A Few AWS Interview Questions!

Question 1) What is the difference between HVM and PVM?

Answer: AWS used XEN as a hyper-visor layer to spin up all the virtual machines.

Linux Amazon Machine Images use one of two types of virtualization: paravirtual (PV) or hardware virtual machine (HVM). The main difference between PV and HVM AMIs is the way in which they boot and whether they can take advantage of special hardware extensions (CPU, network, and storage) for better performance.

AWS recommends use of current generation instance types and HVM AMIs when you launch your instances

S. No.	HVM	PVM
1	Hardware Virtual Machine	Paravirtual Machine
2	HVM AMIs are presented with a fully virtualized set of hardware and boot by executing the master boot record of the root block device of your image.	PV AMIs boot with a special boot loader called PV-GRUB, which starts the boot cycle and then chain loads the kernel specified in the menu.lst file on your image.
3	HVM virtualization type provides the ability to run an operating system directly on top of a virtual machine without any modification, as if it were run on the bare-metal hardware.	Paravirtual guests can run on host hardware that does not have explicit support for virtualization
4	HVM guests, unlike PV guest, can take advantage of hardware extensions that provide fast access to the underlying hardware on the host system.	They **cannot** take advantage of special hardware extensions such as **enhanced networking or GPU processing**.
5	All current generation instance types support HVM AMIs.The CC2, CR1, HI1, and HS1 previous generation instance types support HVM AMIs	C3 and M3 current generation instance types support PV AMIs. The C1, HI1, HS1, M1, M2, and T1 previous generation instance types support PV AMIs.

Question 2) What is the difference between Security groups and NACLs?

Answer: With AWS, Once can harden their instances in 3 ways, It can be OS level firewall, Security and Network Access Control Lists (NACLs). Both security groups and NACLs together helps to build a layered network defense

S. No.	Security Group	NACLs
1	It acts at instance level	It acts at subnet level. It is a numbered list of rule and lowest rule number will have the highest priority
2	It allows to add or remove rules for both ingress and egress traffic to	A Network ACLs (NACLs) is a layer of security for the VPC that acts as a firewall

	the instance	for controlling traffic in and out of one or more subnets
3	It comes with default allow all egress and no ingress traffic	Default ACL allows all inbound and outbound traffic. Newly created ACL denies all in and out traffic
4	Only allow rules, no deny rule	NACLs has separate inbound and outbound rule. Each rule can either allow or deny the traffic
5	These are stateful - Return traffic is automatically allowed, regardless of any rule	These are stateless - Return traffic must be explicitly allowed by rules

Also, a subnet can only be associated with 1 NCAL and if not associated explicitly would be associated implicitly with the default NACL

Question 3) How many IAM keys can a user have?

Answer: At time a user can have only 2 active IAM access and secret key.

Question 4) What will you do if a server in your environment gets compromised and you have your AWS keys on that?

Answer: Firstly, I'll stop the instance so that the attacker will not be able to reach to other instances or if there is no critical workload I will terminate it (Assuming I have a latest AMI of that instance).

Secondly, as there is access key configured on the server. I'll inform the team about the incident, create a new access and secret key, replace the existing key if it is used somewhere else and revoke the old key.

Also, I'll make sure that going further the keys should not be used on the instances and this can be achieved using the IAM roles.

Question 5) How will you revoke the access keys?

Answer: Console > IAM Consoles > User > Security credentials > make inactive

Question 6) How will you do hardening of a new AWS account?

Answer:

1) Never share the root password with any user and disable the root access keys
2) Create IAM groups and assign required policies
3) Create IAM users and add then into respective groups. Make sure all will have only the required access no additional access will be given to any user without approvals
4) Set password retention policy
5) Always allow only required rule in NACLs and Security groups

Question 7) How do you configure a public and private subnet in VPC?

Answer:

1) Create VPC, Create 2 subnets, create Internet gateway and assign IGW to the VPC
2) To create a public subnet: Create a route table associate the subent and create a route using IGW ARN
3) To create a private subnet: Create a NAT gateway, create a route table, associate the subnet and create a route using NAT ARN

Question 8) How do you update an new AMI in autoscaling group?

Answer: Once a launch configuration group is created you cannot modify it. In order to change the AMI you have to create a new launch config group. After creating the new launch configuration group attach that to the autoscaling group and terminate the old instances one by one.

