AWS Services and General AWS Knowledge:

3. What is the AWS Shared Responsibility Model, and how does it relate to security?

security and compiiancis shared responsibility between AWS and the customer, AWS protects the infrastructure that runs all of the services offered known as security of the cloud

4. Describe the AWS Well-Architected Framework and its pillars.

operational excellence
security
reliability
performance efficiency
cost optimisation
sustainability

when architecting technology solutions if you neglect the 6 pillars it can become challenging to build a system that delivers on your expectations and requirements

5. What is the AWS Free Tier, and what services are available under it?

free tier allows you to access ec2, s3, vpc and lambda services for free at a very low configuration level. this is at no cost to you but should you choose higher resources then you would enter into a pay as you go model

free tier is available for 12 months

Amazon EC2 (Elastic Compute Cloud):

6. What is Amazon EC2, and how does it work?

EC2 (elastic compute cloud) is a web service that provides secure, resizable compute capacity in the cloud

7. What are EC2 instances, and how are they classified based on instance types?

EC2s are virtual servers and they can be classified on their characteristics such as cpu, memory, storage and networking capacity.
8. How do you choose the right EC2 instance type for a specific workload?

you need to gather details about the system requirements of the application or software that you plan to run

9. What is the significance of the Amazon Machine Image (AMI) in EC2?

the AMI is the operating system you choose to use for your instance

10. Explain the difference between on-demand, reserved, and spot instances in EC2.

on demand - available for purchase and deployment as and when needed
Also, On-Demand Instances enable you to start, stop, reboot, pause, hibernate, or terminate an instance or virtual server whenever you choose.

spot instance - is a type of compute capacity that a cloud service provider offers at a steep discount whenever it has excess compute capacity. Yet, you can only purchase Spot Instances if they are available in your desired region and availability zone

reserved instance - Reduce your Amazon EC2 costs by making a commitment to a consistent instance configuration, including instance type and Region, for a term of 1 or 3 years.

Cost Optimization:

11. What strategies can you employ to optimize costs when using AWS resources?

Take advantage of volume pricing tiers and bundled discounts. Save even more when combining usage across accounts with consolidated billing. Stop paying for resources during non-operating hours with Instance Scheduler on AWS for EC2 and Amazon RDS instances.

12. How can you schedule EC2 instances to automatically start and stop during non-business hours to save costs?

you can use aws lambda to schedule an instance to spin up or down for when you require it navigate to cloud watch, click on rules to create a rule and under event source create a shecdule. set your cron expression for when you want to start your EC2 instances

13. Describe the AWS Cost Explorer and how it can help analyze cost trends.

aws cost explorer is a tool that enables you to view and analyse your costs and usage. you can explore you usage and costs using the main graph.

14. What is AWS Trusted Advisor, and how does it assist in cost optimization?

AWS trusted advisor provides recommendations that help you follow best AWS practices. trust advisor evaluates your account by using checks these checks optimise your infrastructure, improve security, performance and reduce costs.

15. How can you identify and terminate underutilized EC2 instances?

trusted advisor lets you inspect your environment and identify idle and under-utilised resources.

Amazon Route 53 (DNS Service):

16. What is Amazon Route 53, and what are its primary use cases?

route 53 is a DNS (domain name service) assign ip addresses and domain names

17. Explain the difference between a Route 53 Alias record and a CNAME record.

an alias record can map one dns name to another amazon route 53 dns name. amazon route 53 name record point to any dns record hosted anywhere.

18. How do you configure health checks in Route 53 for high availability?

log into route 53 console, click on health checks and then on create health check set the name of your health check and provide down name.

19. What is the purpose of the Amazon Route 53 Resolver service?

resolver provides a robust toolset for dns query resolution across aws, the internet and on premises networks with secure control over your amazon vpc dns.

20. Describe the benefits of using Route 53 for domain registration and DNS management.

Route53 integrates seamlessly with the larger route52 dns service. enabling you to manage your dns record from within the same console or programmatically.

Content Delivery and CDN:

21. What is content delivery, and why is it important for web applications?

content delivery fdistributes information to duplicate servers to maintain web based content

22. How does Amazon CloudFront function as a Content Delivery Network (CDN)?

iamazon cloud front is a content delivery network service built for high performance, security and developer convenience.

23. Explain the benefits of using CloudFront for caching and distribution.

cloud front speeds up the distribution of your content routing each user requests through the aws backbone network to the edge location that can best serve your account.

24. What are Edge Locations in the context of AWS CloudFront?

cloudfornt delivers your content through a worldwide network of data centres called edge locations. content is delivered with best performance and low latency.

25. How can you set up SSL/TLS encryption for data transferred via CloudFront?

navigate to cloudfront console and edit next to your distribution. scroll down to the ssl certificate section and choose custom ssl certificate from the dropdown menu.

Virtual Private Cloud (VPC):

26. Describe the concept of an Amazon VPC (Virtual Private Cloud).

with amazon virtual private cloud (VPC) you can launch resources in a logically isolated virtual network that you've defined.

27. How do you create and configure subnets within an AWS VPC?

in the navigation pane choose subnet, create a subnet with the vpc ID and the availability zone.

28. What is the purpose of Network Address Translation (NAT) in a VPC?

NAT gateways are configured so that instances in a private subnet can connect to services outside your vpc but external services cannot initiate a connection.

29. Explain the differences between a VPC's main route table and custom route tables.

main route table - route table that automatically comes with your vpc
custom route table - a table that you create for your VPC.

30. How can you establish secure communication between VPCs in different AWS regions?

you can use access vpc peering or AWS transit gateway

Security Groups and Network ACLs:

31. What are Security Groups, and how do they control inbound and outbound traffic to AWS resources?

security groups allow groups of inbound and outbound rules for users like a firewall

32. Explain the stateful nature of Security Groups in AWS.

security groups are stateful. if you send a request from an instance, the response traffic for the truest is allowed to reach the instance regardless of inbound security group rules

33. Describe Network ACLs (Access Control Lists) and their role in network security.

networking ACLs manage access to a network, they provide instructions to switches and routers as to the kinds of traffic that are allowed to interface with the network.

34. What is the key difference between Security Groups and Network ACLs?

security groups are for user and doesn't have a firewall and set with EC2
ACL is associated with a subnet

35. How can you restrict access to a specific EC2 instance using Security Groups?

by specifying resource ARNs or by resource tags as condition keys.

AWS Web Application Firewall (WAF):

36. What is AWS Web Application Firewall (WAF), and why is it used?

AWS Web application firewall is a a firewall to protect web hosted applications to improve security and prevent unwanted attacks. You will create rules to block or monitor web requests based on the conditions you'd define.

37. How does WAF protect web applications from common security threats?

ca WAF protects your web apps by filtering, monitoring and blocking any http/s traffic travelling to the web application and prevents unauthorised data leaving the app.

38. Explain the concept of WAF rules and conditions.

WAS rules are used to define how to inspect HTTP/HTTPS web traffic to an application, where and what parameters and conditions to look for in the request and what action the WAF should take when a request matches those definitions

39. What is rate-based blocking in AWS WAF, and how does it mitigate DDoS attacks?

a rate-based rules limits traffic form IP addresses when they are sending a high volume of requests. rate-based rules help protect your application against web request floods and provide alerts for sudden spikes in traffic which could indicate a DDoS attack.

40. Describe the integration of AWS WAF with other AWS services and resources.

a WAF provides two levels of integration for javascript applications and one for mobile applications. intelligent threat integration verify the client application and provide aws token acquisition and management