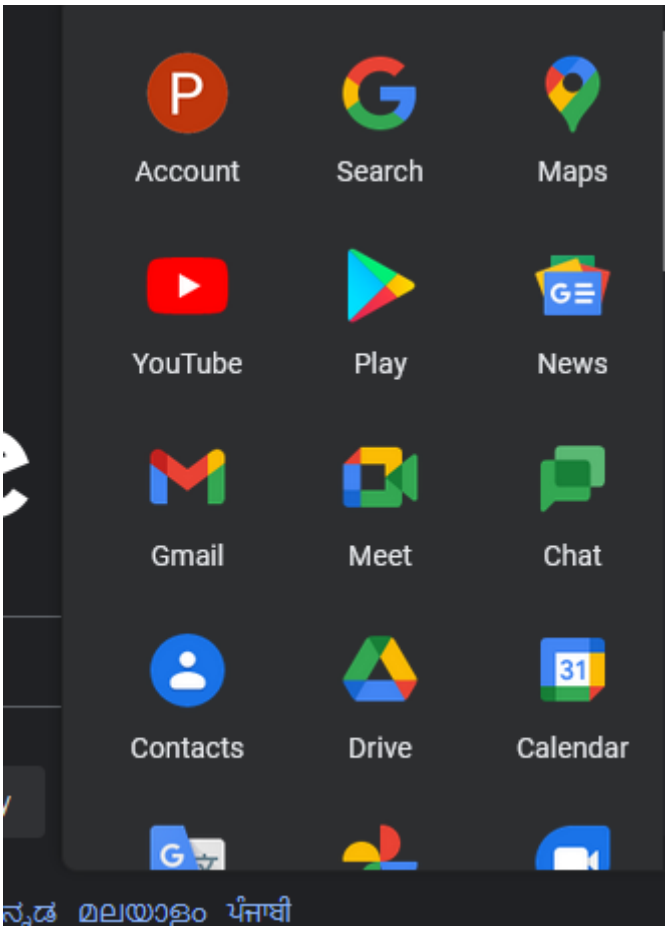
Whenever a user signs in to an SSO service, the service creates an authentication token that remembers that the user is verified. An authentication token is a piece of digital information stored either in the user's browser or within the SSO service's servers, like a temporary ID card issued to the user. Any app the user accesses will check with the SSO service. The SSO service passes the user's authentication token to the app and the user is allowed in. If, however, the user has not yet signed in, they will be prompted to do so through the SSO service.

Using SSO can provide several advantages:

- You enable a better experience for users because they can use their existing credentials to authenticate and don't have to enter credentials as often.
- You ensure that your existing IdP remains the system of record for authenticating users.
- You don't have to synchronize passwords to Cloud Identity or Google Workspace.

Example of Cloud Single Sing-On (SSO)

> Login to Google Account & look up the services



> This is an example of Cloud Single Sing-On (SSO) where the user logs in to one service and is immediate able to user multiple services as user's wish.

Q9. Practical Implementation of cloud security.

- Mention how it works on AWS
  - EC2
  - S3
  - IAM

- Google Drive or any other service of Google
- Facebook groups
- Instagram follow someone

Answer using AWS

When we talk about cloud computing one of the main factors regarding it is Security. If the security conflagrations are not done properly it may a threat to the owner's data.

Considering the service EC2 (Elastic Compute Cloud), AWS provides the admins some powerful tools to tweak any of the security permissions, which maybe with regards to the Network, Hardware or Software of the VM.

In networking for example, admins have an array of options to choose from which increases security and as well as performance of their VM.

Like, admin can set the VM with a custom Network, Subnet and Public IP rather than the default configuration.

Or even admin might wish to add custom IAM roles which further increases the VM's security structure.

Security groups which are a set of firewall rules that control traffic of the VM can also be configured as per the wish of the admin.

Or in S3 admin can block access of our buckets as per our need i.e. Public or Private

And in IAM admin can micro manage permissions for each use as per the need.

So, these are some of the configurations that an admin can do in cloud computing for implementation of a security cloud environment.

Q10. Installing and Developing Application Using Google App Engine.

- Google App Engine (GCP) / Lambda Functions (AWS)
- Student should be able to create one of these 2
- Share screenshots of each and every step

Refer answer to Q7