**Default VPC**

**Introduction to Default VPC in AWS**

In this lecture, we will explore the default Virtual Private Cloud (VPC) in AWS. The demonstration is performed in the AWS Management Console, specifically in the North California region (US West 1). This region is chosen because it has only two availability zones, making it easier to study, learn, and practice VPC configurations. The knowledge gained here applies to other AWS regions as well, but starting with a simpler setup helps reduce complexity during learning.

To begin, search for the VPC service in the AWS console and open it. The VPC dashboard displays various configurations such as VPCs, NAT Gateways, Subnets, and more. Our focus is on the default VPC. Click on "Your VPCs" to view the existing VPCs. You will see a VPC without a name, which is the default VPC. Scrolling horizontally reveals the "default VPC" designation.

It is important to note that you cannot create a default VPC manually. While you can create custom VPCs, the default VPC is automatically created by AWS in every region. If the default VPC is accidentally deleted, you must contact AWS support to have it restored. To easily identify the default VPC, it is common practice to rename it to "DEFAULT VPC" in uppercase letters.

Every AWS region has a default VPC with the CIDR block 172.31.0.0/16. The "/16" subnet mask provides approximately 65,000 IP addresses. To examine the subnets, navigate to the "Subnets" section. You will find two subnets associated with this VPC. These subnets are public subnets, which we will verify shortly. Rename these subnets to "Default-pubsub1" and "Default-pubsub2" for clarity and identification.

Each subnet belongs to the default VPC, which can be confirmed by comparing the VPC ID in the subnet details with the default VPC's ID. The subnets have a CIDR block of /20, which provides around 4,096 IP addresses each. AWS reserves five IP addresses per subnet for internal use. The IP addresses assigned to instances in these subnets will be in the range 172.31.16.x, not in other private IP ranges such as 10.x.x.x or 20.x.x.x. By examining the private IP address of an instance, you can identify the subnet it belongs to. Additionally, each subnet is associated with an availability zone, such as 1a or 1b.

**Identifying Public Subnets via Route Tables**

These two subnets are public subnets. To determine whether a subnet is public or private, examine its route table entries. Select a subnet and view its associated route table. The route table contains routes that define where outbound traffic from the subnet is directed.

* Traffic destined for IP addresses within the VPC range is routed locally within the VPC.
* Traffic destined for all other IP addresses (0.0.0.0/0) is routed to the internet gateway.

The internet gateway ID is visible in the route table and can be further inspected in the Internet Gateways section. The route table also shows which subnets it is associated with, confirming that these two subnets are public because their outbound traffic is routed through the internet gateway.

In contrast, private subnets route outbound traffic through a NAT gateway instead of the internet gateway. This distinction is crucial for managing network security and access.

Remember:

* Traffic routed to the internet gateway indicates a public subnet.
* Traffic routed to a NAT gateway indicates a private subnet.

This knowledge is fundamental and often asked in interviews related to AWS networking.

**Additional VPC Components and Best Practices**

Besides VPCs, subnets, route tables, and internet gateways, the AWS VPC dashboard displays other components such as Egress-only internet gateways, DSCP Option Sets, Endpoints, and Endpoint Services. These are advanced topics beyond the scope of this course.

In upcoming lectures, we will explore NAT Gateways, Elastic IPs, and Network ACLs.

A critical best practice is to never delete the default VPC, its internet gateway, or route tables. By the end of this course, you will be able to create internet gateways and route tables and attach them to your VPCs. However, the default VPC can only be restored by AWS support if deleted.

In the next lecture, we will learn how to create a custom VPC and add subnets to it.

**Key Takeaways**

* The default VPC exists in every AWS region and cannot be created manually; if deleted, AWS support must be contacted to restore it.
* Default VPC in the North California region uses the CIDR block 172.31.0.0/16, providing approximately 65,000 IP addresses.
* Public subnets route outbound traffic to the internet gateway, while private subnets route through a NAT gateway.
* Understanding route tables and subnet associations is essential for managing VPC networking effectively.