AWS Cloud Computing - Week 4 (VPC, R53, WAF)

VPCs

- DCs within an AZ are interconnected, and AZs are connected by high speed links.
- While regions are dispersed across geographic regions to avoid catastrophic events, AZs within a region are localized within several miles (let's say 60 miles) which may not align with certain federal or industry criteria for DR or BC.
- Note that AZs are different across accounts. This is intentional to provide some isolation and avoid wide-spread customer outages. In cases where using the same AZ across accounts is important, the AZ-ID should be used to provide alignment.
- VPC (associated with AZs), region and global services
- CIDR is "Classless Inter-Domain Routing", and is simply a short form of how network is divided.
- Maximum CIDR is /16, minimum is /28
- CIDR calculator: https://www.subnet-calculator.com/cidr.php
- AWS reserved IP space:
    - 10.0.0.0: Network address.
    - 10.0.0.1: AWS reserved for the VPC router.
    - 10.0.0.2: AWS reserved for the VPC DNS router service (always located in the primary CIDR). AWS also reserves the base of each subnet range plus two for all CIDR blocks in the VPC. Reference Amazon DNS server.
    - 10.0.0.3: AWS reserved for future use.
    - 10.0.0.255: AWS reserved for the network broadcast address (note that AWS does not support broadcast in a VPC).
- NAT Gateways have Elastic IPs (can be used in accept list since they are static).
- NAT Gateway does have throughput and connection limits which should be considered. One per AZ is recommended for HA, but also throughput.

Routing

- Routing is crucial!!
- Public subnet is any that has route to IGW.
- NAT Gateway must be in public subnet
- Can use one or more route table, but a subnet must be associated to a single route table
- Shortest (most specific) route takes precedence
- Routes cannot overlap
- Gets complicated (management) as VPCs grow and mesh network takes shape
- Alternative options exist such as shared VPCs, and Transit Gateway (next slide)

- Preferred solution is Transit Gateway for routing across VPCs, as well as between VPCs and on-premise
- Some use cases, such as really high volume traffic (100's of TB) would prefer VPC peering to minimize costs. Use TGW in general, and VPC Peering for edge case.

DNS (Route 53)

- Blue/Green: Updating the alias record, you can route traffic from the blue environment to the green environment. You can shift traffic all at once or you can do a weighted distribution. For weighted distribution with Amazon Route 53, you can define a percentage of traffic to go to the green environment and gradually update the weights until the green environment carries the full production traffic. This provides the ability to perform canary analysis where a small percentage of production traffic is introduced to a new environment. You can test the new code and monitor for errors, limiting the blast radius if any issues are encountered. It also allows the green environment to scale out to support the full production load if you're using Elastic Load Balancing(ELB), for example. If issues arise during the deployment, you can roll back by updating the DNS record to shift traffic back to the blue environment. Although DNS routing is simple to implement for blue/green, you should take into consideration how quickly can you complete a rollback. DNS Time to Live (TTL) determines how long clients cache query results. However, with earlier clients and potentially clients that aggressively cache DNS records, certain sessions may still be tied to the previous environment.
- ASG swap: A blue group carries the production load while a green group is staged and deployed with the new code. When it's time to deploy, you simply attach the green group to the existing load balancer to introduce traffic to the new environment. For HTTP/HTTPS listeners, the load balancer favors the green Auto Scaling group because it uses a least outstanding requests routing algorithm. As you scale up the green Auto Scaling group, you can take blue Auto Scaling group instances out of service by either terminating them or putting them in Standby state

#great-learning #mentoring