Virtual Private Cloud (VPC)

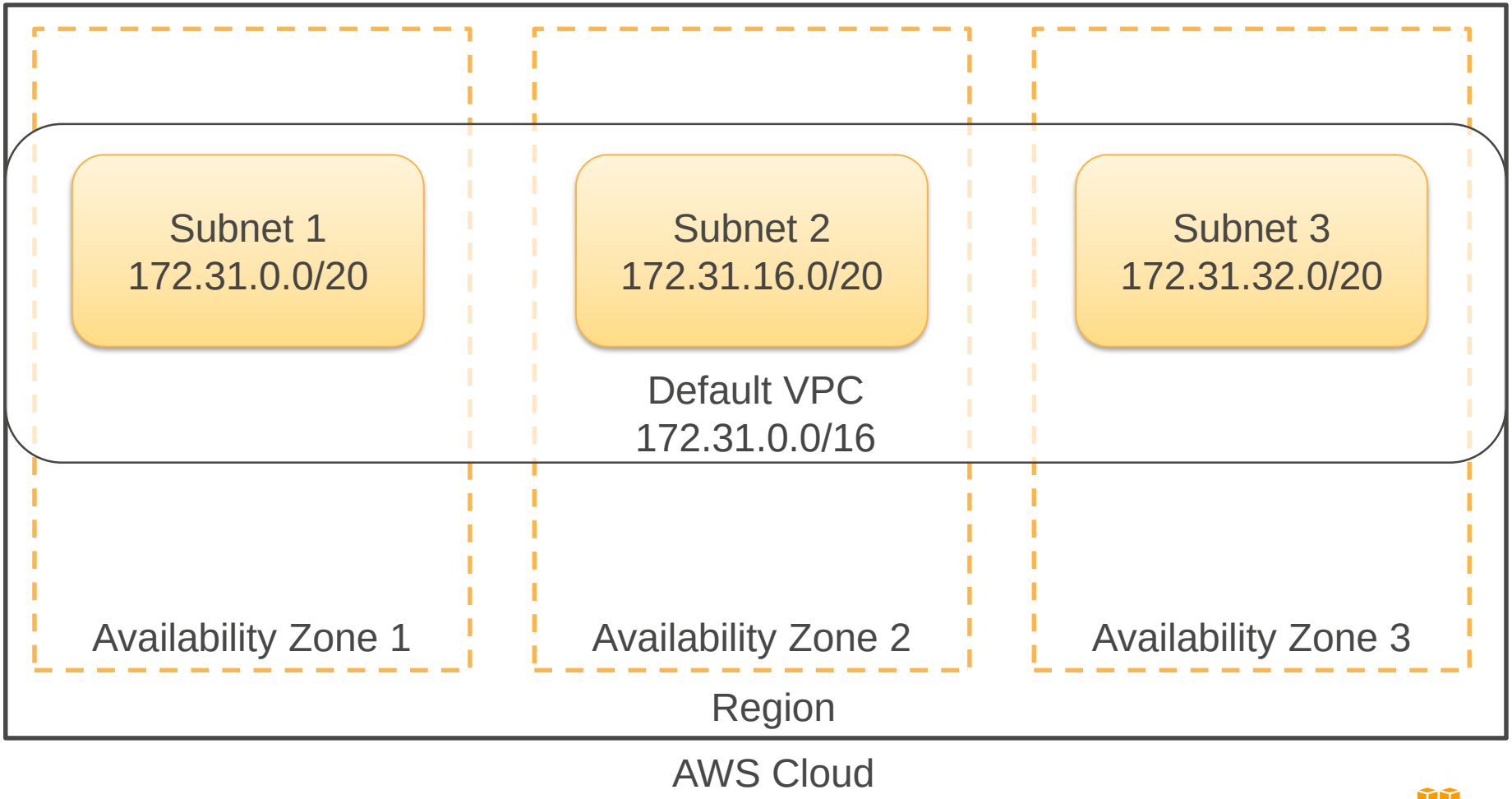
Your own private network in the AWS cloud

