Cloud Network Services & Connectivity

TEKsystems Global Services

WORKFORCE DEVELOPMENT

COURSE STRUCTURE

Day 1: Networking Fundamentals I

Day 2: Networking Fundamentals II

Day 3: Networking in the Cloud Era

Day 4: Cloud Network Services & Connectivity

Day 5: Availability & Troubleshooting in the Cloud

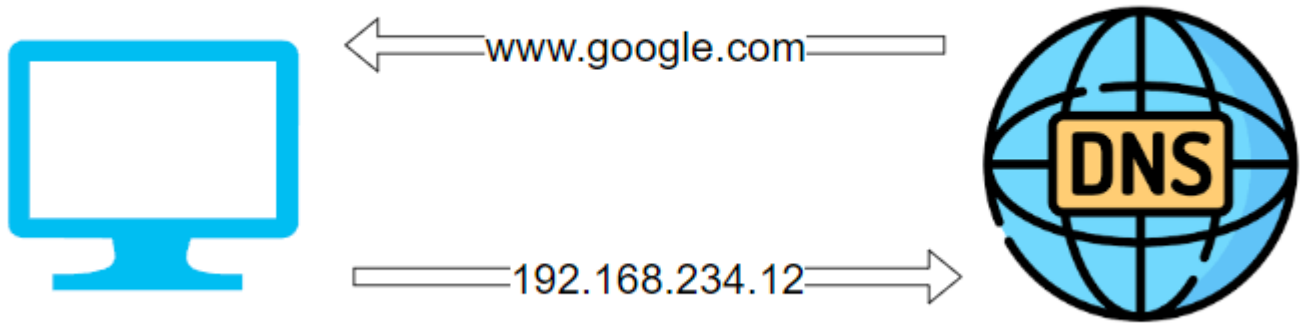
AGENDA FOR DAY 4

1. DNS & Route 53
2. Load Balancing with AWS
3. Hybrid Connectivity & Private Services
4. Troubleshooting Cloud Connectivity

