Amazon - VPC

What is VPC?

"Amazon Virtual Private Cloud (VPC) allows the users to use AWS resources in a virtual network. The users can customize their virtual networking environment as they like, such as selecting own IP address range, creating subnets, and configuring route tables and network gateways."

Amazon - VPC

Core Components:

There are six core components which are fundamental to a VPC and will be created by a user or by AWS as part of a default VPC. These components are:

- VPC CIDR Block
- Subnet
- Gateways
- Route Table
- Network Access Control Lists (NACLs)
- Security Group

Web Services

Amazon - VPC

Benefits:

EASY TO USE

Ease of creating a VPC in very simple steps by selecting network setups as per requirement. define Subnets, IP ranges, route tables, and security groups will be automatically created.

PRICING FOR AMAZON VPC

There's no additional charge for using Amazon VPC. Pay the standard rates for the instances and other Amazon EC2 features that you use.

Amazon - VPC

Features:

- Create an Amazon VPC on AWS scalable infrastructure and specify its private IP address range from any range you choose.
- Expand VPC by adding secondary IP ranges.
- Divide VPC private IP address range into one or more public or private subnets to facilitate running applications and services in VPC.
- Control inbound and outbound access to and from individual subnets using network access control lists.

Amazon - VPC

Features:

- Store data in Amazon S3 and set permissions such that the data can only be accessed from within Amazon VPC.
- Attach one or more Amazon Elastic IP addresses to any instance in VPC so it can be reached directly from the Internet.
- Connect VPC with other VPCs and access resources in the other VPCs via private IP addresses using VPC Peering.

Amazon - VPC

Features:

- Privately connect to other AWS services without using an internet gateway, NAT or firewall proxy through a VPC Endpoint.
- Bridge VPC and onsite IT infrastructure with an encrypted VPN connection.
- VPC Flow Logs to log information about network traffic going in and out of network interfaces in VPC.

Amazon - VPC

Key Concepts VPCs and Subnets:

- A subnet is a range of IP addresses in VPC.
- Use a public subnet for resources that must be connected to the internet, and a private subnet for resources that won't be connected to the internet.
- While creating a VPC, must specify a range of IPv4 addresses for the VPC in the form of a Classless Inter-Domain Routing (CIDR) block.

