AWS Services and General AWS Knowledge:

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

4. Describe the AWS Well-Architected Framework and its pillars. • The AWS Well-Architected Framework is a valuable resource for organizations looking to design, build, and operate cloud-native applications and workloads that are secure, reliable, efficient, and cost-effective. • AWS provides a Well-Architected Tool and consulting services to help organizations assess their workloads against these pillars and make informed improvements based on best practices. Pillars: Operational Excellence Security Reliability Performance Efficiency Cost Optimization

5. What is the AWS Free Tier, and what services are available under it? AWS Free Tier is a free of cost and we have different services like t2 micro and t2 nano which has limited availability

Amazon EC2 (Elastic Compute Cloud):

6. What is Amazon EC2, and how does it work? Amazon EC2 is a virtual server where we provide CPU, storage, memory, operating system by creating an server, where we can start, stop and terminate the sever.

7. What are EC2 instances, and how are they classified based on instance types? EC2 instances are the virtual servers and they classified like CPU, memory, instance size, storage, performance

8. How do you choose the right EC2 instance type for a specific workload? We have to choose based on the application requirements and budget of the project.

9. What is the significance of the Amazon Machine Image (AMI) in EC2? Amazon machine images are like docker images where we can store the data in a image and we can place it wherever we needed.

10. Explain the difference between on-demand, reserved, and spot instances in EC2. On-Demand Instances provide flexibility and are suitable for unpredictable or short-term workloads, but they come at a higher cost. Reserved Instances (RIs) offer significant cost savings for steady workloads over a longer term, requiring upfront commitments. Spot Instances provide the lowest cost but can be interrupted at any time; they are ideal for fault-tolerant and cost-sensitive workloads.

Cost Optimization:*

11. What strategies can you employ to optimize costs when using AWS resources? To optimize the cost we can use amazon free services like free tier. we have to choose right instance type according to our need. we can also set our budget as per the project requirements

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

13. Describe the AWS Cost Explorer and how it can help analyze cost trends. We can see aws resources spending and identify cost trends

14. What is AWS Trusted Advisor, and how does it assist in cost optimization? AWS trusted advisor provides best options for cost optimization and where it will show un utilized resources

15. How can you identify and terminate underutilized EC2 instances? Firstly we can go to the AWS Trusted advisors and there we can stop or terminate

AWS Route 53 Service):*

16. What is Amazon Route 53, and what are its primary use cases? Amazon Route 53 is a service provided by AWS to manage domain name systems and provides DNS services and routes internet traffic

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

Amazon Route 53 is a scalable and highly available domain name system (DNS) web service provided by Amazon Web Services (AWS). It allows you to manage DNS records for your domain names.

Two common types of DNS records in Route 53 are Alias records and CNAME (Canonical Name) records.

Alias records are specific to AWS resources and are used to map domains and subdomains to AWS services with no additional cost, no TTL value of their own, and support for apex domains.

CNAME records are general-purpose and can point to any FQDN, but they have a TTL value, cannot be used for apex domains, and may involve additional DNS lookups.

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

• Create a Health Check: • Sign in to the AWS Management Console: Go to the Route 53 dashboard. • **Select "Health checks" on the left sidebar. • Click "Create health check."

Specify the settings for your health check:

• Name: Give your health check a descriptive name. • IP Address or Domain Name: Specify the IP address or domain name of the resource you want to monitor. • Resource Path: Optionally, specify a specific path or endpoint on the resource to check. • Port: Specify the port to use for the health check (e.g., 80 for HTTP, 443 for HTTPS). • Type: Choose the type of health check you want to perform (e.g., HTTP, HTTPS, TCP). • Request Interval: Set how frequently Route 53 should perform health checks. • Failure Threshold: Define

the number of consecutive failures before considering the resource unhealthy. • Enable "Latency Based Routing" (optional): If you're using latency-based routing, you can enable this option to use the health check's latency data for routing decisions. • Configure "Advanced Configuration" (optional): • You can set additional options such as enabling SSL for HTTPS checks, specifying the regions from which health checks originate, and specifying an S3 bucket to store detailed health check results. • **Click "Next" to review your settings and then "Create health check" to create it.

