**Pre-Assessment**

**AWS**

**Q1) Create IAM Policy which grants access to S3 bucket only**

A1) Below are the following steps:

1. Go to your Amazon my account console and click onto Security Credentials
2. Continue to Security Credentials and click on Create Policy
3. Select the Create your own policy option
4. Fill out:
   1. Policy Name
   2. Description
   3. Policy Documents (A JSON doc including fields like Version and Statement Array and inside Statement, we have effect, action , resource)
      1. And inside this, your will tag resource to only one bucket
5. Click on create policy and the policy is created
6. Now create a New Group and set a group name
7. Search for the policy you just created for a single bucket and attach the policy to the group
8. Click on Create Group
9. Select the group created and click on Group Actions
10. Click on add users to the group and add your username
11. You can now use your Access Key ID and Secret Access Key to run restricted to a single bucket

**Q2)**

A2) For an action of EC2 instances using any resource, will be allowed according to the policy (IAM) and for any other action using any resource, this usage will be denied according to the policy.

**Q3) Steps for launching EC2 Instance**

A3) Following are the steps to launch an EC2 instance:

1. Go to AWS Management Console
2. Click on create instance
3. Select the AMI (Amazon Machine Image - OS) required
4. Select the type of instance (for example: free tier based)
5. Specify number of instances required
6. Specify the storage (30 GB by default)
7. Add a tag (key and value – This Tag Instance is used as an identifier to the EC2 Instance)
8. Configure Security Settings
9. Generate a new key pair (which gets stored in a .pem file)
10. Click on Review and Launch
11. Then launch

**Q4) Steps for hosting a Static Website on Amazon S3**

A4) Following are the steps:

1. Name your AWS S3 bucket
2. Configure the S3 bucket for Static Website Hosting
   1. Click on your bucket and click on properties
   2. Click on Static Website Hosting
   3. Select “Use this bucket”
   4. Enter an “Index.html” as the index doc
3. Once the configuration is complete, you will get an S3 website URL
4. For further additions like access grants:
   1. Select Permission
   2. Under Public Access Setting, Click Edit
   3. False tag the Public ACLs and Public Uploading
5. Update the policy
6. Now you need to add a CNAME(Canonical name) record for your bucket URL because you will have to provide it a mapping from your domain name to your S3 Website URL
7. Now comes to part where you need to put everything into your bucket
   1. Click on upload and add files (Index.html)
   2. Similarly upload your permission and policy based documents
8. And finally go and check from the Browser.

**Q5) Steps and create public and private Subnets**

A5) Following are the steps:

1. Select Your VPC and click on “Create VPC“.
2. Give a name for your VPC, mention the IPv4 CIDR block. Click on “Create”.
3. You will get a message saying that the VPC was created along with the VPC ID.
4. For creating the subnets navigate to “Subnets“, in the “Filter by VPC“, select your VPC and then you will see there are no subnets.
5. Create a subnet named Private. Select your VPC, the Availability Zone, and the IPv4 CIDR block. Click on “Create“.
6. You will get a message saying “The following Subnet was created” along with the “Subnet ID“. Click on “Close“.
7. Create a Public Subnet, fill it in with all the relevant details as I did for the creating a Private Subnet. Click on “Create“.
8. You will get a message saying “The following Subnet was created” with the “Subnet ID“. Click on “Close“.
9. Now we have to create an Internet Gateway to make the subnet public.
10. Navigate to Internet Gateways, click on Create “Internet gateway“.
11. Give a name to your Internet Gateway. Click on “Create“.
12. You will get a message saying “The following internet gateway was created” and the “Internet Gateway ID“. Click on “Close“.
13. Just by creating an Internet Gateway won’t suffice the purpose. You have to attach the Internet Gateway to the VPC.
14. Select the VPC for which you want to attach your Internet Gateway. Click on “Attach“.
15. Now as you have attached the Internet Gateway to your VPC, it’s time to make rules for managing traffic using Route Table. Navigate to Route Tables, and click on “Create route table“.
    1. Give a name to your Route table and select the VPC for which the Route table will work. Click on “Create“
    2. .You will get a message “The following Route Table was created” and the “Route Table ID“. Click on “Close“.
16. Now you have a Route table created. Add the routes for managing the traffic. Navigate to “Routes” and click on “Edit routes“.
17. Click on “Add Routes” and mention the destination 0.0.0.0/0 as you want it to be accessible to Public and then select the target as the Internet Gateway that you created earlier. Click on “Save routes“.
18. Now that the rules are added to the Route table, its time to attach it to the Public Subnet. Select the Public Subnet and navigate to Route Table and click on “Edit route table association“.
19. Select the Route table and click on “Save“.
20. You have successfully made the subnet public.
21. This way you can take a long route to create an Amazon VPC with two subnets, a Public and a Private subnet.