DNS & ROUTE 53

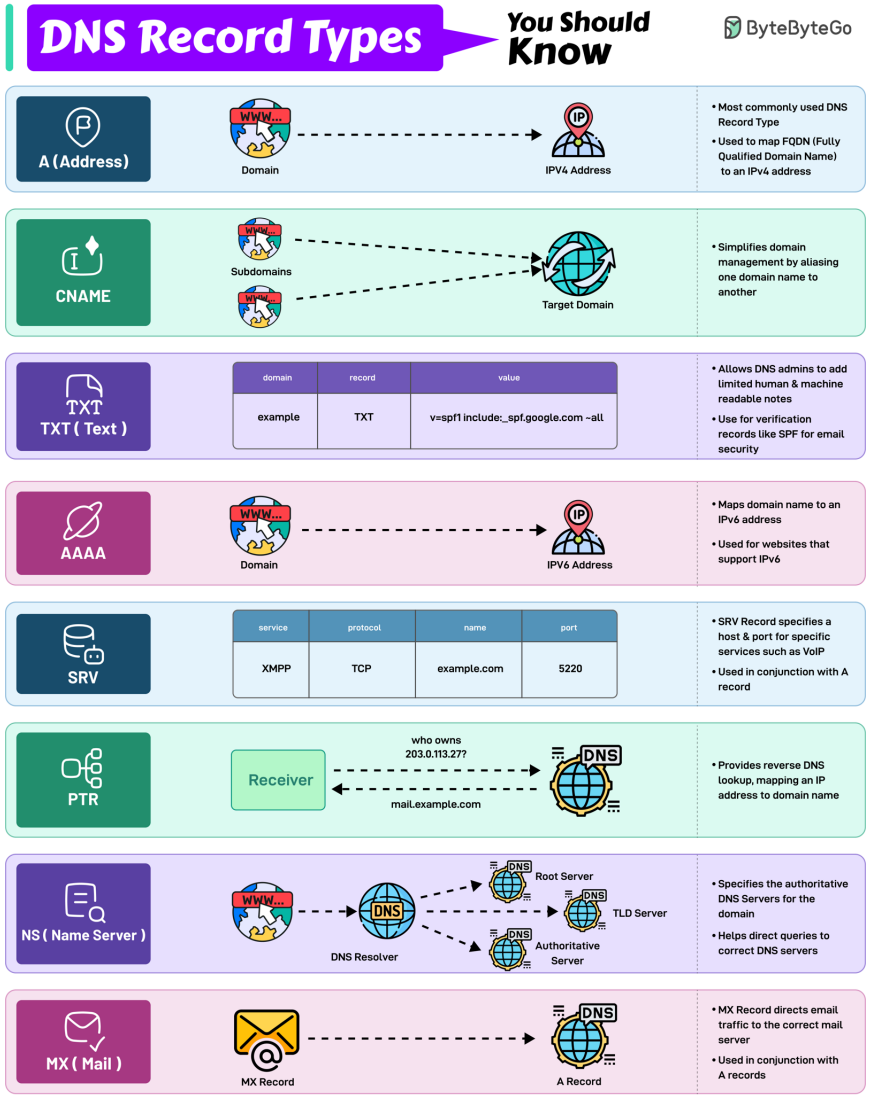
INTRODUCTION TO DNS

- DNS translates human-readable names into IP addresses.
- Hierarchical structure: Root → TLD → Domain → Subdomain.
- Enables scalable and distributed resolution.
- Used both publicly (internet) and privately (VPC internal DNS).



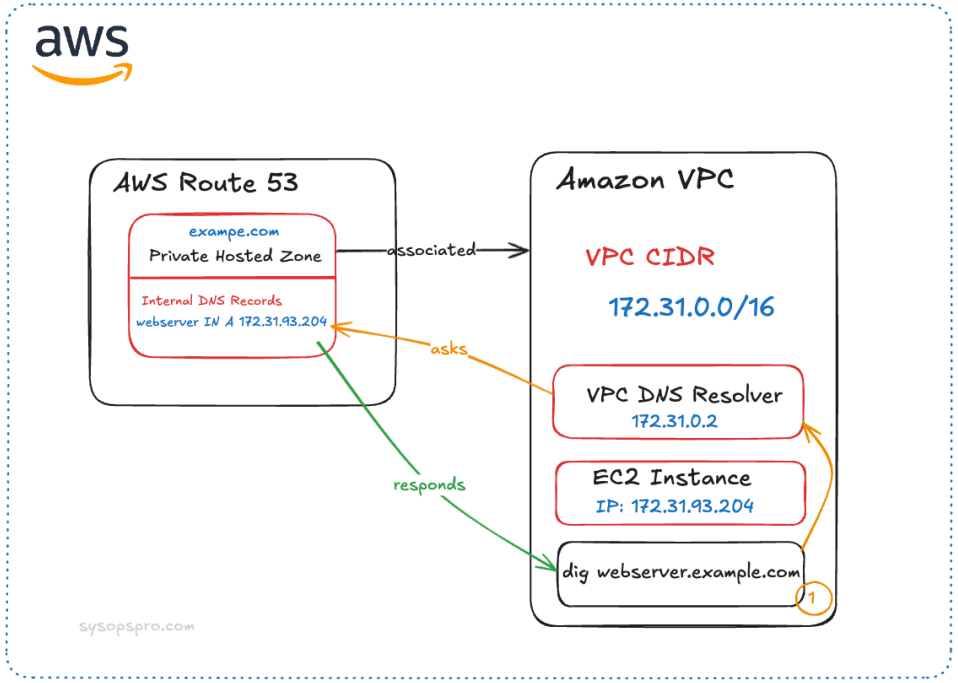
DNS RECORD TYPES

- A / AAAA: Maps name to IPv4/IPv6 address.
- CNAME: Alias to another DNS name.
- MX: Mail exchange records.
- TXT: Text data (e.g., SPF, DKIM).
- Alias: AWS-specific pointer to load balancers, CloudFront, etc.



