|  |  |
| --- | --- |
| Student | Sean Hunt |
| Student Number | l00138043 |
| GitHub | https://github.com/hunty-atu/GHDemo1SH/ |
| Course | PGDip DevOps – IAC – Cloudformation 50% |

**Introduction:**

A default VPC comes with a public subnet in each Availability Zone, an internet gateway, and settings to enable DNS resolution. Therefore, you can immediately start launching Amazon EC2 instances into a default VPC. But for the purpose of this assignment and following AWS best practice, new resources will not be created in the default VPC due to non-critical security features applied. To resolve this, a secondary target <Demo VPC> is launched for resources to be created in for Security.

**Design Build and Test:**

VPC is a virtual private cloud and because a VPC is private, only the private IP ranges are allowed. A maximum of five VPC’s can be created within a region and a further five subnets are allowed per VPC. For each CIDR range:

* Min size is /28 = 16 IP addresses.
* Max size is /16 = 65,536 IP Addresses.

A <Demo VPC> was created using IPv4 CIDR block 10.0.0.0/16 which allocates the maximum 65,536 addresses for the overall network range. It covers from 10.0.0.0 to 10.0.255.255 as per <https://ipaddressguide.com/cidr>. The 10.0.0.0/ range was chosen so not to conflict with the AWS default VPC’s 172.31.0.0/range. A VPC configuration with default shared tenancy was chosen as opposed to dedicated tenancy to lower costs. The resulting Network ACL, DHCP and Route table were created in the backend by AWS. Explicit subnet associations and route tables were configured for routing traffic and creating firewalls because it's not using the default VPC.

Subnets are akin to a smaller network within <Demo VPC>. Four subnets were created within the VPC then tied to availability zones x2. Within each AZ, a public & private subnet was created for high availability. A public subnet is usually smaller than a private subnet due to containing public facing resources such as load balancers. Whereas the private subnet hosts the full backend, such as webservers with load balancers and databases. Furthermore, consideration is given to allocation to IP address range where AWS reserves five IP addresses (first 4 and last 1) in each subnet for; network address, VPC router, mapping to DNS, future use, network broadcast address (not supported). AWS randomly assigns subnets from the CIDR range provided. VPC subnets ranges/ CIDR should not overlap.

EC2 instances launch with a unique private IP address to communicate internally. A Public IP can be accessed from anywhere, this IP changes when an instance is restarted, unless an elastic IP address is created and allocated. Good practice is to use a public IP and assign a DNS or use load balancing. The public EC2 instance was created with security group rules then configured.

***\*\*Note:***Security groups (SG’s) are firewalls that are applied at instance level to control inbound/ outbound traffic. By default, Security groups are stateful, all outbound traffic is allowed out. An instance can be a member of multiple security groups, multiple security groups can be applied to an instance. Security groups are fundamental to connect into Virtual Machines using AWS. A security group is created on an EC2 instance to control inbound/ outbound traffic. They regulate access to Ports and IP Address access. For e.g. All inbound traffic is allowed in from any source over TCP port 22 (reserved for SSH). By default, Security groups are stateful, all outbound traffic is allowed out. An instance can be a member of multiple security groups, multiple security groups can be applied to an instance. CIDR is used for security group rules, or networking in general. It can be used to block a single IP address. A CIDR has two components – the base IP and a slash /.

Security group rules required SSH & HTTP to allow all traffic from anywhere 0.0.0.0/0 over Port 22 & 80. The public facing EC2 instance placed in myPublicSubnetA. Thus, it currently has no internet connectivity and creating an internet gateway will allow internet access.

The IGW gives access to the internet. An IGW scales horizontally and provide high availability and redundancy, it is created separately from a VPC. A VPC can only be attached to one IGW and visa versa. IGW serves as NAT for the instances that have a public IPV4. IGW on their own do not allow internet access, a route table must also be configured. In effect, the public EC2 requires a roadmap through the router to the IGW.

Route tables: Next public route tables were configured and associated for public subnets within <Demo VPC>. A further route destination (0.0.0.0/0) was added to the public route table. Thus, devices within network outside of the local range of IP address assigned (10.0.0/16), then must go across the IGW (0.0.0.0/0).

