General setup (non task related)

CloudTrail must be enabled for all regions and store all trails (API calls) in dedicated S3 bucket with the limited access and enabled log integrity.
Using an MFA-protected bucket for AWS CloudTrail helps to protect your versioned log files from being accidentally or intentionally deleted in case your access credentials are compromised.
For the proper cost estimation, cost allocation tags must be enabled.

The specific setup for Home task

Network and compute architecture

We should have at least 2 load balancers in 2 AWS regions to avoid AWS region outage. Route53 with latency based routing and health check will distribute traffic between available AWS regions.
In each region, there will be Autoscaling group (ASG) with 3 EC2 instances. The EC2 are evenly distributed between all availability zones to avoid AZ outage.
Load balancers and Target group will constantly check all EC2 instances for proper work and inform ASG to destroy and run new EC2 instance.
Once we have reached specified thresholds in ASG for the CPU, the memory, the network bandwidth, and counters related to the application, autoscaling policies would trigger the appropriate action.
In addition, EC2 instances must contain Cloudwatch log agent to deliver all important system and application logs to Cloudwatch.

Deployment strategy

EC2 image in ASG should be prebaked with the latest version of the application code to minimize the delivery time. If it is impossible, we should use Application lifecycle hooks to put instance in the pending.wait state while building the application from the source code to avoid service interruption. Another option is to use Blue-Green deployment procedure.

DB architecture

For DB storage, I decided to use DynamoDB. Scrip is in “additional docs” folder.
To avoid AWS Region outage we should enable Dynamodb stream after creation the DB.
We should enable autoscaling for Read and Write Capacity units.