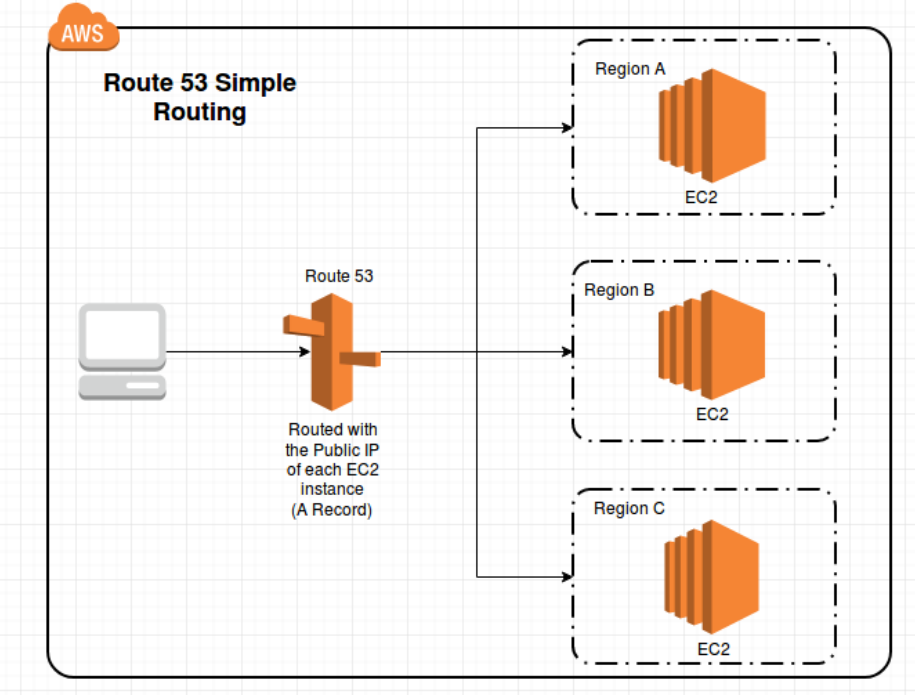
HOSTED ZONES & DELEGATION

- Public Hosted Zone: Accessible from the internet.
- Private Hosted Zone: Resolved only within a VPC.
- Each zone includes record sets managed via Route 53.



ROUTING POLICIES

- Simple: One record per name.
- Weighted: Split traffic between resources.
- Latency-Based: Routes based on user location.
- Failover: Active/passive setup for DR.
- Geolocation: Routes based on country or regior



POP QUIZ:

What is the primary function of DNS?

A. Encrypting network traffic
B. Translating human-readable names into IP addresses
C. Monitoring cloud health
D. Routing only private IPs

POP QUIZ:

What is the primary function of DNS?

A. Encrypting network traffic
B. Translating human-readable names into IP addresses
C. Monitoring cloud health
D. Routing only private IPs

POP QUIZ:

What is the difference between a public and a private hosted zone in Route 53?

A. Public zones are accessible from the internet; private zones resolve only within a VPC
B. Private zones are cached globally
C. Public zones cannot contain MX records
D. Both are identical but billed differently

POP QUIZ:

What is the difference between a public and a private hosted zone in Route 53?

A. Public zones are accessible from the internet; private zones resolve only within a VPC
B. Private zones are cached globally
C. Public zones cannot contain MX records
D. Both are identical but billed differently

POP QUIZ:

Which AWS record type acts as a pointer to other AWS services like ELB or CloudFront?

A. A record
B. CNAME
C. Alias
D. TXT

POP QUIZ:

Which AWS record type acts as a pointer to other AWS services like ELB or CloudFront?

A. A record
B. CNAME
C. Alias
D. TXT

POP QUIZ:

Which Route 53 routing policy directs users based on their geographic location?

A. Simple
B. Weighted
C. Geolocation
D. Latency-Based

POP QUIZ:

Which Route 53 routing policy directs users based on their geographic location?