Question 9) Route53 routing policy use cases

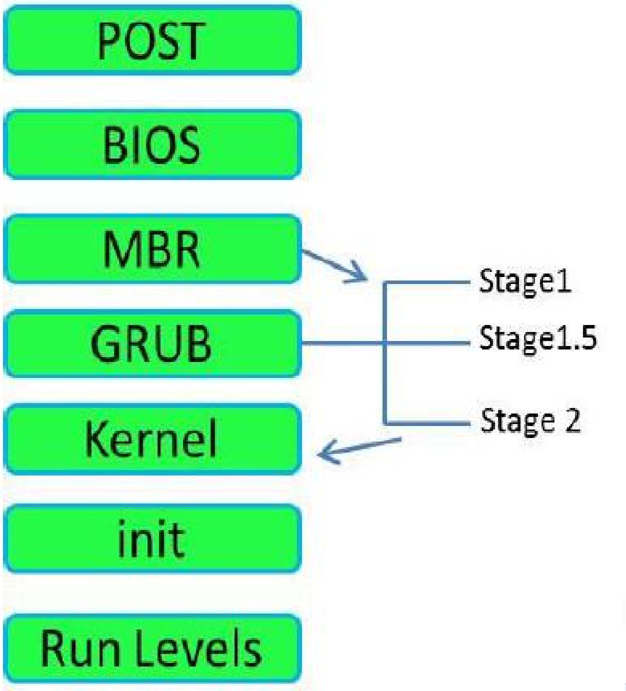
Answer: AWS Route53 is a fully manged DNS service, it allows to host/buy domain with AWS. Route53 support different routing policy to direct your traffic to your resources. Policies are

Read more here:
http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/routing-policy.html

Question 10) What are the types of pricing models for EC2 instances and what is the difference between them?

Answer: Reserved, Spot and On-demand instances.
Read more here: https://aws.amazon.com/ec2/pricing/

Question 11) Linux both process



Question 12) How will you configure a password less access between two servers?

Answer:

1) Create a key pair on both the servers using **ssh-keygen -t rsa**
2) Create a .ssh/autorized_keys on both the servers
3) Copy the key of server A on the above path of server B and vice versa
4) Give permission chmod -R 700 to .ssh directory
5) Give permission chmod -R 600 to authorized_keys file

Question 13) How will you configure password login on your AWS EC2 instance?

Answer:

1) Create a user, assign a password to it
2) Make entry in /etc/sudoers.d/
3) Edit /etc/sshdconfig file and uncomment Password Authentication Yes

Question 14) You have two servers (A & B) in your AWS account and you have allowed ssh access between both of them, but you are not able to ping each other. What could be issue and how do you resolved it?

Answer: ICMP protocol is not allowed between them allow the same in security group. In case ICMP are allowed in security groups. Then allow ICMP on the NACLs

Question 15) Where do you define your subnets while configuring autoscaling?

Answer: You neither define subnets while configuring launch configuration nor while configuring auto-scaling. Subnets are defined while creating ELB.

Question 16) How do you see and retrieve the files from Glacier?

Answer: Amazon Glacier provides a management console, which you can use to create and delete vaults. However, you cannot download archives from Amazon Glacier by using the management console. To download data, such as photos, videos, and other documents, you must either use the AWS CLI or write code to make requests, by using either the REST API directly or by using the AWS SDKs.

Question 17) Difference between AMI and Snapshot?

An Amazon Machine Image (AMI) is a template that contains a software configuration (for example, an operating system, an application server, and applications). From an AMI, you launch an instance, which is a copy of the AMI running as a virtual server in the cloud. Whereas for Snapshots You can back up the data on your EBS volumes to Amazon S3 by taking point-in-time snapshots. Snapshots are incremental backups, which means that only the blocks on the device that have changed after your most recent snapshot are saved. When you delete a snapshot, only the data exclusive to that snapshot is removed.

Question 18) What is a Bastion host?

Answer: Bastion are like jump servers to allow access to the host in the private subnet.

The configurations usually work like below :-
1. Bastion needs to configured to allow inbound ssh access (TCP – 22) only from restricted ips (103.252.24.158/32, 32 here indicates exact IP address)

2. Instances in Private subnet then allow inbound ssh access only from bastion host

Question 19) What is DR, its important aspect you consider while implementing DR strategy and what are the kind of DR strategies available?

Answer: This article covers almost everything:

Question 20) I have created an EBS volume but I'm not able to attach to to my instance. What could be the issue and how to resolve it?

Answer: Possibly, the instance and volume are in different AZs. Create a snapshot of that volume, create the volume using the snapshot in the same region where the EC2 instance is launched and attach it to the instance.

Question 21) How do I change an EBS volume type and increase a volume size?

Answer: Create a snapshot of that volume. Create a new volume using that snapshot,while you create a new volume you'll get an option to select volume type and change disk size. However, you cannot reduce the size.