AWS SCENARIO BASED INTERVIEW QUESTIONS

Question 1: You have been assigned to design a VPC architecture for a 2-tier application. The application needs to be highly available and scalable. How would you design the VPC architecture?

Answer: In this scenario, I would design a VPC architecture in the following way. I would create 2 subnets: public and private. The public subnet would contain the load balancers and be accessible from the internet. The private subnet would host the application servers. I would distribute the subnets across multiple Availability Zones for high availability. Additionally, I would configure auto scaling groups for the application servers.

Question 3: You have a VPC with a public subnet and a private subnet. Instances in the private subnet need to access the internet for software updates. How would you allow internet access for instances in the private subnet?

Answer: To allow internet access for instances in the private subnet, we can use a NAT Gateway or a NAT instance. We would place the NAT Gateway/instance in the public subnet and configure the private subnet route table to send outbound traffic to the NAT Gateway/instance. This way, instances in the private subnet can access the internet through the NAT Gateway/instance.

Question 4: You have launched EC2 instances in your VPC, and you want them to communicate with each other using private IP addresses. What steps would you take to enable this communication?

Answer: By default, instances within the same VPC can communicate with each other using private IP addresses. To ensure this communication, we need to make sure that the instances are launched in the same VPC and are placed in the same subnet or subnets that are connected through a peering connection or a VPC peering link. Additionally, we should check the security groups associated with the instances to ensure that the necessary inbound and outbound rules are configured to allow communication between them.

Question 6: Your organization requires an isolated environment within the VPC for running sensitive workloads. How would you set up this isolated environment?

Answer: To set up an isolated environment within the VPC, we can create a subnet with no internet gateway attached. This subnet, known as an “isolated subnet,” will not have direct internet connectivity. We can place the sensitive workloads in this subnet, ensuring that they are protected from inbound and outbound internet traffic. However, if these workloads require outbound internet access, we can set up a NAT Gateway or NAT instance in a different subnet and configure the isolated subnet’s route table to send outbound traffic through the NAT Gateway/instance.

Question 7: Your application needs to access AWS services, such as S3 securely within your VPC. How would you achieve this?

Answer: To securely access AWS services within the VPC, we can use VPC endpoints. VPC endpoints allow instances in the VPC to communicate with AWS services privately, without requiring internet gateways or NAT gateways. We can create VPC endpoints for specific AWS services, such as S3 and DynamoDB, and associate them with the VPC. This enables secure and efficient communication between the instances in the VPC and the AWS services.

Question 8: What is the difference between NACL and Subnet? Explain with a use case.

Answer: For example, if I want to design a security architecture, I would use a combination of NACLs and security groups. At the subnet level, I would configure NACLs to enforce inbound and outbound traffic restrictions based on source and destination IP addresses, ports, and protocols. NACLs are stateless and can provide an additional layer of defense by filtering traffic at the subnet boundary. At the instance level, I would leverage security groups to control inbound and outbound traffic. Security groups are stateful and operate at the instance level. By carefully defining security group rules, I can allow or deny specific traffic to and from the instances based on the application’s security requirements. By combining NACLs and security groups, I can achieve granular security controls at both the network and instance level, providing defense-in-depth for the sensitive application.

Question 9: What is the difference between IAM users, groups, roles, and policies?

Answer:

- IAM Users: Individual AWS accounts with unique credentials for accessing resources.
- IAM Groups: Collections of users for easier permission management.
- IAM Roles: Used for delegation of permissions to services, applications, or accounts.
- IAM Policies: Documents specifying allowed or denied actions on AWS resources.

The company wants to ensure the highest level of security for its AWS resources. What are some best practices you would recommend?

Answer: I would suggest implementing measures like using IAM roles with least privilege, enabling MFA for all users, encrypting data in transit and at rest, regularly rotating access keys and passwords, and continuously monitoring logs using services like AWS CloudTrail and AWS Config. Additionally, regular security audits and vulnerability assessments should be performed.

The company's application is generating a large volume of logs and metrics. How would you manage and analyze these logs effectively on AWS?

Answer: I would use Amazon CloudWatch Logs to centralize and manage logs. CloudWatch Metrics can be used to monitor specific performance indicators. For more advanced analysis, I might use AWS CloudWatch Logs Insights for querying logs and set up CloudWatch Alarms for triggering notifications based on defined thresholds.

The company needs to migrate a large dataset from on-premises servers to AWS. What are some strategies you would consider?