A. Simple
B. Weighted
C. Geolocation
D. Latency-Based

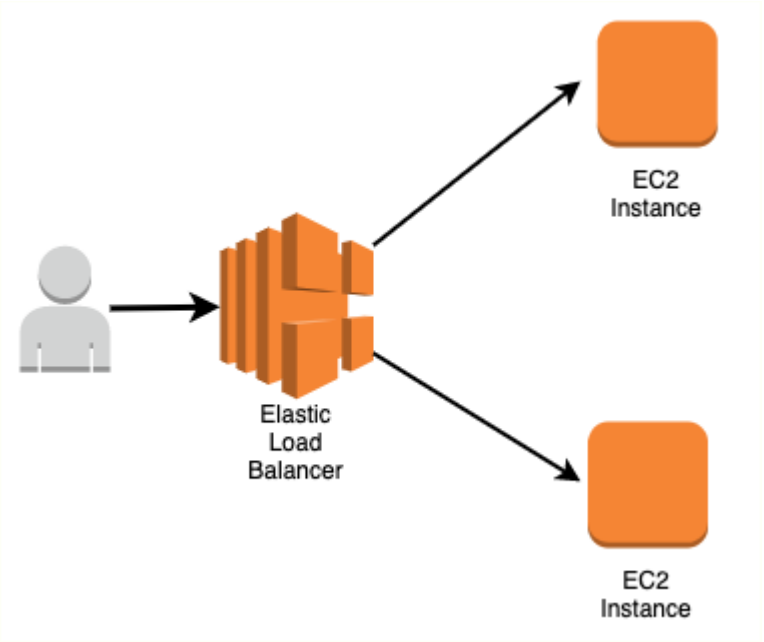
LAB 1: CONFIGURING ROUTE 53

- Goal: Implement scalable DNS management.
- Steps:
  - Register domain and configure hosted zone.
  - Create A, CNAME, and MX records.
  - Set up health checks for failover.
  - Test DNS resolution and propagation.

LOAD BALANCING IN THE CLOUD

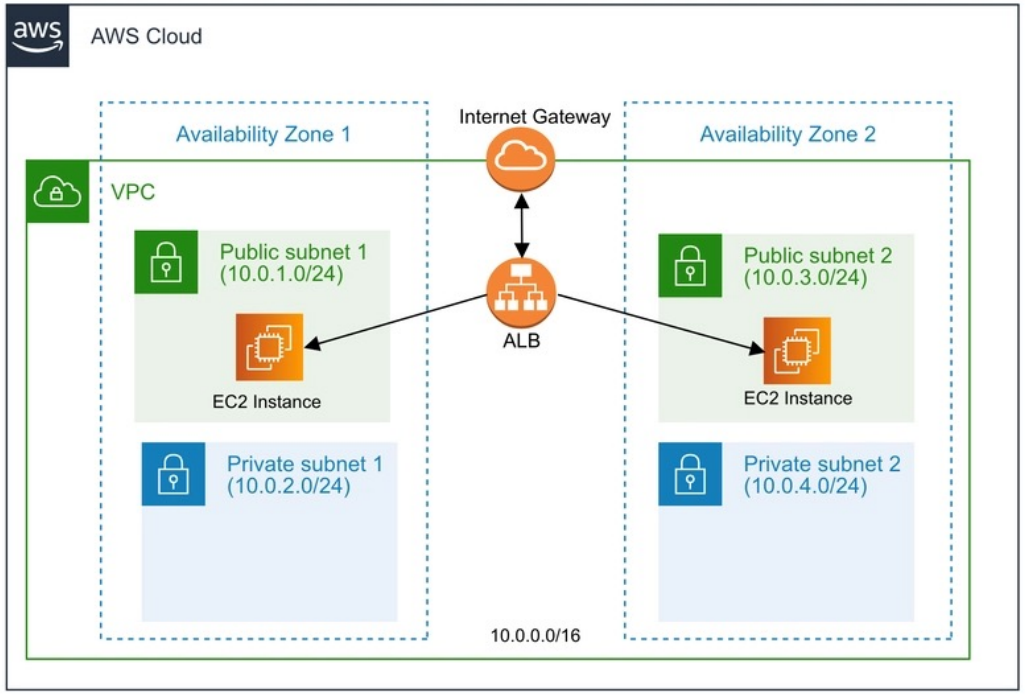
LOAD BALANCING CONCEPTS

- Distributes traffic across multiple instances.
- Ensures high availability and scalability.
- Key AWS types:
  - ALB (Application, Layer 7)
  - NLB (Network, Layer 4)
  - GLB (Gateway, Layer 3/4)