Amazon - VPC

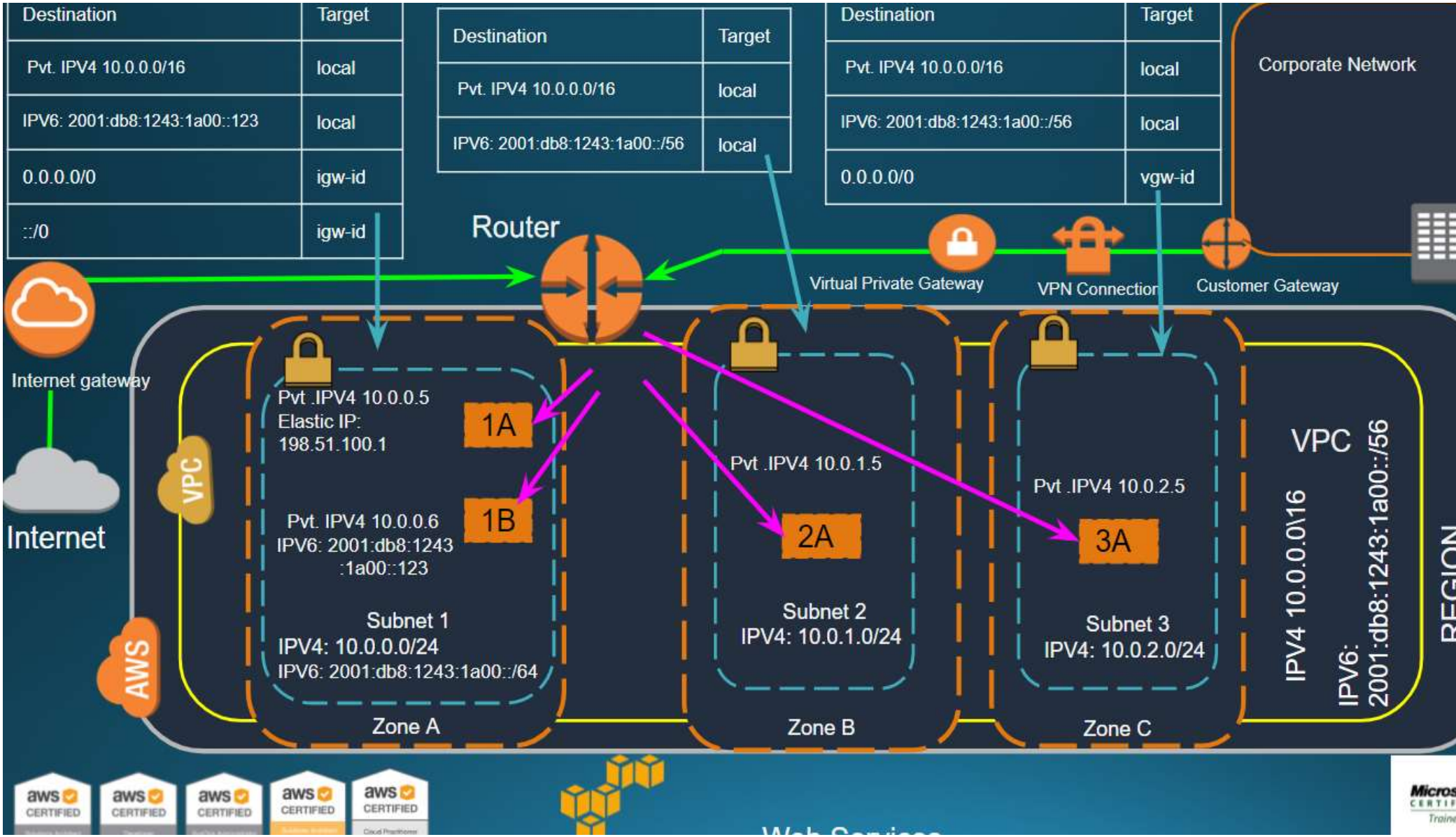
Destination	Target
10.0.0.0/16	Local

The following diagram shows a new VPC with an IPv4 CIDR block, and the main route table.

Amazon - VPC

Key Concepts | VPCs and Subnets:

- After creating a VPC, user can add one or more subnets in each Availability Zone.
- Create a subnet, specify the CIDR block for the subnet, which is a subset of the VPC CIDR block. Each subnet must reside entirely within one Availability Zone and cannot span zones.
- Availability Zones are distinct locations that are engineered to be isolated from failures in other Availability Zones.


Destination
Target
Pvt. IPV4 10.0.0.0/16
local
IPV6: 2001:db8:1243:1a00::123
local
0.0.0.0/0
igw-id
::/0
igw-id
Destination
Target
Pvt. IPV4 10.0.0.0/16
local
IPV6: 2001:db8:1243:1a00::/56
local
Destination
Target
Pvt. IPV4 10.0.0.0/16
local
IPV6: 2001:db8:1243:1a00::/56
local
0.0.0.0/0
vgw-id
Corporate Network
Router
Virtual Private Gateway
VPN Connection
Customer Gateway
Internet gateway
Internet
VPC
AWS
Pvt .IPV4 10.0.0.5
Elastic IP:
198.51.100.1
1A
Pvt. IPV4 10.0.0.6
IPV6: 2001:db8:1243
:1a00::123
1B
Subnet 1
IPV4: 10.0.0.0/24
IPV6: 2001:db8:1243:1a00::/64
Zone A
Pvt .IPV4 10.0.1.5
2A
Subnet 2
IPV4: 10.0.1.0/24
Zone B
Pvt .IPV4 10.0.2.5
3A
Subnet 3
IPV4: 10.0.2.0/24
Zone C
VPC
IPV4 10.0.0.0\16
IPV6:
2001:db8:1243:1a00::/56
REGION
aws CERTIFIED
aws CERTIFIED
aws CERTIFIED
aws CERTIFIED
aws CERTIFIED

Amazon - VPC

Key Concepts | VPCs and Subnets:

The above mentioned diagram shows a VPC that has been configured with subnets in multiple Availability Zones. 1A, 1B, 2A, and 3A are instances in the VPC.