Answer: Depending on the specifics, I might use AWS Database Migration Service (DMS) for database migrations, AWS Snowball for large-scale offline data transfers, or AWS DataSync for automated data synchronization. For real-time data migration, I would explore options like AWS Direct Connect or VPN connections.

The company has multiple business units that require separate AWS accounts. How would you design a multi-account architecture to ensure isolation and cost management?

Answer: I would recommend setting up an AWS Organizations hierarchy, with a master account and separate member accounts for each business unit. This allows for centralized management while providing isolation between units. I would also implement cross-account roles for controlled access between accounts.

The company wants to conduct regular disaster recovery tests to ensure the effectiveness of the recovery plan. How would you approach this on AWS?

Answer: I would create a separate environment (e.g., in a different AWS region) mirroring the production environment. Then, I would simulate a disaster scenario and execute the disaster recovery plan. This would involve tasks like launching standby resources, restoring backups, and validating system functionality. After the test, I would conduct a thorough evaluation to identify and address any gaps or improvements.

The company is adopting DevOps practices and wants to set up a toolchain on AWS. How would you design this toolchain for continuous integration, delivery, and deployment?

Answer: I would use services like AWS CodePipeline for orchestrating the pipeline, AWS CodeCommit for version control, AWS CodeBuild for building and testing, and AWS Elastic Beanstalk, ECS, or EKS for deployment. Additionally, I might integrate with third-party tools for specific stages like testing or code quality checks.

Q

: You have an application that requires extremely low-latency communication between instances. How can you achieve this on Amazon EC2?

To achieve low-latency communication between instances, you can use EC2 Placement Groups. Placement Groups enable instances to be placed in close proximity within the same Availability Zone (AZ). There are two types of Placement Groups: Cluster Placement Groups for low-latency and High-Performance Computing (HPC) workloads and Spread Placement Groups for critical instances that require maximum separation to minimize the risk of simultaneous failure.

: Your application needs to store sensitive data, and you want to ensure that the data is encrypted at rest on EC2 instances. How can you enable this encryption?

To encrypt data at rest on EC2 instances, you can use Amazon Elastic Block Store (EBS) volumes with encryption enabled. When creating or modifying an EBS volume, you can specify the use of AWS Key Management Service (KMS) to manage the encryption keys. Data written to the EBS volume is automatically encrypted, and it remains encrypted at rest.

Q

: Your team is developing a containerized application and wants to deploy it on EC2 instances. Which service can you use to manage the containers on EC2 efficiently?

You can use Amazon Elastic Container Service (ECS) or Amazon Elastic Kubernetes Service (EKS) to manage containers on EC2 instances. ECS is a fully-managed service for running containers at scale, while EKS provides Kubernetes management capabilities for container orchestration. Both services simplify the process of deploying, managing, and scaling containerized applications on EC2 instances.

Q

: You want to enhance the security of your EC2 instances by restricting incoming traffic only to specific IP addresses. How can you implement this security measure?

To restrict incoming traffic to specific IP addresses on EC2 instances, you can configure security group rules. Security groups act as virtual firewalls and allow you to control inbound and outbound traffic. By specifying the desired IP ranges in the inbound rules, you can ensure that only traffic from those IP addresses is allowed to reach the instances.

: Your organization needs to store and share data files across multiple EC2 instances. What service can you use to achieve scalable and durable file storage?

You can use Amazon Elastic File System (EFS) to achieve scalable and durable file storage for multiple EC2 instances. EFS provides a managed file system that can be mounted concurrently by multiple instances within a VPC. It supports the Network File System (NFS) protocol and automatically scales capacity as data grows.

: Your team wants to minimize the cost of running EC2 instances for non-production environments (e.g., development and testing). How can you achieve cost savings without compromising availability?

To minimize costs for non-production environments while maintaining high availability, you can use EC2 Spot Instances. Spot Instances allow you to bid on spare EC2 capacity, and they can significantly reduce costs compared to On-Demand Instances. However, keep in mind that Spot Instances can be terminated when the Spot price exceeds your bid, so they are best suited for stateless and fault-tolerant workloads.

: Your organization needs to host a web application that requires consistent CPU performance and low latency. Which EC2 instance type would you recommend, and why?

For applications requiring consistent CPU performance and low latency, I would recommend using an EC2 instance from the “c5” or “m5” instance families. Both families are designed for compute-intensive workloads, with the “c5” instances offering higher CPU performance and the “m5” instances providing a balance of compute and memory resources.

: Your application involves batch processing of large datasets. How can you optimize the EC2 instances for such a workload?

