AWS INTERVIEW QUESTIONS

1. Name 5 aws services you have used and what's the use cases?

Here are five AWS services I have used and their use cases:

Amazon EC2 (Elastic Compute Cloud) - It provides scalable compute capacity in the cloud. I have used it to launch and manage virtual machines (EC2 instances) for various purposes such as web hosting and data processing.

Amazon S3 (Simple Storage Service) - It is an object storage service that offers industry-leading scalability, data availability, security, and performance. I have used it to store and manage large amounts of data such as images, videos and documents.

Amazon RDS (Relational Database Service) - It is a managed database service that makes it easy to set up, operate, and scale a relational database in the cloud. I have used it to create and manage MySQL databases for web applications.

AWS Lambda - It is a serverless compute service that allows developers to run code without provisioning or managing servers. I have used it to build event-driven applications, perform data processing tasks, and create APIs using functions written in languages such as Python and Node.js. With Lambda, you only pay for the compute time you consume and can easily scale up or down based on demand.

Amazon CloudWatch - It is a monitoring and observability service for AWS resources and applications. I have used it to collect and track metrics, collect and monitor log files, set alarms, and automatically react to changes in AWS resources. CloudWatch can be used to monitor services like EC2, RDS, S3, and Lambda, as well as custom metrics generated by your applications.

2. What are the tools used to send logs to the cloud environment?

There are several tools that can be used to send logs to the cloud environment in AWS. Here are some examples:

Amazon CloudWatch Logs Agent - It is a tool provided by AWS that enables you to send logs from EC2 instances to CloudWatch Logs. You can configure the agent to monitor log files, Windows event logs, or application logs, and it will automatically send the logs to CloudWatch Logs.

AWS Lambda - It is a serverless compute service that can be used to process logs and send them to CloudWatch Logs. You can create a Lambda function that subscribes to a CloudWatch Logs log group and processes the log data before sending it to another destination.

AWS CloudTrail - It is a service that enables you to log, continuously monitor, and retain account activity related to actions across your AWS infrastructure. You can use CloudTrail to capture logs for API calls made by or on behalf of AWS services in your account, and send them to CloudWatch Logs.

3. What are IAM Roles? How do you create /manage them?

IAM (Identity and Access Management) Roles are AWS entities that define a set of permissions for making AWS service requests. A role is a secure way to grant permissions to entities that you trust, such as AWS services, IAM users, or resources outside of AWS.

IAM Roles are created and managed in the AWS Management Console or via the AWS CLI. steps for creating and managing IAM Roles:

1. Sign in to the AWS Management Console and open the IAM console.
2. Navigate to the Roles page, and click on the Create role button.
3. Select the AWS service that will use this role, such as EC2 or Lambda.
4. Choose the use case for the role, such as granting permissions to access specific AWS resources or allowing cross-account access.
5. Define the permissions for the role by attaching one or more policies to the role.
6. Define the trust policy, which specifies who can assume the role and under what conditions.
7. Review and confirm the role details, and then click on the Create role button.

To manage an existing IAM Role, you can navigate to the Roles page in the IAM console and select the role that you want to manage. You can then perform various actions on the role, such as editing the role policy, adding or removing permissions, or deleting the role. You can also use the AWS CLI or SDKs to manage IAM Roles programmatically.

4. How to upgrade or downgrade a system with zero downtime?

Blue-green deployment: This approach involves creating two identical environments, one with the current system and one with the upgraded or downgraded system. Traffic is initially routed to the current environment (blue), and once the new environment (green) has been fully tested and is ready, traffic is switched to the new environment. This ensures zero downtime since traffic is never interrupted during the switch.

Canary deployment: This approach involves gradually rolling out the upgraded or downgraded system to a small percentage of users at first, while keeping the majority of traffic on the current system. This allows you to test the new system with real traffic and make sure it's working as expected. If there are any issues, you can quickly roll back to the previous version.

Rolling deployment: This approach involves upgrading or downgrading one server at a time, while still serving traffic from the remaining servers. Once the first server has been upgraded or downgraded and verified to be working correctly, traffic is shifted to that server while the next server is upgraded or downgraded. This process continues until all servers have been upgraded or downgraded. This approach requires careful planning and monitoring to ensure that no server becomes overloaded during the process.

5. What is infrastructure as code and how do you use it?

Infrastructure as Code is a practice of defining and managing IT infrastructure through code. It involves writing scripts or configuration files that describe the desired state of the infrastructure, which can then be automatically provisioned and managed by tools such as AWS CloudFormation or HashiCorp Terraform.

To use IAC, you need to define your infrastructure as code by creating scripts or configuration files that describe the desired state of your infrastructure. Once the code has been written, you can use a tool like CloudFormation or Terraform to provision and manage the infrastructure.The key benefits of IAC include version control, consistency, and automation. By using IAC, you can ensure that all environments are created and configured in the same way, reduce the risk of errors and inconsistencies, and speed up the deployment process by automating the provisioning and configuration of infrastructure.

6. What is a load balancer? Give scenarios of each kind of balancer based on your experience.

A load balancer is a device or software that distributes incoming network traffic across multiple servers to improve performance, availability, and scalability of applications or services. It can help to distribute the workload among servers and prevent overloading.

