Module 5 - Networking and Content Delivery

Slides

Objectives / Topics

- Recognize the basics of networking
- Describe virtual networking in the cloud with Amazon VPC
- Label a network diagram
- Design a basic VPC architecture
- Indicate the steps to build a VPC
- Identify security groups
- Create your own VPC and add additional components to it to produce a customized network
- Identify the fundamentals of Amazon Route 53
- Recognize the benefits of Amazon CloudFront

Labs / Activities

- Knowledge Check
- Activity: Label a Network Diagram
- Activity: Design a VPC
- Lab: Build Your VPC and Launch a Web Server -- Lab Instructions

Section 1: Networking Basics

Network: Two or more machines that are connected together in order to communicate. A network can be divided into subnets and networking requires a networking device such as a router or a switch.

IP Address: A unique numerical label assigned to each device connected to a computer network. IPv4 defines an IP address as a 32-bit number, but because of the growth of the Internet IPv6 was created, using 128 bits for the IP address.

Classless Inter-Domain Routing (CIDR): A method for allocating IP addresses and IP routing. CIDR notation is a compact representation of an IP address and its associated routing prefix. The notation is constructed from an IP address, a slash ('/') character, and an integer. The integer is the count of leading 1 bits in the subnet mask. Larger values here indicate smaller networks. The maximum size of the network is given by the number of addresses that are possible with the remaining, least-significant bits below the prefix.

- Example: The IPv4 block 192.168.100.0/22 represents the 1024 IPv4 addresses from 192.168.100.0 to 192.168.103.255.

Open Systems Interconnection (OSI) Model: A conceptual model that characterises and standardises the communication functions of a computing system without regard to its underlying internal structure and technology. Its goal is the interoperability of diverse communication systems with standard communication protocols. The model partitions a communication system into abstraction layers.

| Layer | Number | Function | Protocol/Address | |-------------|--------|--|-------------------------------------| | Application | 7 | Means for an application to access a computer network | HTTP(S), FTP, DHCP, LDAP | | Presentation | 6 | - Ensures that the application layer can read the data
- Encryption | ASCI, ICA | | Session | 5 | Enables orderly exchange of data | NetBIOS, RPC | | Transport | 4 | Provides protocols to support host-to-host communication | TCP, UDP | | Network | 3 | Routing and packet forwarding (routers) | IP | | Data Link | 2 | Transfer data in the same LAN network (hubs and switches) | MAC | | Physical | 1 | Transmission and reception of raw bit streams over a physical medium | Signals (1s and 0s) |

Section 2: Amazon VPC

- Enables you to provision a logically isolated section of the AWS Cloud where you can launch AWS resources in a virtual network that you define

- Gives you control over your virtual networking resources, including: Selection of IP address range, creation of subnets, and configuration of route tables and network gateways
- Closely resembles a traditional network that you would operate in your own data center, with the benefits of using the scalable infrastructure of AWS
- Enables you to customize the network configurationfor your VPC
- Enables you to use multiple layers of security
- You can create a VPC that spans multiple Availability Zones

VPCs

- Logically isolated from other VPCs
- Dedicated to your AWS account
- Belong to a single AWS Region and can span multiple Availability Zones
- When you create a VPC, you assign it to an IPv4 or IPv6 CIDR block. You cannot change the address range after creation.

Subnets

- Range of IP addresses that divide a VPC
- Belong to a single Availability Zone
- Classified as public (has route to the internet) or private (no internet)
- CIDR blocks of subnets cannot overlap
- Each CIDR block has 5 reserved addresses for: network address, internal communication, DNS resolution, future use, and network broadcast address

Elastic Network Interface

- An Elastic IP address is a static IPv4 address, associated with your AWS account, designed for dynamic cloud computing. You can mask the failure of an instance or software by rapidly remapping the address to another instance in your account.
- A virtual network interface that you can attach to an instance.You can detach from the instance, and attach to another instance to redirect network traffic.
- Its attributes follow when it is reattached to a new instance.
- Each instance in your VPC has a default network interface that is assigned a private IPv4 address from the IPv4 address range of your VPC

Routes and Route Tables

- The route table controls routing for the subnet
- A route table contains a set of rules (or routes) that you can configure to direct network traffic from your subnet
- Each route specifies a destination and a target
- By default, every route table contains a local route for communication within the VPC
- Each subnet must be associated with a single route table

Section 3: VPC Networking

Internet Gateway

A scalable, redundant, and highly available VPC component that allows communication between instances in your VPC and the public internet. An internet gateway serves two purposes:

1. Provide a target in your VPC route tables for internet traffic
2. Perform network address translation for instances that were assigned public IPv4 addresses.

To make a subnet public, you attach an internet gateway to your VPC and add a route entry to the route table associated with the subnet.

Network Address Translation (NAT) Gateway

Enables instances in a private subnet to connect to the internet or other AWS services, but it prevents the public internet from initiating a connection with those instances. To create a NAT Gateway you must:

1. Specify the public subnet in which the gateway should live.
2. Specify an elastic IP address to associate with the NAT Gateway when you create it.