- An IPv6 CIDR block is associated with the VPC, and an IPv6 CIDR block is associated with subnet 1.
- An internet gateway enables communication over the internet, and a virtual private network (VPN) connection enables communication with your corporate network.
- If, a subnet's traffic is routed to an internet gateway, the subnet is known as a public subnet. In this diagram, subnet 1 is a public subnet.

Amazon - VPC

Key Concepts | VPCs and Subnets:

- If instance in a public subnet to communicate with the internet over IPv4, it must have a public IPv4 address or an Elastic IP address (IPv4).
- If instance in the public subnet to communicate with the internet over IPv6, it must have an IPv6 address.
- If a subnet doesn't have a route to the internet gateway, the subnet is known as a private subnet. In this diagram, subnet 2 is a private subnet.

Amazon - VPC

Key Concepts | VPC and Subnet Sizing:

VPC AND SUBNET SIZING FOR IPV4

While creating a VPC, must specify an IPv4 CIDR block for the VPC. The allowed block size is between a /16 netmask (65,536 IP addresses) and /28 netmask (16 IP addresses). After you've created your VPC, you can associate secondary CIDR blocks with the VPC.

Amazon - VPC

Key Concepts | VPC and Subnet Sizing:

VPC AND SUBNET SIZING FOR IPV4

The first four IP addresses and the last IP address in each subnet CIDR block are not available for you to use and cannot be assigned to an instance. For example, in a subnet with CIDR block 10.0.0.0/24, the following five IP addresses are reserved:

10.0.0.0: Network address.
10.0.0.1: VPC router (Gateway).
10.0.0.2: Amazon DNS server to allow for name resolution through the internet gateway
10.0.0.3: Reserved by AWS for future use.
10.0.0.255: Network broadcast address.

Amazon - VPC

VPC Endpoints

- A VPC endpoint enables you to privately connect your VPC to supported AWS services and VPC endpoint services powered by AWS Private Link without requiring an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection.
- Instances in your VPC do not require public IP addresses to communicate with resources in the service.
- Traffic between your VPC and the other service does not leave the Amazon network.

Amazon - VPC

Key Concepts | VPC Security:

- **Security groups** — Act as a firewall for associated Amazon EC2 instances, controlling both inbound and outbound traffic at the instance level
- **Network access control lists (ACLs)** — Act as a firewall for associated subnets, controlling both inbound and outbound traffic at the subnet level
- **Flow logs** — Capture information about the IP traffic going to and from network interfaces in your VPC

Web Services

Amazon - VPC

Key Concepts | VPC Security:

Security Group

Operates at the instance level security.

Supports allow rules only

Is stateful: Return traffic is automatically allowed, regardless of any rules

We evaluate all rules before deciding whether to allow traffic

Network ACL

Operates at the subnet level

Supports allow rules and deny rules

Is stateless: Return traffic must be explicitly allowed by rules

We process rules in number order when deciding whether to allow traffic

Amazon - VPC

Amazon VPC | Integrated with Other AWS Services:

- AWS Data Pipeline
- Amazon EC2
- Auto Scaling
- Elastic Beanstalk
- Elastic Load Balancing
- Amazon WorkSpaces
- Amazon ElastiCache
- Amazon EMR
- AWS OpsWorks
- Amazon RDS
- Amazon Redshift
- Route 53

Amazon - VPC

Hands-On Lab

- Create a VPC with Public & Private Subnet using VPC Wizard
- Create a VPC by using individual VPC components & Verify
- Create a VPC Peering and Endpoint