Types of load balancers:

Classic Load Balancer (CLB): This load balancer routes traffic based on either the IP address of the client or the requested host name. It supports both HTTP and HTTPS protocols, as well as TCP and SSL protocols.

some scenarios where Classic load balancer may be used are:

- Serving static websites or applications that do not rely on cookies
- Distributing traffic across multiple web or application servers in a simple setup
- Handling TCP or SSL traffic for non-HTTP/HTTPS applications

Application Load Balancer (ALB): This is a more advanced load balancer that operates at the application layer (Layer 7) and can route traffic based on the content of the request. ALB supports features such as path-based routing, host-based routing, and routing based on HTTP headers or query strings. It can also handle sticky sessions for applications that require session persistence, such as e-commerce websites or SaaS applications.

some scenarios where application load balancer may be used are:

- Routing traffic to multiple microservices based on path or host
- Handling traffic for complex web applications with multiple tiers

Network Load Balancer(NLB): It is a Layer 4 (transport layer) load balancer that can handle high volumes of traffic with low latency and high throughput. Also used to handle TCP and UDP traffic at the transport layer.

7. What is CloudFormation and why is it used for?

AWS CloudFormation is a service that allows you to model and provision AWS resources in a declarative way using templates. It is used to automate the deployment and management of infrastructure as code in AWS, making it easier to create, update, and delete stacks of resources with minimal effort. By using CloudFormation, you can create and configure resources in a consistent and repeatable way, reducing the time and effort required to manage your infrastructure.

8. Difference between AWS CloudFormation and AWS Elastic Beanstalk?

AWS CloudFormation is a service that automates the deployment and management of infrastructure resources, CloudFormation is focused on infrastructure management, and provides more flexibility and control over the resources being deployed. It allows for custom scripts and more granular resource configuration.

AWS Elastic Beanstalk is a platform that simplifies the deployment and management of applications by providing a preconfigured platform.It is focused on application management and provides a preconfigured platform that simplifies the deployment and management of applications. It includes a variety of prebuilt components, such as load balancers and databases, which can be quickly and easily configured.

9. What are the kinds of security attacks that can occur on the cloud? And how can we minimize them?

There are several kinds of security attacks that can occur on the cloud, including:

- Distributed Denial of Service (DDoS) attack
- Malware and viruses
- Data breaches and theft
- Cross-site scripting (XSS) attacks
- SQL injection attacks
- Phishing attacks

To minimize these security attacks, here are some best practices:

- Use strong authentication and authorization mechanisms, such as multi-factor authentication and role-based access control.
- Implement encryption for data at rest and in transit.
- Implement network security controls such as firewalls and intrusion detection and prevention systems.
- Implement regular security audits and vulnerability assessments.
- Maintain compliance with industry standards and regulations.
- Implement security monitoring and logging to detect and respond to security incidents.
- Use a trusted cloud service provider with a strong track record of security and compliance.

10. Can we recover the EC2 instance when we have lost the key?

We can recover an EC2 instance when we have lost the key pair by creating a new key pair, stopping the instance, detaching the root volume, launching a new instance with the new key pair, attaching the root volume to the new instance, starting the new instance, and updating security groups and IP addresses as needed.

There is another way to recover an ec2 instance, if we have lost the key pair, we can create an AMI of the existing instance, and then launch a new instance. We can then select a new key pair by following the instance launch wizard.

What is a gateway

gateway is a network component that serves as a bridge or a transition point between different networks. It is used to facilitate communication and data transfer between networks that may have different communication protocols and addressing schemes.Gateways can be used to connect different cloud environments together.

11. What is the difference between the Amazon RDS, Dynamodb, and Redshift?

Amazon RDS, DynamoDB, and Redshift are three different database services offered by Amazon Web Services (AWS) with different use cases and functionalities.

Amazon RDS (Relational Database Service) is a fully managed relational database service that makes it easy to set up, operate, and scale a relational database in the cloud. It supports popular database engines like MySQL, PostgreSQL, Oracle, and SQL Server. With RDS, you don't have to worry about managing the underlying infrastructure, including patching, backups, and replication. Instead, you can focus on building and optimizing your applications.

Amazon DynamoDB, on the other hand, is a fully managed NoSQL database service that provides fast and predictable performance with seamless scalability. It is designed to handle large amounts of unstructured data, such as documents, images, and social media content. DynamoDB is a serverless database, which means that you don't have to manage any servers or infrastructure.

Amazon Redshift is a fully managed data warehouse service that makes it easy to analyze large amounts of data using SQL and business intelligence tools. It is designed for online analytical processing (OLAP) and supports big data analytics. Redshift is optimized for querying and analyzing large datasets and is based on a columnar storage format. It provides fast query performance and allows you to scale your cluster up or down depending on your needs.

12. Do you prefer to host a website on S3? What's the reason if your answer is either yes or no?

Hosting a website on S3 may be a good option for simple static websites that don't require server-side scripting or complex functionality. S3 charges based on the amount of storage used and data transferred, which can be significantly cheaper than using a traditional web hosting service.
However, for more advanced websites or applications, other web hosting services may be a better fit. S3 doesn't support server-side scripting, which means you can't use popular web technologies like PHP or ASP.NET. S3 also lacks some features that are typically included in web hosting services, such as domain name registration, email hosting, and database support.