Cloud Guru

Practice Test

1. You can attach a network interface to an instance when it's running (hot attach), when it's stopped (warm attach), or when the instance is being launched (cold attach).
2. You can have up to five read replicas per master, each with its own DNS endpoint.
3. Multi-AZ deployments have synchronous replication (Non-Aurora) and asynchronous replication (Aurora)
4. Amazon Kinesis Data Firehose is the easiest way to load streaming data into data stores and analytics tools. It can capture, transform, and load streaming data into Amazon S3, Amazon Redshift, Amazon Elasticsearch Service, and Splunk, enabling near real-time analytics with existing business intelligence tools and dashboards you’re already using today.
5. The default configuration of the default NACL is Allow, and the default configuration of a custom NACL is Deny.
6. By default, each custom network ACL denies all inbound and outbound traffic until you add rules.
7. Your VPC includes a default security group. You can't delete this group, however, you can change the group's rules.
8. The default network ACL is configured to allow all traffic to flow in and out of the subnets with which it is associated. You are able to add and remove your own rules from the default network ACL. However, each network ACL also includes a rule whose rule number is an asterisk. This rule ensures that if a packet doesn't match any of the other numbered rules, it's denied. You can't modify or remove this rule.
9. To enable access to or from the internet for instances in a subnet in a VPC, you must do the following:
   1. Attach an internet gateway to your VPC.
   2. Add a route to your subnet's route table that directs internet-bound traffic to the internet gateway. If a subnet is associated with a route table that has a route to an internet gateway, it's known as a public subnet. If a subnet is associated with a route table that does not have a route to an internet gateway, it's known as a private subnet.
   3. Ensure that instances in your subnet have a globally unique IP address (public IPv4 address, Elastic IP address, or IPv6 address).
   4. Ensure that your network access control lists and security group rules allow the relevant traffic to flow to and from your instance.
10. Max 5 security group in an instance
11. CloudWatch cannot work with SES
12. Bypass internet- direct connect
13. We can perform both read and write operation when snapshot is being created
14. AWS Managed VPN lets you reuse existing VPN equipment and processes, and reuse existing internet connections. It supports static routes or dynamic Border Gateway Protocol (BGP) peering and routing policies.
15. The Reserved Instance Marketplace is a platform that supports the sale of third-party and AWS customers' unused Standard Reserved Instances

















































































































