**Creating New Account and IAM settings**

1. IAM is not region specific, it is universal. Any change done on IAM console will be applicable to all the regions.
2. Aws has a default region US-East (N.Virginia)
3. Aws allows you to have access to your own IAM. You will get an account id as "[https://29\*\*\*\*\*\*\*\*\*\*.signin.aws.amazon.com/console](https://29**********.signin.aws.amazon.com/console)", You can change it to your application or company name. This must be unique.
4. MFA - Multi Factor Authentication, for Root account which has access to all services in your AWS account. There are 2 types of MFA:
5. U2F security keys generate a response when you tap the device. The user does not manually enter a code on the sign-in screen.
6. Virtual and hardware MFA devices generate a code that you view on the app or device and then enter on the sign-in screen.
7. After setting up MFA, when you will login to your aws root account, it will take you to another window in which you will have to authenticate using Google authenticator.
8. Create a user with in: \*\*\*\*\*\* and pw: \*\*\*\*\*\*\*\*.  Secret Access Key ID: "\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*" Password: "\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*" will be something like this.
9. You should always recreate access key and secret key after some days like 10-15 days.

**EC2 -Elastic Computing Cloud**

1. Default VPC:
   1. Every AWS account created after Dec. 4, 2013 supports VPCs and these accounts are assigned a default VPC in every AWS Region.
   2. These default VPCs are designed to make it easy for AWS users to set up networking for their EC2 instances.
2. **Step1: *Choose an AMI*** (Amazon Machine Image). An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance.
3. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.
4. **Step2: *Select AMI Type***. AMI Types are defined as per the need of the user. The type could be General purpose, compute optimized, GPU graphics, Memory optimized and storage optimized etc.
5. We are selecting General Purpose t2.micro which is Free tier eligible.
6. **Step3: *Configure Instance Details****.* You can choose to provide multiple number of instances. By default it is 1.
7. Purchasing Option: You have the option to request Spot Instances and specify the maximum price you are willing to pay per instance hour. If you bid higher than the current Spot Price, your Spot Instance is launched and will be charged at the current Spot Price. Spot Prices often are significantly lower than On-Demand prices, so using Spot Instances for flexible, interruption-tolerant applications can lower your instance costs by up to 90%.
8. If you select spot instance, it will give your information about current price as per availability zone. You will need to provide maximum price you are willing to pay.
9. Network will let you select your VPC, you can create your own VPC and assign ec2 instance to that or you can select default Virtual Private Cloud.
10. Subnet we will select the default one. No preference. You can also select default subnet region specific.
11. Auto assign public IP – select Use subnet setting. Requests a public IP address from Amazon's public IP address pool, to make your instance reachable from the Internet.
12. In most cases, the public IP address is associated with the instance until it’s stopped or terminated, after which it’s no longer available for you to use. If you require a persistent public IP address that you can associate and disassociate at will, use an Elastic IP address (EIP) instead. You can allocate your own EIP, and associate it to your instance after launch.
13. Do not assign any role to your ec2 instance for now.
14. Shutdown behavior: Specify the instance behavior when an OS-level shutdown is performed. Instances can be either terminated or stopped.
15. Enable Termination Protect: You can protect instances from being accidentally terminated. Once enabled, you won't be able to terminate this instance via the API or the AWS Management Console until termination protection has been disabled.
16. Monitoring: Monitor, collect, and analyze instance metrics through Amazon CloudWatch. The default is free, basic monitoring, where data is available in 5-minute periods. You can enable detailed monitoring, where data is available in 1-minute periods. Additional charges are applicable for this.
17. Tenancy: You can choose to run your instances on physical servers fully dedicated for your use. The use of host tenancy will request to launch instances onto Dedicated hosts
18. User Data: You can specify user data to configure an instance or run a configuration script during launch. If you launch more than one instance at a time, the user data is available to all the instances in that reservation.
19. ***Step 4: Add Storage***.You will have a default storage device for your ec2 instance.
20. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes.
21. The default root volume of EC2 has a checkbox selected by default which says the volume will be deleted when you terminate your EC2 instance.
22. The root volume does not have encryption by default.
23. You can select the volume type when you are using a new volume, there are 2 SSDs and 3 Magnetic disk options available.
24. ***Step 5: Add Tags***. A tag consists of case sensitive key-value pair. Tags have the basic defined rule, you can add name, Environment type (like Dev, Cert, Prod).
25. ***Step 6: Configure Security Group***. Security Group is a set of firewall rules to control the traffic for your instance.
26. When you launch an instance, you can specify one or more security groups; otherwise, we use the default security group. You can add rules to each security group that allow traffic to or from its associated instances.
27. You can modify the rules for a security group at any time; the new rules are automatically applied to all instances that are associated with the security group.
28. Create a new security group and assign it to the Ec2 instance. You can name it as LinuxEC2. Give type as SSH as it’s a linux machine. Protocol is TCP, Port no is 22. In source you can define Custom/Anywhere/My IP which will provide access to either a custom IP or range of IPs, anywhere means giving access to the whole world and My IP will keep it private.
29. ***Step 7: Review instance launch***. Will allow you to review your instance settings and then launch it.
30. When Launching EC2 instance, you will get a popup to select an existing key pair or create a new pair, which will be your EC2 Public key. You can download the .pem key and Launch the instance.
31. It will take some time to be up and running.

**Connecting to a Linux instance**

1. Use PuttyGen to generate the ppk from the pem key generated while launching ec2 instance.
2. Copy EC2 instance’s public ip address from aws ec2 instances description, Go to putty, in host name type “ec2-user@” and Paste the public ip. Default port is 22, keep it as is. Connection type is SSH.
3. Navigate to SSH in left panel, then click on Auth, upload the .ppk file in it.
4. Go to save session, give relevant session name and save it. select the session, load it and open. It will connect to your EC2 instance.
5. Go to aws console, click on ‘Actions’ drop down, go to instance state and Terminate. It will shut down the system.

**Connecting to a Windows instance**

1. Go to aws console’s EC2 instances list, select windows instance. Copy the public ip address and save it.
2. Go to actions, click on ‘Get Windows Password’. Click on browse and upload the public key which is a .pem file and click on decrypt password.
3. You will get a popup saying, ‘Password Decrypted Successful’. Public DNS, username and password will be provided.
4. Copy Public DNS. Go to Run on window start menu, type ‘mstsc’, it will open Remote Desktop Connection. Paste the Public DNS in Computer name.
5. Provide username and password provided to you. You will connect to your windows EC2 instance using Remote Desktop Connection.

**Security Groups**

1. Security Group is a set of firewall rules to control the traffic for one or more instances.
2. When you launch an instance, you can associate one or more security group(s) with the instance.
3. You add rules to each security group that allow traffic to and from its associated instances.
4. You can modify the rules of security groups later, the new rules are automatically applied to all instances associated with the security groups.

What is the range of IP addresses you can select in a VPC?

Max 16 and Min 28