19. What is the purpose of the Amazon Route 53 Resolver service? Amazon Route 53 Resolver service simplifies DNS configuration and management within Amazon VPCs and facilitates DNS resolution in hybrid cloud environments. It provides features for private DNS namespaces, conditional forwarding, DNS firewall rules, and query logging, making it a valuable tool for enhancing the connectivity, security, and reliability of your AWS resources and networks.

20. Describe the benefits of using Route 53 for domain registration and DNS management. • Route 53 offers DNS query routing based on the geographic location of the requester, helping to reduce latency and improve the performance of your applications. This is especially valuable for global or multi-region deployments. • Route 53 allows you to implement advanced traffic routing policies like weighted routing, latency-based routing, failover routing, and geolocation-based routing. These policies enable you to distribute traffic across multiple resources for load balancing and high availability. • Route 53 allows you to set up private DNS namespaces within your Amazon Virtual Private Cloud (VPC). This is valuable for internal applications and services that require custom DNS names. • Route 53 offers DNSSEC (DNS Security Extensions) support, enhancing the security of your DNS infrastructure by providing data integrity and authentication of DNS responses. • Route 53 provides detailed query logging and analytics, allowing you to monitor DNS traffic, troubleshoot issues, and gain insights into the usage of your domain names. • Route 53 offers domain registration services, making it easy to register and manage domain names directly within the AWS Management Console. This simplifies domain management by consolidating it with DNS management

Content Delivery and CDN:*

21. What is content delivery, and why is it important for web applications? Content delivery, often referred to as Content Delivery or Content Delivery Network (CDN), is a technology and network infrastructure designed to deliver web content (such as text, images, videos, scripts, and other assets) to users or clients in the most efficient, reliable, and scalable manner possible. CDNs work by strategically distributing copies of content to multiple data centers or points of presence (PoPs) located around the world, and they aim to reduce latency, improve website performance, and enhance the user experience Importance • Improved Performance • Reduced Server Load • Reliability and Redundancy • Security • Global Reach • Bandwidth Savings • Analytics and Reporting • Load Balancing • Mobile Optimization

22. How does Amazon CloudFront function as a Content Delivery Network (CDN)? Amazon CloudFront functions as a CDN by distributing and caching web content at strategically located edge locations, reducing latency for end-users and improving the scalability and reliability of web applications. It seamlessly integrates with other AWS services and provides a range of features for content delivery, security, and customization, making it a powerful tool for optimizing the delivery of web content and applications. How? • Content Caching and Distribution • Edge Locations • Request Routing • Cache Control • Content Updates • Origin Fetch • Automatic Scaling

23. Explain the benefits of using CloudFront for caching and distribution. When you use Amazon CloudFront, you configure it to serve as a distribution point for your web content. This content can include static assets like images, videos, scripts, stylesheets, and dynamic content from your web application.

24. What are Edge Locations in the context of AWS CloudFront? "Edge Locations" are a crucial component of the Content Delivery Network (CDN) infrastructure provided by CloudFront. Edge Locations are endpoints or data centers located in various geographic locations worldwide. These locations serve as the points of presence (PoPs) where CloudFront caches and delivers content to end-users. They play a crucial role in caching and delivering content with low latency, high availability, and scalability, making CloudFront an essential service for improving the performance and reliability of web applications and media distribution.

25. How can you set up SSL/TLS encryption for data transferred via CloudFront? Security socket layer or transport layer security to transfer the data Acquire an SSL/TLS Certificate Configure SSL/TLS for Your CloudFront Distribution DNS Configuration Ensure that your DNS records (e.g., CNAME or ALIAS records) for your domain point to your CloudFront distribution. If you're using a custom domain, make sure it's configured to use HTTPS and the CloudFront distribution as the origin server. Testing After configuring SSL/TLS for CloudFront, test your setup by accessing your web application using the HTTPS protocol (e.g., https://www.example.com). Verify that your SSL/TLS certificate is properly installed and valid.