After you create a NAT Gateway, you must update the route table that is associated with one or more of your private subnets to point internet-bound traffic to the NAT gateway. This allows instances in your private subnets to communicate with the internet.

VPC Sharing

Enables customers to share subnets with other AWS accounts in the same organization. VPC Sharing enables multiple AWS accounts to create their application resources in a shared, centrally managed VPC.

The account that owns the VPC shares one or more subnets with other accounts, called participants, that belong to the same organization. After a subnet is shared, participants can view, create, modify, and delete their application resources in the subnets that are shared with them.

VPC Peering

Enables you to privately route traffic between two VPCs. Instances in either VPC can communicate with each other as if they were on the same network. You can create VPC peering connection between your own VPCs with a VPC in another AWS accounts, or between regions.

When you set up the VPC peering connection, you create rules in your route table to allow the VPCs to communicate with each other. VPC peering has some restrictions:

- IP Spaces cannot overlap
- Transitive peering (chaining VPC peering) is not supported
- You can only have one peering resource between the same two VPCs

AWS Direct Connect

Enables your to establish a dedicated private connection between your network and one of the direct connect locations. The private connection can increase bandwidth, throughput, and provide a more consistent network experience than internet-based or VPN connections.

VPC Endpoints

A virtual device that enables you to privately connect a VPC to supported AWS services. There are two types of endpoints:

1. Gateway endpoints that you specify as a target for a route in your route table to either S3 or DynamoDB
2. Interface endpoints are powered by AWS PrivateLink. PrivateLink provides private connectivity between VPCs, AWS services, and on-premises applications.

AWS Transit Gateway

A network transit hub that is used to interconnect virtual private clouds, on-premises networks, VPCs, Direct Connect gateways, and VPN connections to a transit gateway.

The topology of a Transit Gateway is a hub and spoke which reduces the number of connections required, and the complexity to implement and maintain it.

Activity: Label a Network Diagram

Section 4: VPC Security

Security Groups

- Act at the instance level
- Security groups have rules that control inbound and outbound instance traffic.
- Default security groups deny all inbound traffic and allow all outbound traffic.
- Security groups are stateful - return traffic is automatically allowed, regardless of rules
- You can specify allow rules, but not deny rules.
- All rules are evaluated before the decision to allow traffic.

Network Access Control Lists (ACLs)

- Act at the subnet level

- A network ACL has separate inbound and outbound rules, and each rule can either allow or deny traffic.
- Default network ACLs allow all inbound and outbound IPv4 traffic.
- Network ACLs are stateless - return traffic must be explicitly allowed by rules
- Customn network ACLs deny all inbound and outbound traffic until you add rules.
- You can specify both allow and deny rules.
- Rules are evaluated in number order, starting with the lowest number

Activity: Design a VPC

Lab: Build Your VPC and Launch a Web Server -- Lab Instructions

Section 5: Amazon Route 53

- A highly available and scalable Domain Name System (DNS) web service
- Used to route end users to internet applications by translating names (like www.example.com) into numeric IP addresses (like 192.0.2.1) that computers use to connect to each other
- Fully compliant with IPv4 and IPv6
- Connects user requests to infrastructure running in AWS and also outside of AWS
- Is used to check the health of your resources
- Features traffic flow
- Enables you to register domain names

Supported Routing

- Simple routing â€“ Use in single-server environments
- Weighted round robin routing â€“ Assign weights to resource record sets to specify the frequency
- Latency routing â€“ Help improve your global applications
- Geolocation routing â€“ Route traffic based on location of your users
- Geoproximity routing â€“ Route traffic based on location of your resources
- Failover routing â€“ Fail over to a backup site if your primary site becomes unreachable. Improve the availability of your applications that run on AWS by:
- Configuring backup and failover scenarios for your own applications
- Enabling highly available multi-region architectures on AWS
- Creating health checks
- Multivalue answer routing â€“ Respond to DNS queries with up to eight healthy records selected at random

Section 6: Amazon CloudFront

- Fast, global, and secure CDN service
- Global network of edge locations and Regional edge caches
- Self-service model
- Pay-as-you-go pricing

CloudFront Infrastructure

Edge locations â€“ A network of data centers that CloudFront uses to serve popular content quickly to customers.

Regional edge cache â€“ CloudFront location that caches content that is not popular enough to stay at an edge location. It is located between the origin server and the global edge location.

Content Delivery Network

- A globally distributed system of caching servers
- Caches copies of commonly requested files (static content)
- Delivers a local copy of the requested content from a nearby cache edge or Point of Presence
- Accelerates delivery of dynamic content
- Improves application performance and scaling

CloudFront Pricing

- Charged for the volume of data transferred out from Amazon CloudFront edge location to the internet or to your origin.
- Charged for number of HTTP(S) requests.
- No additional charge for the first 1,000 paths that are requested for invalidation each month. Thereafter, $0.005 per path that is requested for invalidation.
- $600 per month for each custom SSL certificate that is associated with one or more CloudFront distributions that use the Dedicated IP version of custom SSL certificate support.

Knowledge Check