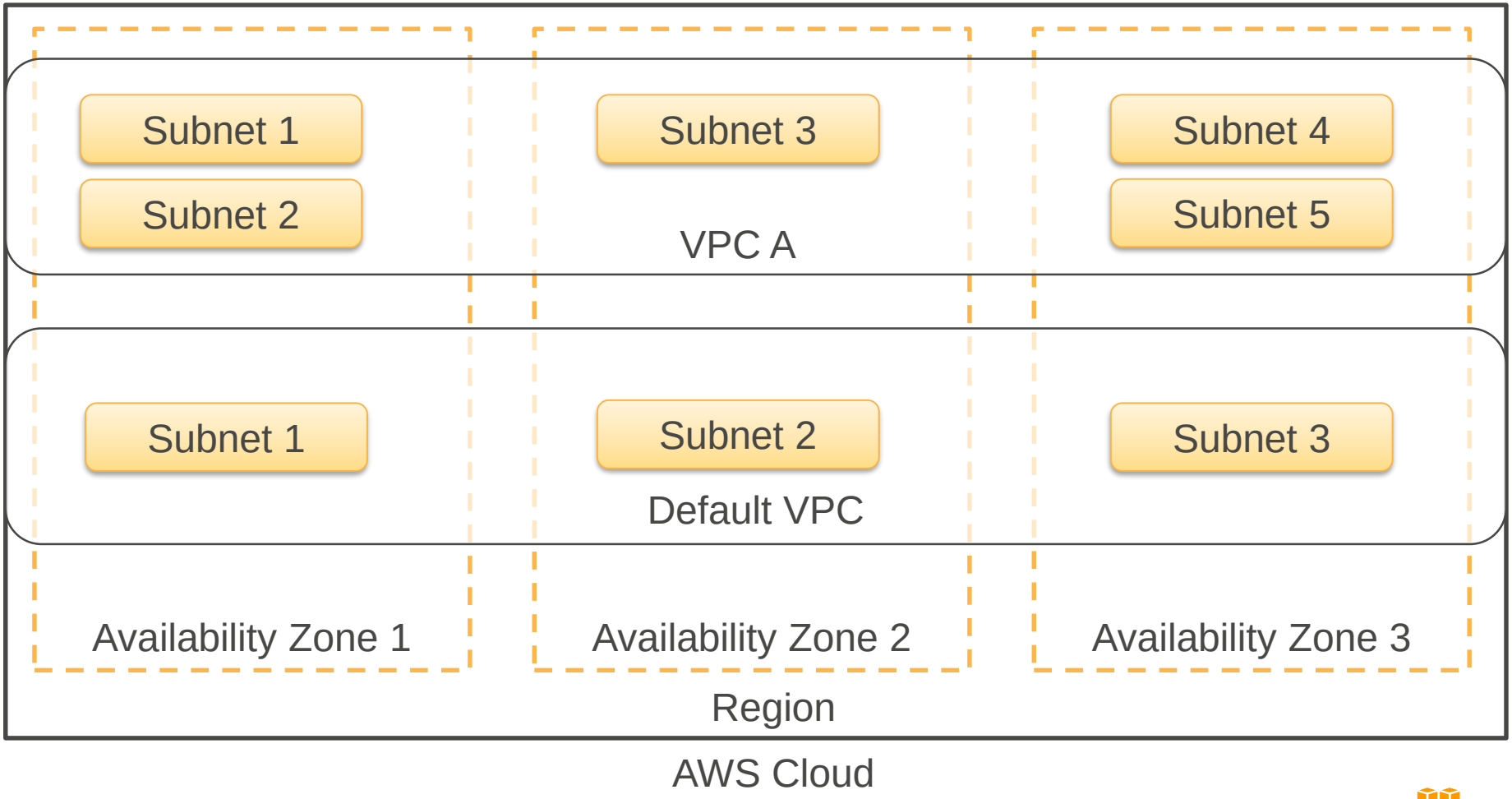
Content Prepared By: Chandra Lingam, Cotton Cola Designs LLC

amazon web services

VPC

- Virtual Network Dedicated to your AWS Account
- Logically isolated from other virtual networks in the AWS Cloud
- Launch resources such as EC2 instances in your VPC
- Select your own IP Address range
- Create Subnets
- Configure route tables, network gateways
- Support for IPv4 and IPv6
- Simple to use





VPC Connectivity

- Connect to Internet from public subnets
- Connect to Internet from private subnets with Network Address Translation
- Connect to corporate datacenter using Virtual Private Network (VPN)
- Connect VPCs together using Peering
- Connect to S3 with private IP address using VPC endpoint
- Combine connectivity methods

VPC Security

- Inbound and Outbound filtering
  - Instance level using Security Groups
  - Subnet level using Access Control Lists
- Configure S3 bucket to be accessible only from your instances in VPC
- Support for Dedicated EC2 instances

History - Before VPC

- *EC2-Classic*. Original Release of EC2 supported a single, flat network that was shared with all customers
- Older AWS Accounts still support EC2-Classic
- VPC Benefits
    - Assign Static Private IP Addresses to your instance
    - Multiple IP Addresses per instance
    - Define network interface, attach one or more network interface to your instance
    - Security Groups and ACLs for ingress and egress filtering
    - Single Tenant Hardware Support

VPC Components

Component	Description
VPC	Isolated virtual network in AWS cloud
Subnet	Isolated segment of your VPC
Internet Gateway	VPC side of connection to internet
NAT Gateway	AWS managed Network Address Translation Service to make outbound internet connection from your private subnet (IPv4)
NAT Instance	Customer managed NAT (IPv4)
Egress-only Internet Gateway	IPv6 outbound internet access