Virtual Private Cloud (VPC):

26. Describe the concept of an Amazon VPC (Virtual Private Cloud). • Amazon Virtual Private Cloud (Amazon VPC) is a fundamental building block of Amazon Web Services (AWS) infrastructure that allows you to create a logically isolated section of the AWS Cloud where you can launch AWS resources, such as EC2 instances, RDS databases, and Lambda functions • Amazon VPC plays a central role in securing and organizing your AWS resources, providing network isolation, and allowing you to build complex and secure network architectures in the cloud. It's a critical component for designing and deploying AWS workloads in a controlled and customized networking environment.

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

configuring subnets within an Amazon Virtual Private Cloud (VPC) involves defining smaller IP address ranges within your VPC's CIDR block and specifying their characteristics, such as availability zones (AZs) and route tables Steps: Log in to the AWS Management Console Open the VPC Dashboard Select Your VPC Create a Subnet Configure Subnet Details Click "Create subnet" to Create the Subnet Repeat for Additional Subnets

28. What is the purpose of Network Address Translation (NAT) in a VPC? Network Address Translation (NAT) in a VPC serves the essential purpose of enabling outbound internet access for resources in private subnets while providing security, access control, and preservation of private IP addresses. It is a critical component for securely connecting your VPC-based workloads to external services and the internet while maintaining control over traffic flow and security policies.

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

main route table is automatically associated with all subnets in a VPC and provides basic local routing for communication within the VPC.

Custom route tables, on the other hand, offer greater flexibility and control over routing decisions and allow you to create custom routing rules for specific subnets, making them ideal for more complex networking requirements and segmentation of traffic within your VPC.

30. How can you establish secure communication between VPCs in different AWS regions? One common approach to achieve this is by using AWS services and features like VPC peering, AWS Direct Connect, and VPN connections.

Security Groups and Network ACLs:

31. What are Security Groups, and how do they control inbound and outbound traffic to AWS resources? Amazon Web Services (AWS) Security Groups are virtual firewalls that control inbound and outbound traffic to and from AWS resources, such as Amazon Elastic Compute Cloud (EC2) instances, Relational Database Service (RDS) instances, and Elastic Load Balancers (ELBs). Security Groups act as stateful traffic filters, allowing you to specify which traffic is allowed or denied based on defined rules.

To control inbound traffic, you create inbound rules in your Security Group. Each rule consists of the following components: Type: Specifies the type of traffic (e.g., HTTP, SSH, RDP). Protocol: Indicates the network protocol (e.g., TCP, UDP, ICMP) used for the traffic. Port Range: Specifies the port range (e.g., 80, 443) for the traffic. Source: Defines the source IP range or source Security Group that is allowed to send traffic.

Controlling Outbound Traffic with Security Groups: Outbound traffic is controlled implicitly by allowing or denying inbound traffic and establishing the

stateful nature of Security Groups. When you create an EC2 instance and associate it with a Security Group, you can specify the rules for inbound traffic. The outbound traffic from that instance is allowed automatically as long as the corresponding inbound traffic is allowed.

32. Explain the stateful nature of Security Groups in AWS. Security Groups are stateful, meaning that if you allow inbound traffic from a specific IP address, the corresponding outbound traffic (response traffic) is automatically allowed. You don't need to define separate rules for outbound traffic; AWS handles it for you.

33. Describe Network ACLs (Access Control Lists) and their role in network security. Network Access Control Lists (Network ACLs or NACLs) are a fundamental component of network security in Amazon Virtual Private Cloud (VPC). NACLs act as stateless, rule-based network-level firewalls that control inbound and outbound traffic at the subnet level. They provide an additional layer of security beyond Security Groups by allowing you to define rules that govern the flow of traffic in and out of your VPC subnets Role of Network ACLs in Network Security: Traffic Control Public and Private Subnets Defense-in-Depth traffic Control Protection Against Misconfigurations Logging and Monitoring

34. What is the key difference between Security Groups and Network ACLs? Security Groups focus on instance-level security and are stateful, while NACLs operate at the subnet level, are stateless, and provide network-level filtering and control. Depending on your security requirements, you may use both in combination to create comprehensive security policies for your VPC resources.