**GCP**

**Q1) Steps to create VPC and subnets in GCP**

A1) Following are the steps:

1. Go to the VPC network page in the Google Cloud Console
2. Click on Create VPC
3. Enter a Unique name for your VPC
4. Select a region
5. Choose a custom for the Subnet Creation Mode
   1. Provide a name for the Subnet
   2. Select a region
   3. Enter an IP address range (10.1.2.0/24)
   4. Click on secondary IP address range to provide such
   5. Choose whether to enable private Google access
   6. Choose whether to enable VPC flow log (log record of a sample network that is sent and received by the VM instances
6. To add more subnets, click on the tab and repeat the previous methods
7. Choose dynamic routing mode for VPC network and say create
8. After creating a network, you can create firewall rules

**Q2) Steps to create a service account and add IAM roles which grants access to GCE and GCS only**

A2) Following are the steps:

1. Open Service Account page
2. Click Select a project, choose the project, and click Open.
3. Click Create Service Account.
4. Enter a service account name, description, select a role you wish to grant to the service account, and then click Save.
5. To grant roles to the account
6. Open the IAM & Admin Page
7. Click on select a project, choose the project and click Open
8. Identify the service account to which we want to add roles, click on edit
9. Select the roles (GCE & GCS)
10. Click on Save to apply those roles to the account

**Q3)** Steps to create bucket and transfer files from local to GCS using gsutil

A3)

To create a bucket (these are basic containers that hold your data in the Cloud Storage) using gsutil:

1. Open Terminal on window
2. Use the gsutil mb commands and a unique name to create a bucket
   1. gsutil mb -l us-east1 gs://my-bucket/
3. If successful, the command returns:
   1. Creating gs://my-awesome-bucket/...

To upload/transfer an object into your bucket:

1. Let’s say I want to store an image object in the bucket
2. Right click and save the image
3. Use the gsutil cp command to copy the image from the location where you have saved it to your bucket you just created
   1. gsutil cp Desktop/kitten.png gs://my-awesome-bucket

**Q4) Steps to create GCE VM and deploy nginx**

A4) **NGINX** is open source software for web serving, reverse proxying, caching, load balancing, media streaming, and more.

Steps are as follows:

1. Go to the VM instances page.
2. Click Create instance.
3. Specify a Name for your instance.
4. In the Container section, select the Deploy a container image to this VM instance checkbox.
5. Specify the Container image to use.
   1. For example, you can specify gcr.io/cloud-marketplace/google/nginx1:1.12 to select an NGINX 1.12 container image from Cloud Launcher.
   2. If you use a container image from Docker Hub, always specify the full Docker image name. For example, specify the following image name to deploy an Apache container image: docker.io/httpd:2.4.
6. Optionally, click advanced container options. For more information, see [Configuring options to run your container](https://cloud.google.com/compute/docs/containers/configuring-options-to-run-containers).
7. Click Create to create the instance, boot the instance, and launch the container.

**LINUX**

**Q1) Consider a text file which has multi-lines text, output all the lines which has a specific word and also output the total number of occurrences of that word.**

A1) Here is a Shell Script that can be executed on the text file to know the output:

Script

Echo “Enter file name…”

Read fname;

Echo “Enter search pattern”

Read pattern;

for line in $fname;

do

grep –c $pattern line;

done

**Q2)** Search for all the files that have a ‘.txt’ extension in the current working directory

A2) Linux provides us with a simple commands to find all files that have a .txt extension in the current working directort

find . -type f -name "\*.txt" ( this is reliable, however you can also use locate to have faster outputs\_

**Q3) Execute a specific command in all the subdirectories whose names starts with “aws”. For example, your sub-directories are “aws\_1”, “aws\_2”, “gcp\_1”, “aws\_3”., Execute “pwd” command in the directories “aws\_1”, “aws\_2” and “aws\_3”**

A3)

Script:

for d in ./\*/ ;

do

result=${d##\*/}

if [“$result” == “aws%” ]

then

pwd "$d"

fi

done

**Q4) Consider a text file and replace a specific word with any word of your choice**

A4)

Sed is a Stream Editor used for modifying the files in unix (or linux). Whenever you want to make changes to the file automatically, sed comes in handy to do this.

Text file:

hello world

hello everyone

Syntax: sed -i 's/original/new/g' file.txt

• sed = Stream EDitor

• -i = in-place (i.e. save back to the original file)

The command string:

• s = the substitute command

• original = a regular expression describing the word to replace (or just the word itself)

• new = the text to replace it with

• g = global (i.e. replace all and not just the first occurrence)

• file.txt = the file name

Command used: sed -i ‘s/hello/hi/g’ file.txt

Output:

hi world

hi everyone

**Q5) How to find a specific file in the system**

A5)

**Locate command:**

The locate command is faster than the find command because it uses a previously built database, whereas the find command searches in the real system, through all the actual directories and files. The locate command returns a list of all path names containing the specified group of characters.

The database is updated periodically from cron, but you can also update it yourself at any time so you can obtain up-to-the-minute results. To do this, type the following command at the prompt:

Command: sudo updatedb

If you want to find all files or directories that contain exactly and only your search criteria, use the -b option with the locate command, as follows.

Command: locate -b ‘\mydata’

The backslash in the above command is a globbing character, which provides a way of expanding wildcard characters in a non-specific file name into a set of specific filenames. A wildcard is a symbol that can be replaced by one or more characters when the expression is evaluated. The most common wildcard symbols are the question mark ( ? ), which stands for a single character and the asterisk ( \* ), which stands for a contiguous string of characters.

**Find Command:**

The “find” command allows you to search for files for which you know the approximate filenames.

To find files that match a specific pattern, we can use the -name argument. You can use filename metacharacters (such as \* ), but you should either put an escape character ( \ ) in front of each of them or enclose them in quotes.

For example, if we want to find all the files that start with “pro” in the Documents directory, we would use the cd Documents/ command to change to the Documents directory, and then type the following command:

Command: find . -name pro\\*