amazon web services

Scenario Based Interview Questions on EC2, IAM & VPC

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 ?

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.

Your organization has a VPC with multiple subnets. You want to restrict outbound internet access for resources in one subnet, but allow outbound internet access for resources in another subnet. How would you achieve this ?

To restrict outbound internet access for resources in one subnet, we can modify the route table associated with that subnet. In the route table, we can remove the default route (0.0.0.0/0) that points to an internet gateway.

This would prevent resources in that subnet from accessing the internet. For the subnet where outbound internet access is required, we can keep the default route pointing to the internet gateway.

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 ?

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.

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 ?

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.

You want to implement strict network access control for your VPC resources. How would you achieve this ?

To implement granular network access control for VPC resources, we can use Network Access Control Lists (ACLs).

NACLs are stateless and operate at the subnet level. We can define inbound and outbound rules in the NACLs to allow or deny traffic based on source and destination IP addresses, ports, and protocols.

By carefully configuring NACL rules, we can enforce fine-grained access control for traffic entering and leaving the subnets.

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

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 or instance.

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

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.

What is the difference between NACL and Security groups ? Explain with a use case ?

For example, 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.

You have a private subnet in your VPC that contains a number of instances that should not have direct internet access. However, you still need to be able to securely access these instances for administrative purposes. How would you set up a bastion host to facilitate this access?

To securely access the instances in the private subnet, you can set up a bastion host (also known as a jump host or jump box). The bastion host acts as a secure entry point to your private subnet. Here's how you can set up a bastion host:

Create a new EC2 instance in a public subnet, which will serve as the bastion host. Ensure that this instance has a public IP address or is associated with an Elastic IP address for persistent access.

Configure the security group for the bastion host to allow inbound SSH (or RDP for Windows) traffic from your IP address or a restricted range of trusted IP addresses. This limits access to the bastion host to authorized administrators only.

Place the instances in the private subnet and configure their security groups to allow inbound SSH (or RDP) traffic from the bastion host security group.

SSH (or RDP) into the bastion host using your private key or password. From the bastion host, you can then SSH (or RDP) into the instances in the private subnet using their private IP addresses.

What is IAM Users ?

IAM Users: An IAM user is an identity within AWS that represents an individual or application needing access to AWS resources. IAM users have permanent long-term credentials, such as a username and password, or access keys (Access Key ID and Secret Access Key). IAM users can be assigned directly to IAM policies or added to IAM groups for easier management of permissions.

What is IAM Roles ?

IAM Roles: An IAM role is similar to an IAM user but is not associated with a specific individual. Instead, it is assumed by entities such as IAM users, applications, or services to obtain temporary security credentials. IAM roles are useful when you want to grant permissions to entities that are external to your AWS account or when you want to delegate access to AWS resources across accounts. IAM roles have policies attached to them that define the permissions granted when the role is assumed.

What is IAM Groups ?

IAM Groups: An IAM group is a collection of IAM users. By organizing IAM users into groups, you can manage permissions collectively. IAM groups make it easier to assign permissions to multiple users simultaneously. Users within an IAM group inherit the permissions assigned to that group. For example, you can create a "Developers" group and assign appropriate policies to grant permissions required for developers across your organization.

What is IAM Policy ?

IAM Policy: An IAM policy is a document that defines permissions and access controls in AWS. IAM policies can be attached to IAM users, IAM roles, and IAM groups to define what actions can be performed on which AWS resources. IAM policies use JSON (JavaScript Object Notation) syntax to specify the permissions and can be created and managed independently of the users, roles, or groups. IAM policies consist of statements that include the actions allowed or denied, the resources on which the actions can be performed, and any additional conditions.