For batch processing of large datasets, you can use EC2 instances from the “r5” instance family, which is optimized for memory-intensive workloads. By choosing an instance with sufficient memory, you can avoid performance bottlenecks caused by frequent disk swapping, enhancing the efficiency of your batch processing.

: Your team is developing a microservices-based application and wants to deploy it on EC2 instances. What are some best practices to ensure the scalability and maintainability of the microservices architecture?

To ensure the scalability and maintainability of a microservices-based application on EC2, consider the following best practices:

- Deploy each microservice on separate EC2 instances to achieve isolation.
- Use containerization technology like Docker to package and deploy microservices consistently.
- Implement an orchestration service like Amazon ECS or Amazon EKS to manage the containerized microservices efficiently.
- Design microservices with loosely coupled communication to enable independent scaling and deployment.

You need to migrate an on-premises virtual machine (VM) to AWS EC2. What service can you use to simplify the VM migration process?

To simplify the migration of on-premises VMs to AWS EC2, you can use AWS Server Migration Service (SMS). SMS allows you to automate, schedule, and track incremental replications of VMs from your data center to AWS, reducing the complexity of the migration process.

Your application requires frequent changes and updates, and you want to test new features without affecting the production environment. How can you achieve this with EC2?

To test new features and changes without affecting the production environment, you can create an Amazon Machine Image (AMI) of the existing production EC2 instance. Launch a new EC2 instance using the AMI in a separate testing environment. This isolated environment allows you to experiment and validate changes before applying them to the production instance.

: Your development team needs to share sensitive data securely between EC2 instances. How can you set up a secure communication channel for this purpose?

To set up a secure communication channel between EC2 instances, you can use Virtual Private Cloud (VPC) peering or AWS PrivateLink. VPC peering allows you to connect VPCs within the same AWS account privately. AWS PrivateLink enables secure and private communication between VPCs and supported AWS services without traversing the internet.

: Your organization requires on-premises resources to communicate securely with EC2 instances within a VPC. How can you establish a secure connection between your on-premises network and the VPC?

To establish a secure connection between your on-premises network and an EC2 instance within a VPC, you can use AWS Site-to-Site VPN or AWS Direct Connect. Site-to-Site VPN creates an encrypted tunnel over the internet, whereas Direct Connect provides a dedicated connection through a private network link.

: Your team wants to ensure that only authorized personnel can access the EC2 instances via SSH. What security measure should be implemented?

To ensure that only authorized personnel can access the EC2 instances via SSH, you should configure the security group rules to allow inbound SSH access only from specific IP addresses or ranges associated with authorized personnel. Additionally, you can manage SSH access using IAM roles and AWS Systems Manager Session Manager for secure remote management.

Q

: You need to run Windows-based applications on EC2 instances, and your team requires remote desktop access for management purposes. How can you enable remote desktop access to Windows EC2 instances?

To enable remote desktop access to Windows EC2 instances, you need to configure the Windows Firewall and EC2 Security Groups to allow Remote Desktop Protocol (RDP) traffic (port 3389). Additionally, ensure that you have the necessary credentials to log in to the instances remotely.

: Your team wants to monitor the performance of EC2 instances and set up alerts for abnormal behavior. What AWS service can help you achieve this?

To monitor the performance of EC2 instances and set up alerts, you can use Amazon CloudWatch. CloudWatch provides a comprehensive set of monitoring and alerting capabilities, allowing you to collect and track metrics, set alarms, and automatically react to changes in your EC2 instances' performance.

You want to deploy your web application to multiple regions to ensure high availability and low latency. What AWS service can you use to automate the deployment process across regions?

You can use AWS Elastic Beanstalk to automate the deployment process of your web application across multiple regions. Elastic Beanstalk simplifies application deployment by automatically handling capacity provisioning, load balancing, scaling, and application health monitoring.

: Your application requires persistent data storage that survives instance termination. What storage option can you use on EC2 for this purpose?

For persistent data storage that survives instance termination, you can use Amazon Elastic Block Store (EBS) volumes. EBS volumes are durable, block-level storage devices that can be attached to EC2 instances and persist independently of the instance lifecycle.

: Your application needs to support both IPv4 and IPv6 traffic. How can you ensure that EC2 instances can handle both types of traffic?

To ensure that EC2 instances can handle both IPv4 and IPv6 traffic, you need to enable dual-stack networking on your VPC. With dual-stack enabled, EC2 instances can communicate with both IPv4 and IPv6 addresses.