AWS SERVICES & GENERAL AWS KNOWLEDGE

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

It's like a security handshake. AWS takes care of securing the cloud infrastructure (physical servers, data centers), while customers are responsible for securing their applications and data running on AWS.

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

It's like a blueprint for building well-designed systems. The framework has five pillars: Operational Excellence, Security, Reliability, Performance Efficiency, and Cost Optimization.

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

It's like a free trial for AWS services. The Free Tier offers limited usage of services like EC2, S3, and RDS at no cost for a 12-month period for new AWS customers.

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

EC2 is like renting virtual computers. It provides resizable compute capacity in the cloud. You choose an instance type, launch it, and have full control over your virtual machine.

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

EC2 instances are like different models of virtual computers. They're classified based on instance types, which specify the combination of CPU, memory, storage, and networking they provide.

6.How do you choose the right EC2 instance type for a specific workload?

It's like picking the right tool for the job. You consider factors like CPU, memory, storage, and the workload's specific requirements to choose the most suitable instance type.

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

AMIs are like templates for EC2 instances. They contain the software, configurations, and even data needed to launch instances. You use them to create and clone EC2 instances.

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

- On-Demand is like renting by the hour with no commitment.
- Reserved is like subscribing for a discount on a one- or three-year term.
- Spot is like bidding on spare capacity at a lower cost but with the risk of termination if the price goes up.

COST OPTIMIZATION

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

Strategies include rightsizing instances, using reserved instances, monitoring and managing underutilized resources, and leveraging automation for cost control.

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

You can use AWS services like Auto Scaling and Lambda to schedule instance start and stop times or use the built-in scheduling feature in EC2.

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

Cost Explorer is like a financial report. It helps you visualize and understand your AWS cost and usage patterns over time, making it easier to budget and forecast.

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

Trusted Advisor is like a financial advisor for your AWS usage. It checks your account for cost optimization opportunities and provides recommendations to reduce spending.

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

You can use EC2 monitoring tools, such as CloudWatch, to identify underutilized instances by analyzing CPU and network metrics. Once identified, you can manually terminate them.

AMAZON ROUTE 53 (DNS SERVICE)

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

Route 53 is like a phone book for the internet. It's a scalable DNS service that translates human-readable domain names into IP addresses. It's used for domain registration, routing traffic to AWS resources, and more.

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

- Alias records are like shortcuts for AWS resources, including AWS services like S3 or CloudFront.
- CNAME records are like redirects that point to other domain names.

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

Health checks are like periodic check-ups for your resources. You configure them in Route 53 to monitor the health of your endpoints (e.g., web servers) and route traffic to healthy instances.

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

The Resolver is like a traffic cop for DNS resolution. It routes DNS queries between your on-premises network and Route 53, helping you manage DNS for hybrid cloud environments.

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

Route 53 offers domain registration and DNS management in one place. It provides reliability, scalability, and features like routing policies and health checks for high availability and performance.

CONTENT DELIVERY NETWORK

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

Content delivery is like delivering pizza quickly. It's the distribution of web content (images, videos, files) from servers geographically closer to users. It improves website performance and user experience.

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

CloudFront is like a delivery network for your web content. It caches and delivers your content from edge locations worldwide, reducing latency and providing high availability.

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

CloudFront is like a fast cache for web content. It accelerates content delivery, reduces the load on origin servers, and ensures high availability with global edge locations.

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

Edge locations are like local distribution centers for CloudFront. They are where cached content is stored and delivered from. AWS has many edge locations worldwide.

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

You can configure CloudFront to use SSL/TLS encryption by associating a valid SSL/TLS certificate with your CloudFront distribution, ensuring secure data transfer.

VIRTUAL PRIVATE CLOUD (VPC)

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

A VPC is like your private space in the AWS cloud. It allows you to create isolated networks with their own IP address ranges, subnets, and security controls. It's the foundation for building your AWS infrastructure.

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

Subnets are like neighborhoods within your VPC. You create them by dividing the IP address range of your VPC. You can configure them with route tables, security groups, and network ACLs to control traffic.

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

NAT is like a postal service for outbound traffic. It allows instances in private subnets to access the internet by translating their private IP addresses into a public IP address.

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

- The main route table is like a default set of directions for traffic in the VPC.
- Custom route tables are like personalized routes for specific subnets. They override the main route table for those subnets.

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

You can use AWS Direct Connect, VPN connections, or VPC peering to establish secure connections between VPCs in different regions, allowing data to flow safely between them.

SECURITY GROUPS AND NETWORK ACLS

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

Security Groups are like firewalls for AWS resources. They define the rules for allowing or denying traffic to and from instances. They work at the instance level and are stateful.

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

Stateful means Security Groups remember outbound connections, so they automatically allow the return traffic. You only need to define rules for incoming traffic, making it simpler to manage.

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

Network ACLs are like filters for subnets. They control traffic at the subnet level by allowing or denying specific IP addresses or ranges. They're stateless and work in conjunction with Security Groups.

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

Security Groups work at the instance level and are stateful, while Network ACLs work at the subnet level and are stateless. Security Groups are more specific and are evaluated first.

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

You can create a Security Group with specific rules that only allow traffic from specified sources (e.g., IP addresses) to access a particular EC2 instance, effectively restricting access to that instance.

AWS WEB APPLICATION FIREWALL (WAF)

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

WAF is like a bouncer for your web applications. It protects against common web security threats (like SQL injection and cross-site scripting) by allowing or blocking web traffic based on predefined rules.

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

WAF inspects incoming web traffic and applies security rules to filter out malicious requests and protect against known attack patterns, ensuring the safety of web applications.

36.Explain the concept of WAF rules and conditions.

WAF rules are like security guidelines, and conditions are like criteria. You use rules to define how to handle specific conditions, like blocking requests with certain patterns or from specific IP addresses.

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

Rate-based blocking is like a traffic cop. It monitors incoming requests and blocks those that exceed predefined request rates. It helps mitigate DDoS (Distributed Denial of Service) attacks by limiting excessive traffic.

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

AWS WAF can be integrated with services like CloudFront, API Gateway, and Application Load Balancers. It provides an additional layer of security to protect these resources against web threats and attacks.