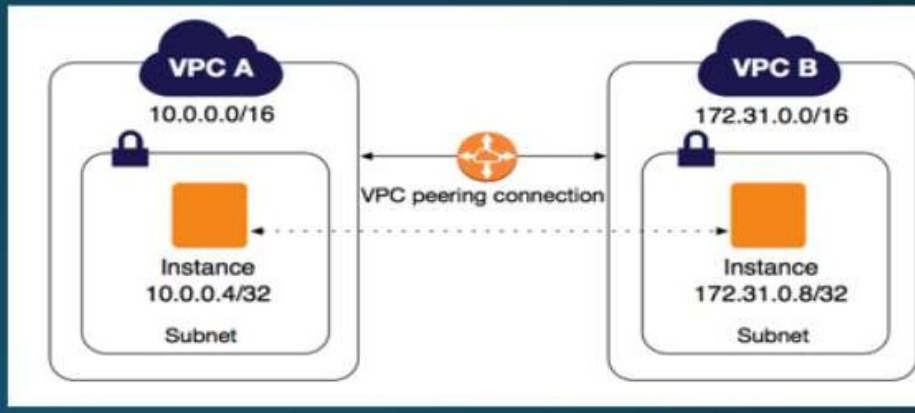
SR1

Amazon - VPC

VPC Peering

A VPC peering connection is a networking connection between two VPCs that enables you to route traffic between them using private IPv4 addresses or IPv6 addresses. Instances in either VPC can communicate with each other as if they are within the same network. You can create a VPC peering connection between your own VPCs, or with a VPC in another AWS account. The VPCs can be in different regions (also known as an inter-region VPC peering connection).

https://docs.aws.amazon.com/vpc/latest/peering/invalid-peering-configurations.html#edge-to-edge-vgw



Invalid Configurations

- Overlapping CIDR blocks
- Transitive peering
- Edge to edge routing through a gateway or private connection

Slide 20

SR1 Sohaib Rehman, 2/23/2024

VPC Peering

- VPC (Virtual Private Cloud) peering is a method of connecting two virtual private clouds in the same or different AWS (Amazon Web Services) regions, allowing them to communicate with each other securely using private IP addresses. There are mainly three types of VPC peering:
- **Intra-Region VPC Peering**: This type of peering occurs between VPCs within the same AWS region. It allows communication between VPCs in the same region but different AWS accounts.
- **Inter-Region VPC Peering**: Inter-region VPC peering enables communication between VPCs in different AWS regions. This allows for connectivity between resources deployed in different geographic regions within the AWS ecosystem.
- **Transitive VPC Peering**: Transitive VPC peering involves establishing connectivity between VPCs through a hub-and-spoke architecture. In this setup, VPCs are interconnected through a central VPC acting as a hub. It allows communication between VPCs that are not directly peered with each other, enabling a network topology where multiple VPCs can communicate with each other through the hub VPC.

VPC Peering

- Transitive peering refers to the ability for traffic to flow between multiple VPCs through an intermediate VPC, known as a transit VPC. In other words, if VPC A is peered with VPC B, and VPC B is peered with VPC C, transitive peering allows communication between VPC A and VPC C through VPC B.

- However, native VPC peering in cloud providers like AWS does not support transitive peering by default. Each VPC peering connection establishes a one-to-one relationship between two VPCs. Therefore, VPCs cannot use another VPC as a transit point to communicate with VPCs beyond their immediate peering connections.

- To achieve transitive peering in AWS, organizations often deploy a transit VPC architecture. In this architecture, a central transit VPC acts as a hub through which all inter-VPC communication flows. Each VPC establishes a peering connection with the transit VPC, allowing traffic to be routed through it to reach other VPCs in the network. This approach enables a scalable and centralized way to manage VPC connectivity and routing within a multi-VPC environment.

VPC Peering

Benefits and Limitations:

- *Benefits:* VPC peering enables low-latency communication between VPCs in different regions, simplifies network architecture, reduces data transfer costs by leveraging AWS's internal network, and enhances security by keeping traffic within the AWS backbone.
- *Limitations:* VPC peering does not support transitive peering (i.e., VPCs cannot communicate via a transit VPC), and there are limits on the number of VPC peering connections per VPC and the number of routes that can be propagated.