NAT instances (Network address translation) allows instances in private subnets to connect to internet. NAT must be launched in public subnet and must disable EC2 flag: Source/ Destination check. All traffic from Private EC2 will route through NAT instance and through IGW to the internet.

A NAT instance is chosen instead of a NAT Gateway to lower costs. The NAT SG is configured with HTTP access from our <Demo VPC> IP range. (HTTPS is optional). \*\* *A NAT gateway is best recommended for availability and larger networks\*\*.*

A private instance is configured in PrivateSubnetA so it will receive a private IP that can be accessed anywhere inside the VPC only, such as, the Public EC2 instance can SSH into the private instance. The private route table is then created to cross into the NAT instance. Next private route tables were configured and associated for private subnets within <Demo VPC>.

VPC endpoints allow to connect services using private network instead of a public www network. They remove the need for IGW, NAT to access AWS Services. There are two types 1). *Interface:* provision an ENI (private IP address). 2). *Gateway:* provisions a target and must be used in a route table – S3 and Dynamo DB.

Create an IAM role to allow private EC2 instance to access S3. To SSH into private instance requires a bastion host configured. This resolves jumping from outside network through public EC2 instance to EC2 private instance. Thus, Bastion host security group only allows that one IP address through. *Then using Putty, chmod 0400 private-keypair and SSH ec2-user@10.\*.\*.\*. (Instance)*. Create VPC Endpoint and associate com.amazonaws.eu-west-1.s3 with privateSubnetA in <Demo VPC>. Ensure DNS setting for resolution in VPC/ Traffic doesn't go straight into route table Gateway.

Flow Logs capture info about IP traffic going into interfaces (VPC/Subnet/ENI). It helps monitor and troubleshoot connectivity issues. Flow Logs can be stored in S3 and exported to Athena or CloudWatch logs insights.

VPN is used to connect the VPC to a corporate network. Must create a customer gateway on Corporate data center (DC) i.e. on Microsoft server (software) or Sonic/Juniper Firewall (hardware). Attached to the VPC is a VPN gateway. Connecting the two is a site-to-site VPN.

RDS database mySQL engine is launched on an instance. A security group is created. Cloudformation does not offer Enable automatic backups (Max 35 days) & max storage (1TB ) which can be updated via AWS-CLI later. An EC2 instance is launched with a WordPress script added.

From there connect from EC2 public IP address to WP site with credentials (DB\_Name, U/P/ endpoint from DB). New window with config file is shown and install onto EC2 instance. Cd /var/www/html, run wp-config.php.Return to EC2 public IP and login.

**CloudFormation limitation:** Unable to auto-assign an AUTO IPv4 address in the subnet, so all future instances created within Subnet have this setting.

Reason: Subnets created by AWS are called default subnets. These subnets have their auto-assign property set to true by default. Non-default subnets, set the property's value to false by default. The one exception to this rule is a subnet created by the Instance Launch Wizard. The wizard sets the auto-assign property to true.

* The AWS portal can be used to modify this setting.
* The AWS CLI can enable or disable <aws ec2 modify-subnet-attribute --subnet-id <your-subnet-id> --map-public-ip-on-launch>

Fix: Auto-assign an IPv4 address at instance level instead. So must be set at AWS::EC2::Instance > "NetworkInterfaces" for all EC2 instances in the Public subnet. Not required at the Private Subnet.

**Best practice to tidy up the code** is via nested stacks. For this assignment code was seperated into a number of yaml files. Further info can be found via:

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/best-practices.html>

**Security CIDR** is used for security group rules, or networking in general for e.g. It can be used to block single IP address. A CIDR has two components – the base IP and a slash /. For Reliability and high availability consideration was assessed spreading across availability zones. The architecture created above is fully secure, albeit EBS, EFS, Scalability and security of an instance can be further increased at Load balancers (application, network) level. S3 & S3 versioning, encryption, storage classification I.e. general purpose is an example of an AWS storage service.