FAQ Document: Course 1, Module 4: Working with AWS

Course 1, Module 4: Working with AWS Session Session 1 - AWS CLI		
SN	**Question**	**Answer**
1	AWS CLI error on EC2 instance	Please perform **sudo apt-get update** **sudo apt-get install awscli** If you cannot perform the above functions, then you can download AWS CLI as below and install it manually $ curl "https://awscli.amazonaws.com/awscli-exe-linux-x86_64.zip" -o "awscliv2.zip" `Further reference -->` https://docs.aws.amazon.com/cli/latest/userguide/install-cliv2-linux.htm
2	Not able to create user from CLI	First create the role and assign the permission/policy to this role. aws iam attach-role-policy --role-name role1 --policy-arn:aws:iam::014382703886:policy/policy1
3	How to create role and policy through CLI?	https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_policies_actions-resources-contextkeys.html if you are looking for format to write policy, below is simple one { "Version" : "2012-10-17" #This is version of aws language syntax rules "Statement": #Write your statement to deny or allow access to resource this is mostly nested list [

		{
		"Effect" : "Allow/Deny" , #Effect tells to allow or deny access to actions
		"Action" : "s3:*", #What actions to perform on defined resource. In this case list, delete, copy etc.,
		"Resource" : "*" ,#Resource ARn if you want to specify any resource in particular
		}
		]
		}
		Once you are done with policy definition, you can verify it with below.
		https://jsonlint.com/
		Once defined, save it into some file and attach it to role
		aws iam create-policy --policy-name policy1 --policy-document file://test.json
		aws iam create-role --role-name role1 --assume-role-policy-document file://test_role.json

4	What is the maximum number of Access Keys we can generate for a given user in IAM?	You can have a maximum of two **access keys for a IAM user**. This allows you to rotate the active keys according to best practices. Please check this link below. https://docs.aws.amazon.com/IAM/latest/UserGuide/reference_iam-limits.html
Course 1, Module 4: Working with AWS Session Session 3 - Applications in AWS		
1.	Connecting to Jupyter Notebook to instance Error: "ssh: Could not resolve hostname i: No such host is known." and unable to connect	Make sure you are running the below command on a command prompt on your local machine and not on EC2. instance. **ssh -i "keypair.pem" -N -f -L 8888:localhost:8888 ec2-user@<ec2-public-ip-address>**

	the jupyter notebook.	check if port 8888 is free and no application is running on it. Try running the below command. **lsof -i :8888** This will let you know if anything is running on port 8888. You can also try another command; **netstat -lep --tcp** This will give you the list of ports which are currently occupied and listening. Stop it from listening to other applications on your machine then go ahead. **Note :** If you have your Jupyter Notebook launched on your local machine, that takes up port 8888 by default. So close it first and then try the port forwarding.

2.	NoCredentialsError: Unable to locate credentials
	When i am executing "response = s3.list_buckets()" getting error as 'Unable to locate credentials':
		Please attach the IAM role with s3fullacess to ec2 instance before access the bucket from jupyter server.
		1. Create role and assign **s3fullaccess** permission to this role.
		2. Go to ec2 dashboard> select ec2 instance> Action> instance setting> attache/replace IAM> attach role
		3. Then restart the jupyter kernel.
		import boto3
		s3= boto3.client('s3')
		response = s3.list_buckets()
		print(response)