VPC Components

Component	Description
Hardware VPN Connection	Secure connection between your datacenter and VPC
Virtual Private Gateway	Amazon VPC side of VPN connection
Customer Gateway	Customer side of VPN connection
Router	Routes traffic inside VPC
Peering Connection	Connect two VPCs and access resources with private IP address
VPC Endpoint	Access AWS resources like S3 without using NAT or Internet Gateway Control access to resources from specific VPCs

VPC Wizard

- VPC with a Single Public subnet
- VPC with Public and Private subnets
- VPC with Public and Private subnets and Hardware VPN Access
- VPC with Private subnet and Hardware VPN Access

VPC Configuration Examples

Default VPC

Non-default VPC with private only access

Non-default VPC with Elastic IP + Internet Gateway

Internet Access from public subnet - Inbound and Outbound

1. Attach Internet Gateway to your VPC
2. EC2 instances need to have either a public IP Address or Elastic IP address
3. Update Route
4. Connect to Internet or other AWS Services
5. Receive requests from Internet (Example: webserver)

VPC Configuration Examples

Non-default VPC Private subnet + NAT Gateway

Non-default VPC Private subnet + NAT Instance

Internet Access from Private subnet – Outbound Only

1. Attach Internet Gateway to your VPC
2. Attach Network Address Translation to your VPC Public subnet - NAT Gateway or NAT Instance
3. Attach Elastic IP to NAT
4. Update Route to send outbound internet traffic from Private subnet to NAT
5. Connect to Internet or other AWS Services

VPC Configuration Examples

VPC to Corporate/Home Network

VPN CloudHub

Extend your corporate datacenter to AWS Cloud

1. Attach Virtual Private Gateway to your VPC
2. Attach Customer Gateway to your datacenter
3. Establish IPSec VPN connection (encrypted channel)
4. Update Route to send traffic to Virtual Private Gateway
5. Connect to your datacenter systems from VPC and vice versa

VPC Configuration Examples

IPv6 Routing

IPv6 Internet Access from public subnet - Inbound and Outbound

1. IPv6 routes are separate from IPv4 routes
2. Attach Internet Gateway to your VPC
3. Add IPv6 CIDR to your VPC
4. Launch instances in VPC
5. Update route to send IPv6 traffic to Internet gateway
6. Connect to Internet or other AWS services

VPC Configuration Examples

IPv6 Traffic + Egress only Internet Gateways

Internet Access from Private subnet for IPv6 Traffic – Outbound Only

1. Attach Egress-only Internet Gateway to your VPC
2. Update Route to send IPv6 outbound internet traffic to egress only internet gateway
3. Connect to Internet or other AWS Services

VPC Direct Connect

- Dedicated network connection between your network and one of AWS Direct Connect locations
- Consistent Network Performance
- Reduce bandwidth costs

Billing

- Pricing
- VPC – No additional charge for creating or using VPC
- VPN – $0.05 per VPN Connection Hour
- NAT Gateway
  - $0.045 per hour
  - $0.045 per GB data processed
- NAT Instance – Pricing varies based on Instance Type and applicable data transfer charges

VPC and AWS Services

List: VPC with other AWS Services

Deploy resources from other AWS services into your VPC

Demo

New VPC with Public only subnet

New VPC for IPv6

IPv4 and IPv6

Table: Comparison between IPv4 and IPv6

Security - Firewall

- Security Group – Firewall at EC2 instance level
- Access Control List – Firewall at subnet level
- Architecture Diagram
- Usage and Demo - discussed in detail under EC2 Lecture

Security – Resource Access

- Identity and Access Management (IAM) – VPC level access management
- VPC Endpoints – Specify IAM policies on S3 to restrict access from specific VPC
- VPC Flow Logs – Capture information about IP traffic going to and from network interface in your VPC

Route Tables

- Most specific route that matches the traffic determine how traffic is routed
- VPC has a main route table that is implicitly applied to all subnets
- You can apply custom route table to a subnet
- You can make your custom table as main route table
- CIDR blocks are used to specify routes. IPv4 and IPv6 CIDR are treated separately

VPC Peering Connection

- VPC Peering connection allows you connect two VPCs together and route traffic using private IPv4 addresses or IPv6 addresses
- Address should not overlap between VPCs
- Instances communicate as if they are within same network
- Supported for VPCs in the same region
- VPCs can be part of one account or different accounts
- Owner of the peer VPC needs to accept the request

VPC Peering Connection

- Only one peering connection between two VPCs
- Multiple peering connections are supported from one VPC to multiple VPCs

VPC Peering Demo

Create another VPC, peer with default vpc

Update route tables on custom vpc, default vpc

Launch instance using private ip

Access instance from default vpc using ssh bastion

VPC Peering Scenarios

VPC Peering Examples and Scenarios

VPC Limits

Table: VPC Limits for your account