Author: Norman Wong Chiew Look

VPC Subnet Design

This is an over restrictive VPC design to lock down inbound/outbound traffic to ensure that services are only sending or receiving traffic from the source/destination that they only need.

3 availability zones. Therefore:

2 subnets bit (2^2 = 4. For **3 AZs** and **1 spare**)

Each availability zone needs a public and private tier. Thus:

1 subnet bit (2^1) = 2. For 1 **Public** and **Private Tier**

Each Public tier will have an isolated subnet for 2 services, ALB and NAT. Thus:

1 subnet bit (2^1) = 2. For 1 **ALB-Tier** and **NAT-Tier**

Each Private Tier will have an isolated subnet for Web-tier and Data-tier. Thus:

1 subnet bit (2^1) = 2. For 1 **Web-Tier** and **Data-Tier**

Each data tier has an isolated subnet for 2 services, MySQL RDS and Redis Elasticache. Thus:

1 subnet bit (2^1) = 2. For 1 **MySQL Tier and Redis Tier**

Ipv4 subnets references used for the VPC

Development network

Parent network: `10.0.0.0/16:`

```
10.0.0.0/18 — AZ A

      10.0.0.0/19 - Public

            10.0.0.0/20 – ALB-tier

            10.0.16.0/20 – NAT-tier

      10.0.32.0/19 – Private

            10.0.32.0/20 – WebApp-tier

            10.0.48.0/20 – Data-tier

                  10.0.48.0/21 – MySQL-tier

                  10.0.56.0/21 – Redis-tier

10.0.64.0/18—AZ B
```

```
      10.0.64.0/19 — Public

            10.0.64.0/20 – ALB-tier

            10.0.80.0/20 – NAT-tier

      10.0.96.0/19 – Private

            10.0.96.0/20 – WebApp-tier

            10.0.112.0/20 – Data-tier

                  10.0.112.0/21 – MySQL-tier

                  10.0.120.0/21 – Redis-tier

10.0.128.0/18—AZ C

      10.0.128.0/19 — Public

            10.0.128.0/20 – ALB-tier

            10.0.144.0/20 – NAT-tier

      10.0.160.0/19 - Private

            10.0.160.0/20 – WebApp-tier

            10.0.176.0/20 – Data-tier

                  10.0.176.0/21 – MySQL-tier

                  10.0.184.0/21 – Redis-tier

10.0.192.0/18—Spare
```

Production-Sydney network

Parent network： 10.1.0.0/16:

```
10.1.0.0/18 — AZ A

      10.1.0.0/19 - Public

            10.1.0.0/20 – ALB-tier

            10.1.16.0/20 – NAT-tier

      10.1.32.0/19 – Private

            10.1.32.0/20 – WebApp-tier

            10.1.48.0/20 – Data-tier
```

```
                  10.1.48.0/21 – MySQL-tier

                  10.1.56.0/21 – Redis-tier

10.1.64.0/18—AZ B

      10.1.64.0/19 — Public

            10.1.64.0/20 – ALB-tier

            10.1.80.0/20 – NAT-tier

      10.1.96.0/19 – Private

            10.1.96.0/20 – WebApp-tier

            10.1.112.0/20 – Data-tier

                  10.1.112.0/21 – MySQL-tier

                  10.1.120.0/21 – Redis-tier

10.1.128.0/18—AZ C

      10.1.128.0/19 — Public

            10.1.128.0/20 – ALB-tier

            10.1.144.0/20 – NAT-tier

      10.1.160.0/19 - Private

            10.1.160.0/20 – WebApp-tier

            10.1.176.0/20 – Data-tier

                  10.1.176.0/21 – MySQL-tier

                  10.1.184.0/21 – Redis-tier

10.1.192.0/18—Spare
```

Production-{Insert Region Name} network

Parent network： `10.2.0.0/16 – 10.255.0.0/16`