VPC Peering

- **Step-by-Step Explanation:**
- When VPC peering is established, AWS creates a direct network route between the VPCs involved.
- Each VPC advertises its CIDR block to the other VPC, allowing them to communicate directly using private IP addresses.
- Traffic between the peered VPCs traverses the AWS backbone network, ensuring low latency and high throughput.

VPC Peering

Security Measures:

- Encrypt data in transit using technologies such as SSL/TLS or VPN connections.
- Implement strict security group and network ACL rules to control traffic flow.
- Enable VPC flow logs to capture network traffic for monitoring and analysis.
- Regularly audit and review VPC peering connections for compliance with security policies.

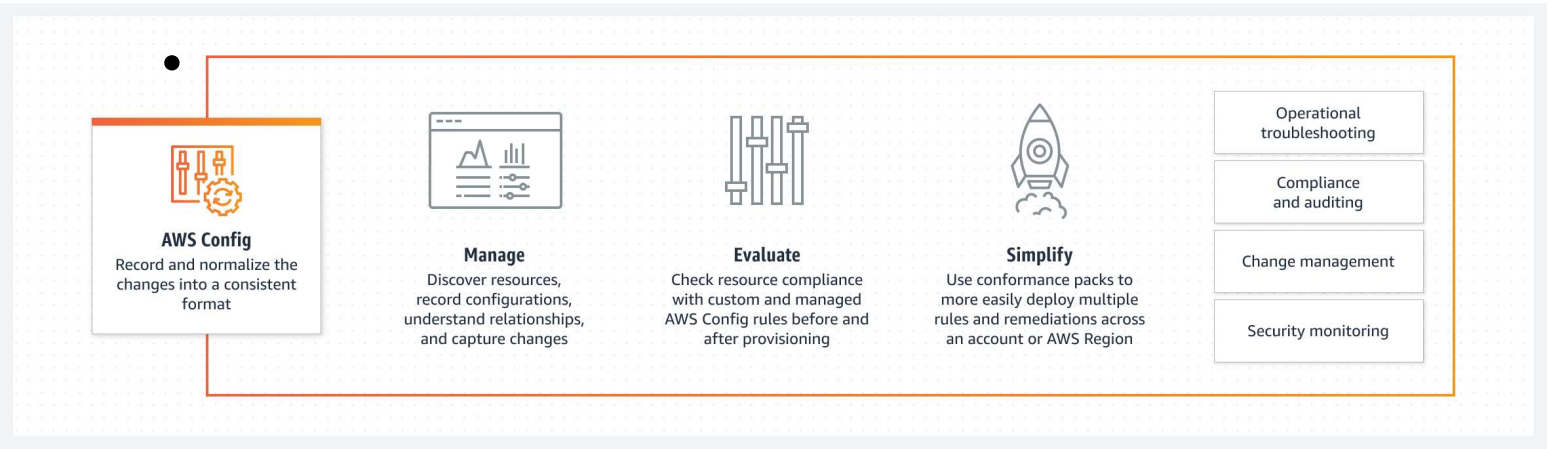
VPC Peering

- **Monitoring and Management Strategy:**
- Set up CloudWatch alarms to monitor VPC peering connection status and network performance metrics.
- Utilize AWS Config to track changes to VPC peering configurations and ensure compliance with security policies.
- Implement automated backups and snapshots of critical resources for disaster recovery purposes.
- Conduct regular performance testing and optimization to ensure optimal network performance across VPC peering connections.

VPC Peering

- **Monitoring and Management Strategy:**
- Set up CloudWatch alarms to monitor VPC peering connection status and network performance metrics.
- Utilize AWS Config to track changes to VPC peering configurations and ensure compliance with security policies.
- Implement automated backups and snapshots of critical resources for disaster recovery purposes.
- Conduct regular performance testing and optimization to ensure optimal network performance across VPC peering connections.

AWS Config


AWS Config
Record and normalize the changes into a consistent format
Manage
Discover resources, record configurations, understand relationships, and capture changes
Evaluate
Check resource compliance with custom and managed AWS Config rules before and after provisioning
Simplify
Use conformance packs to more easily deploy multiple rules and remediations across an account or AWS Region
Operational troubleshooting
Compliance and auditing
Change management
Security monitoring