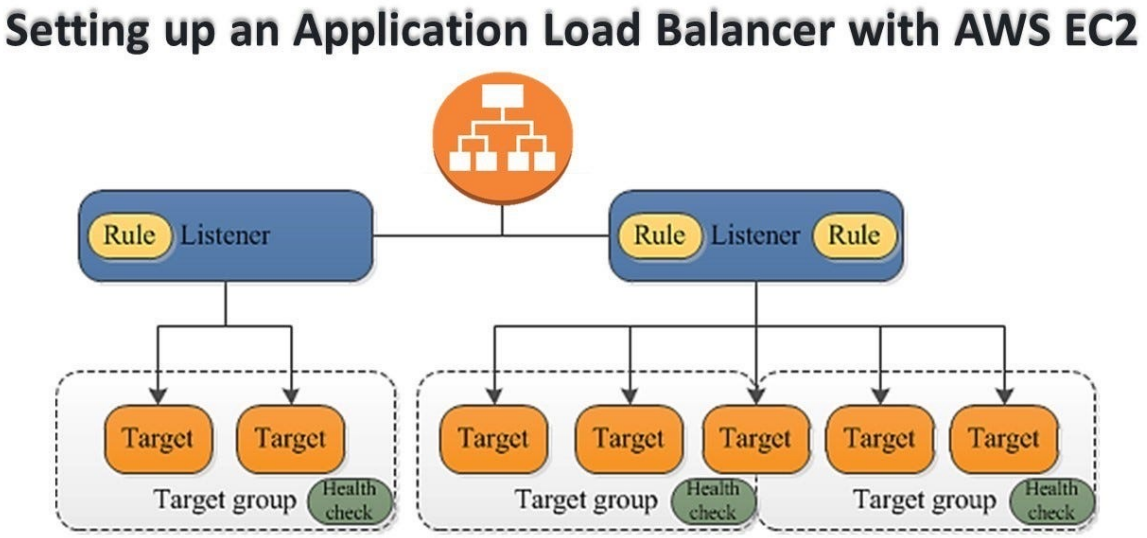
ARCHITECTURE OVERVIEW

- ALB sits in public subnets.
- Targets reside in private subnets.
- Internet Gateway provides external access.
- Multi-AZ design for redundancy.



LISTENERS & TARGET GROUPS

- Listener: Port/protocol (e.g., HTTP 80).
- Rules: Define routing logic (path or host-based).
- Target Group: Registered instances or IPs.
- Health checks ensure targets are responsive.



HEALTH CHECKS & MONITORING

- Periodic HTTP/TCP checks for instance health.
- Automatically removes unhealthy targets.
- Monitor using CloudWatch metrics:
  - UnhealthyHostCount
  - RequestCount
  - TargetResponseTime

SSL CERTIFICATE

- Use AWS Certificate Manager (ACM) for SSL/TLS.
- Terminate SSL at ALB for simplicity.
- Re-encrypt traffic to backend (optional).
- Automatic certificate renewal.

LAB 2: BUILDING A LOAD-BALANCED WEB TIER

- Goal: Distribute traffic across multiple web servers.
- Steps:
  - Deploy Application Load Balancer.
  - Configure target groups and health checks.
  - Set up Auto Scaling Group for elasticity.
  - Test load distribution and failover scenarios.

POP QUIZ:

What is the main function of a load balancer?

A. To encrypt data at rest
B. To distribute network traffic across multiple instances
C. To increase DNS resolution speed
D. To create private VPCs

POP QUIZ:

What is the main function of a load balancer?

A. To encrypt data at rest
B. To distribute network traffic across multiple instances
C. To increase DNS resolution speed
D. To create private VPCs

POP QUIZ:

Which AWS load balancer operates at Layer 7 (Application Layer)

A. NLB
B. GLB
C. ALB
D. CLB

POP QUIZ:

Which AWS load balancer operates at Layer 7 (Application Layer)

A. NLB
B. GLB
C. ALB
D. CLB

POP QUIZ:

What is the role of health checks in load balancing?

A. To update route tables
B. To verify instance responsiveness and remove unhealthy targets
C. To renew SSL certificates
D. To manage IAM permissions

POP QUIZ:

What is the role of health checks in load balancing?

A. To update route tables
B. To verify instance responsiveness and remove unhealthy targets
C. To renew SSL certificates
D. To manage IAM permissions

HYBRID CONNECTIVITY & PRIVATE SERVICES

HYBRID NETWORKING INTRODUCTION

- Combines on-prem and cloud resources.
- Use cases:
  - Data migration
  - DR
  - Centralized authentication
- Key tools: VPN, Direct Connect, Peering, PrivateLink.

VPN ARCHITECTURE

- Customer Gateway (CGW): The on-premises endpoint — typically a physical or software VPN device managed by your organization.
- Virtual Private Gateway (VGW): The AWS-side endpoint attached to your VPC for inbound/outbound VPN traffic.
- Connection:
  - Uses an encrypted IPsec tunnel over the public Internet to ensure data confidentiality and integrity.
- Routing Options:
  - Supports both static routes and dynamic routing using BGP (Border Gateway Protocol).

