Web Service Runbook

Short Description

Ultimately, this Web Service employs infrastructure that can be immediately applied to a network to get several databases and web services up and running using Terraform and Ansible, as IT automation software.

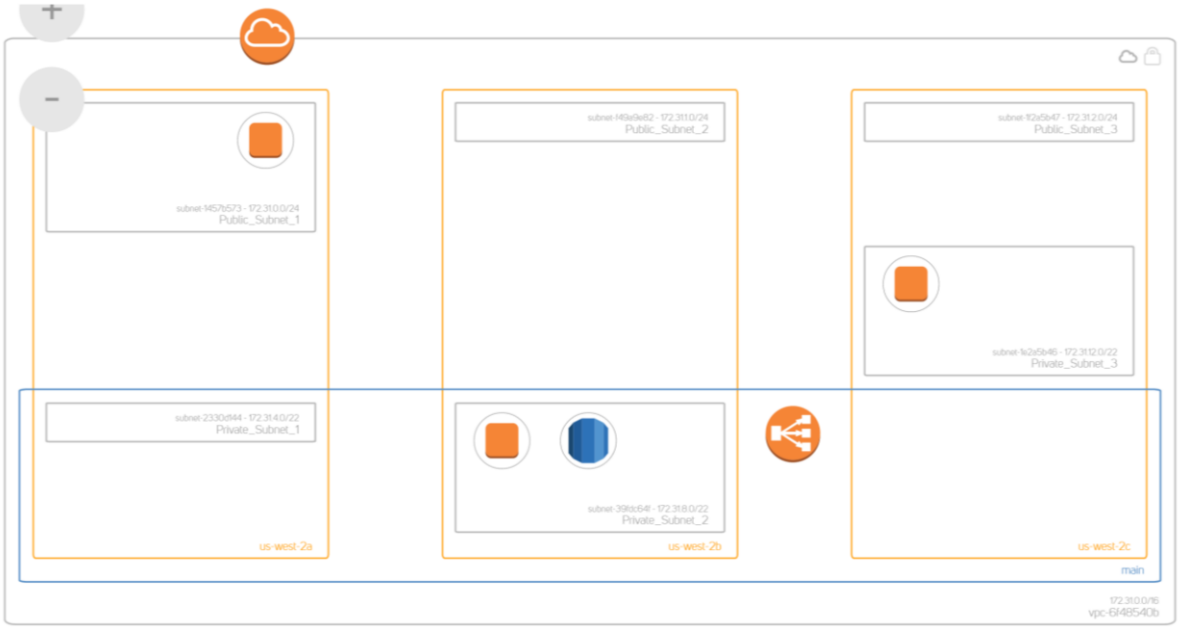
Required Software

Terraform: Uses the resources below

- RDS, using AWS
- One VPC
- One Nat Gateway
- Two Route Tables
- One Internet gateway
- Load Balancer
- Two EC2 Instances
- MariaDB-Client
-Nginx
-Composer

Ansible – Runs two playbooks db.yml and web.yml

Architecture Diagram



Deployment

Running Terraform:
./terraform apply – to apply the infrastructure
Enter user-selected password

To SSH into web server instance from Shell

Enter Downloads folder
Enter: ssh -i "cit360.pem" ec2-user@ec2-35-164-12-197.us-west-2.compute.amazonaws.com

Run Ansible Playbooks, configure Hosts.ini file to use Private IPs instead of localhost

ansible-playbook -i hosts.ini db.yml –ask-vault-pass
ansible-playbook -i hosts.ini web.yml –ask-vault-pass

Issues

Title: System Overload
Description: A server overloads can be caused by a large bottleneck influx of traffic which clogs the network. Typically, this happens during peak traffic hours.
Remediation Steps: Do a deep capacity analysis of the network traffic, to ensure there is a balanced ratio of virtual servers, examining the loads on the CPU and memory to the amount of "work" needed on each server. Sometimes this means improving the physical hardware to support a higher capacity.

Title: DDos attack
Description: Distributed Denial of Service attack basically bombards a server with an overflow of packets that the server is not able to handle create a bottleneck state, which makes the service (server) become unavailable.
Remediation Steps: Several technical things can be done, 1) rate limit your router to prevent the server from being overwhelmed, add filters to tell the router to drop packets from "suspicious sources" 3) timeout half-open connects more aggressively, 4) drop spoofed and malformed packets. If the problem persists, call a DDoS specialist to analyze your network setup.

Title: Natural Disaster
Description: Natural Disaster wipes out all your electricity thereby taking your severs down.
Remediation Steps: Possibly look into investing in cloud technology some kind of SaaS type of technology. For example, with Amazon there are server farms, which in case "your server" goes down there is redundancy so that it is backed up on another server which takes command.