35. How can you restrict access to a specific EC2 instance using Security Groups? By configuring inbound and outbound rules

AWS Web Application Firewall (WAF):

36. What is AWS Web Application Firewall (WAF), and why is it used? AWS Web Application Firewall (WAF) is a managed web application firewall service provided by Amazon Web Services (AWS). It helps protect web applications from common web exploits and vulnerabilities by allowing you to configure rules and policies that control and filter incoming web traffic. AWS WAF is designed to enhance the security and availability of your web applications, APIs, and content delivery.

37. How does WAF protect web applications from common security threats? • WAF provides protection for web applications from common security threats by allowing you to create and configure rules that filter and inspect incoming web traffic. • AWS WAF enables you to create custom rules and conditions that define how incoming web traffic should be handled. • AWS offers preconfigured managed rulesets, such as the AWS Managed Rules for WAF. • AWS WAF allows you to implement rate limiting rules to restrict the number of requests from a single IP address or IP address range within a specified time frame. • AWS WAF can work in conjunction with other AWS services, such as

AWS Lambda, to automate threat mitigation actions.

38. Explain the concept of WAF rules and conditions. WAF rules and conditions are fundamental building blocks that allow you to define how incoming web traffic to your web applications should be handled.

1. Rules:

Definition: Rules in AWS WAF are the core components that define the logic for inspecting and controlling web traffic.

Use Cases: You create rules to implement specific security policies and protections against common web application security threats, such as SQL injection, cross-site scripting (XSS), and bad bots.

Rule Types: AWS WAF supports two main types of rules: WebACL (Web Access Control List) Rules: These rules are associated with a WebACL, which is a collection of rules that define the overall security policy for a web application. WebACL rules evaluate incoming requests against the conditions you specify and take action (allow, block, count) based on the match results. Rule Group Rules: Rule groups are sets of rules that you can reuse across multiple WebACLs. Rule group rules are designed for common use cases and can be shared and managed centrally.

2. Conditions:

Definition: Conditions are the criteria or attributes that AWS WAF evaluates when determining whether a rule should be applied to incoming web requests. Use Cases: You use conditions to specify what aspects of incoming traffic should be examined, such as HTTP headers, query strings, URI paths, IP addresses, or request methods. Types of Conditions: AWS WAF provides several types of conditions that you can use to build your rules: String Match Conditions: These conditions evaluate string values in web requests. For example, you can use them to inspect and match specific query string parameters or HTTP headers. IP Match Conditions: These conditions evaluate IP addresses. You can use them to allow or block requests from specific IP addresses, IP address ranges, or IP address sets. Geo Match Conditions: These conditions evaluate the geographic origin of the request based on the source IP address. You can use them to allow or block traffic from specific countries or regions. Size Constraint Conditions: These conditions evaluate the size of specific parts of a web request, such as the length of query strings or request body content. Rate-Based Rule Conditions: These conditions are used for rate limiting and evaluate the rate at which requests are made from specific IP addresses.

39. What is rate-based blocking in AWS WAF, and how does it mitigate DDoS attacks? Rate-based blocking is a feature in AWS Web Application Firewall (WAF) that helps mitigate Distributed Denial of Service (DDoS) attacks by controlling the rate at which incoming requests are allowed from a single IP address or a set of IP addresses. It is designed to protect your web applications from aggressive or abusive traffic patterns that may overwhelm your resources

and cause downtime or service degradation how it helps mitigate DDoS attacks Rate-Based Blocking in AWS WAF • Rate-Based Rules • Counting Requests • Rate Exceeded

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

AWS Web Application Firewall (WAF) is a managed service that helps protect your web applications from common web exploits and threats. It can be integrated with various AWS services and resources to enhance the security of your web applications. Here's an overview of the integration of AWS WAF with other AWS services and resources:

AWS WAF can send logs and metrics to Amazon CloudWatch and Amazon S3, allowing you to monitor traffic patterns and perform in-depth analysis for security and compliance purposes.