DIRECT CONNECT OVERVIEW

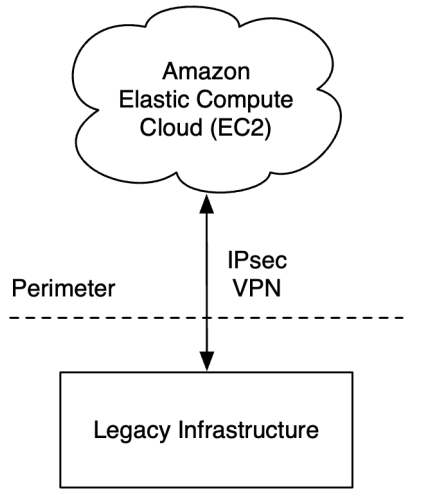
- **Dedicated Fiber Link:** Establishes a private, high-speed fiber connection between your on-premises data center and AWS.
- **No Internet Dependency:** Bypasses the public Internet, providing a more secure and consistent network experience.
- Ideal Use Cases:
  - Low Latency: For real-time applications and high-performance workloads.
  - High Throughput: For large data transfers or hybrid cloud architectures.
  - Regulatory Compliance: Meets strict data sovereignty and security requirements.

VPC PEERING CONCEPTS

Private VPC-to-VPC Communication: Enables secure, private connectivity between two VPCs using the AWS global backbone — no Internet traffic involved.

Manual Configuration: Route tables must be manually updated in both VPCs to enable bidirectional communication.

- Non-Transitive: Peering connections are point-to-point — VPC A can't communicate with VPC C through VPC B.
- Use Case: Ideal for interconnecting environments (e.g., development ↔ production) or multi-account architectures.



Virtual Private Cloud (VPC)

PRIVATELINK (INTERFACE ENDPOINTS)

- Private Service Access: Enables secure, private connectivity to services across VPCs using the AWS internal network.

- How It Works:
  - Service Providers expose services privately through VPC Endpoints.
  - Service Consumers connect to these endpoints without using public IPs.

- Supported Services:
- Works with both AWS-managed services (e.g., S3, EC2 API, Kinesis) and custom applications.

- Key Benefit:
- Eliminates Internet exposure, improving security, latency, and compliance.

TROUBLESHOOTING CLOUD CONNECTIVITY

- VPC Flow Logs: Capture and analyze allowed and denied network traffic for your VPC, subnets, or ENIs.
- Reachability Analyzer: Visually maps network paths to identify configuration or routing issues between resources.
- Network Utilities: Use traceroute, ping, or curl commands to verify connectivity and latency from instances.
- Amazon CloudWatch Metrics:
  - Monitor performance indicators such as latency, packet drops, and throughput trends to detect anomalies.

WRAP-UP & KEY TAKEAWAYS

- DNS enables discoverability and routing.
- Load Balancers provide scalability and availability.
- Hybrid solutions integrate cloud with on-prem securely.
- Next: Multi-AZ design and availability patterns (Day 5).

POP QUIZ:

What is the purpose of hybrid networking?

A. To isolate cloud from on-premises systems
B. To integrate on-prem infrastructure with cloud services
C. To replace VPNs entirely
D. To manage IAM policies

POP QUIZ:

What is the purpose of hybrid networking?

A. To isolate cloud from on-premises systems
B. To integrate on-prem infrastructure with cloud services
C. To replace VPNs entirely
D. To manage IAM policies

POP QUIZ:

What type of connection allows private VPC-to-VPC communication over AWS's backbone network?

A. VPN
B. VPC Peering
C. NAT Gateway
D. CloudFront

POP QUIZ:

What type of connection allows private VPC-to-VPC communication over AWS's backbone network?

A. VPN
B. VPC Peering
C. NAT Gateway
D. CloudFront

POP QUIZ:

Which AWS service provides real-time metrics like latency and packet loss for network monitoring?

A. CloudFormation
B. CloudWatch
C. IAM
D. Route 53

POP QUIZ:

Which AWS service provides real-time metrics like latency and packet loss for network monitoring?

A. CloudFormation
B. CloudWatch
C. IAM
D. Route 53

LAB 3: VPC PEERING HYBRID CONNECTIVITY

- Goal: Connect multiple VPCs and on-premises networks.
- Steps:
  - Create VPC peering connections.
  - Configure Site-to-Site VPN tunnel.
  - Set up routing for hybrid connectivity.
  - Test cross-VPC and on-premises communication.