Networking in AWS
Overview

- AWS networking services including:
  - VPC – Extend your network into a virtual private cloud
  - EIP – Elastic IP
  - Direct Connect – Physical cross connect into AWS
  - ELB – Managed load balancer service
  - Route53 – Managed DNS service
Amazon VPC
Amazon VPC

- Virtual network topology that you define
- Your own logically isolated section of AWS
- Complete control of your networking environment
  - IP ranges
  - Subnets
  - Routing tables
  - Gateways
- Multiple Connectivity Options
- Advanced Security Features
Networking Building Blocks

Amazon Virtual Private Cloud (VPC)

- Bring your own network
Networking Building Blocks

Amazon Virtual Private Cloud (VPC)

- Bring your own network
- Create your own subnets
Networking Building Blocks

Amazon Virtual Private Cloud (VPC)

- Bring your own network
- Create your own subnets
- Configure custom routing rules
Plan your VPC IP space before creating it

- Consider future AWS region expansion
- Consider future connectivity to corporate networks
- Consider subnet design
- VPC can be /16 between and /28
- CIDR cannot be modified once created
- Overlapping IP spaces = future headache
Network Building Blocks

Network Control

- Security Groups
Network Building Blocks

Network Control

- Security Groups
Network Building Blocks

Network Control

- Security Groups
- Network Access Control Lists
Network Building Blocks

Network Control

- Security Groups
- Network Access Control Lists
- Routing rules
Network Building Blocks

**VPC Gateways**

- Virtual Private Gateway (VGW)
  - IPSec VPN
Network Building Blocks

**AWS Direct Connect**

- Virtual Private Gateway (VGW)
  - IPSec VPN
  - AWS Direct Connect
Network Building Blocks

VPC Gateways

- Virtual Private Gateway (VGW)
- Internet Gateway (IGW)
Network Building Blocks

Connecting to Instances

- IP Address
  - Private IP
  - Public IP (EIP or dynamically assigned)
Network Building Blocks

Connecting to Instances

- IP Address
  - Reassociating EIPs
Network Building Blocks

Connecting to Instances

• IP Address
• Load Balancer
  • External Elastic Load Balancing
Network Building Blocks
Connecting to Instances

- IP Address
- Load Balancer
  - Mid-tier Elastic Load Balancing
Network Building Blocks
Connecting to Instances

- IP Address
- Load Balancer
  - Intranet-facing Elastic Load Balancing
VPC NAT Gateway

- High availability – built-in redundancy
- High bandwidth – up to 10Gbpt
- Managed by Amazon
- Control NAT IP address by assigning an EIP at launch
- View NAT gateways’ traffic using Flow Logs
- NAT gateways support TCP, UDP, and ICMP protocols
- Network ACLs apply to NAT gateway’s traffic
- CloudTrail Support
VPC Endpoints: Amazon S3 access without an Internet Gateway

- No IGW
- No NAT
- No public IPs
- Free
- Robust access control
Connecting to other VPCs - VPC peering

VPC 172.31.0.0/16

VPC Peering

VPC 10.0.0.0/16

<table>
<thead>
<tr>
<th>Private Route Table</th>
<th>Destination</th>
<th>Target</th>
</tr>
</thead>
<tbody>
<tr>
<td>172.31.0.0/16</td>
<td>Local</td>
<td></td>
</tr>
<tr>
<td>10.0.0.0/16</td>
<td>VPC Peer</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Private Route Table</th>
<th>Destination</th>
<th>Target</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.0/16</td>
<td>Local</td>
<td></td>
</tr>
<tr>
<td>172.31.0.0/16</td>
<td>VPC Peer</td>
<td></td>
</tr>
</tbody>
</table>
Default VPCs

Default VPC
• Simplicity and Convenience
• Automatically assigned network and subnets

Security of VPC
• Customer may create additional subnets and change routing rules
• Additional network controls (Security Groups, NACLs, routing)
• Hardware VPN options between corporate networks
• Instances in default subnets have Security Group–controlled public and private IPs
# IP Addressing

<table>
<thead>
<tr>
<th>Default VPC</th>
<th>Virtual Private Cloud</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dynamic Private IP</td>
<td>Dynamic or Static Private IP Address</td>
</tr>
<tr>
<td>Dynamic Public IP</td>
<td>None by default (can be created with publicIP=true)</td>
</tr>
<tr>
<td>Optional Static Public IP (EIP)</td>
<td>Optional Static Public IP (EIP)</td>
</tr>
<tr>
<td>AWS-provided DNS names</td>
<td>AWS-provided public DNS lookup</td>
</tr>
<tr>
<td>• Private DNS name</td>
<td>AWS-provided private DNS names</td>
</tr>
<tr>
<td>• Public DNS name</td>
<td>Customer-controlled DNS options</td>
</tr>
</tbody>
</table>
Recap

1. Create VPC
2. Create Subnets – Across Multiple AZ’s
3. Configure Route Tables
4. Create Gateways – IGW and VGW (VPC and DX)
5. Configure Security – Security Groups and NACLs
6. Create VPC Endpoints
7. Create NAT Gateway
8. Configure VPC Peering
9. Create Instances
Direct Connect
AWS Direct Connect

- 1 Gbps or 10 Gbps fiber cross connect
  - 50M, 100M, 200M, 300M, 400M, & 500M available through APN Partners
- Consistent Network Performance
- Compatible with all AWS Services
- Private connectivity into your VPC
- Reduce Bandwidth Charges
AWS Direct Connect
Cross-Connect Details

- Decide on an AWS DX location and port size
- Use AWS Management Console to create connection request(s)
  - Sends Letter of Authorization – Connecting Facility Assignment (LOA-CFA) via email
- Establish WAN connectivity to DX location*
  - APN Partner or a network carrier of your choice
- Provide LOA-CFA to an APN Partner or your service provider to establish the connection at the DX location
- Use AWS Management Console to configure one or more virtual interfaces
- [AWS DX Locations](#)

* Can be done in parallel with remaining steps once the AWS DX location has been selected
3

ELB
Elastic Load Balancing

• In-Region Load Balancing Service

• Distributes traffic across multiple Availability Zones
  – HTTP/S, TCP/S

• Built-in Health Check

• Fully fault-tolerant
  – Can span multiple AZs
ELB Considerations

- ELB is a service, but runs on EC2
- The IP Addresses will change over time
  - Use CNAME records in DNS or Route 53 “Alias” records
  - Never use an A record
- SSL is supported
  - Client SSL Termination
  - Backend ELB-to-Server mutual SSL
- Cross-Zone Load Balancing
- Sticky sessions
- Best Practices for Evaluating ELB
  - http://aws.amazon.com/articles/1636185810492479
Route 53
Route53

- Managed DNS Service
- Domain Name Registration
- Fast Zone Updates
- Multiple DNS routing features
  - Geo Based Routing
  - Latency Based Routing
  - Weighted Round Robin
  - DNS Failover
Route53

- Zone Apex integration
  - ELB, S3, CloudFront
- Private DNS within VPC
  - Internal DNS names not exposed to Internet
  - Supports split-horizon DNS
Route53

Getting Started

• Register DNS name with Route 53 or transfer from external registrar

• Create a Route53 hosted zone
  • AWS Management Console or API

• Update your domain registrar (if transferred)
  • Provide Route53 name servers associated with your hosted zone

• Create DNS resource records for your domain
Any Questions?