Se elige como host de nuestra infraestructura Amazon web services, dentro del cual se eligió la región US-EAST-1 ya que en esta misma podemos encontrar absolutamente todos los servicios de aws, para tener una infraestructura resistente al fallo de una Availability zone se eligió desplegarla entre 2 de las mismas.

En caso de que nuestra aplicación fuera de una alta criticidad también podríamos agregar a nuestra infraestructura la posibilidad de recuperarse ante una falla regional con Pilot light que es una estrategia que replica nuestros datos a otra región y mantiene encendidas réplicas de nuestras bases, pero apagadas nuestras instancias.

La infraestructura consiste de un frontend hosteado en instancias EC2 con nginx dentro de una subred pública distribuidas equitativamente entre 2 AZ que tienen como balanceador un Application load balancer, estas instancias se comunican con otro ALB el cual redistribuye la carga entre otras instancias EC2 en una subred privada que conforman el backend de nuestra aplicación las cuales también están distribuidas entre ambas AZ, estas mismas envían datos a Aurora nuestra base relacional que se encuentra en la subred privada n°2 la cual crea una replicación sincrónica en nuestra segunda AZ, también se eligió DynamoDB como nuestra base de datos no relacional la cual recibe datos de nuestra aplicación backend a través de un VPC Gateway Endpoint, ya que dynamodb es un servicio público de aws y no queremos que nuestros datos se transfieran a través del internet con lo cual de esta manera hacemos que esta transferencia de datos sea privada.

Para asegurar nuestra infraestructura al máximo coloque:

* NACLs en cada subred de nuestra VPC
* Configure security groups a nuestro ALB público, luego a nuestras instancias frontend para que solo puedan recibir tráfico del ALB público, luego a nuestro ALB privado para que solo pueda recibir tráfico de nuestras instancias frontend y a nuestras instancias backend para que solo puedan recibir tráfico del ALB privado.-
* Tomé la decisión de encriptar el tráfico tanto de Route 53 a cloudfront como cloudfront a nuestro ALB público con certificados SSL que almacenamos en nuestro certificate manager y en frente de Cloudfront configurar tanto Shield como WAF para evitar ataques DDOS y agregar un layer de seguridad extra a las peticiones http/https
* Se configura Amazon Inspector en todas las instancias EC2 para que monitoree las mismas

Se elige configurar nuestra infraestructura con Cloudfront y Route 53, para mejorar la latencia que brindamos de nuestra web al usuario final ya sea a nivel dns como a nivel distribución de contenido, ya que en Route 53 podremos configurar la latency policy y con cloudfront que al recibir una petición de descarga de contenido de nuestra web utilice las edge location más cercanas al usuario final para brindarle la menor latencia posible

* Para mejorar la seguridad de la utilización de los mismos también configure el logeo hacia un bucket s3 el cual Config estaría monitoreando y en caso de que algo saliera de lo habitual podría enviar una notificación vía SNS o remediar el problema (También lograrían al bucket los ALB)

Algunas cosas me quedaron fuera del diagrama de red ya que se me acabó la cantidad de elementos de la versión free de lucidchart pero no quería dejar de mencionarlas.