<Curriculum> Runbook

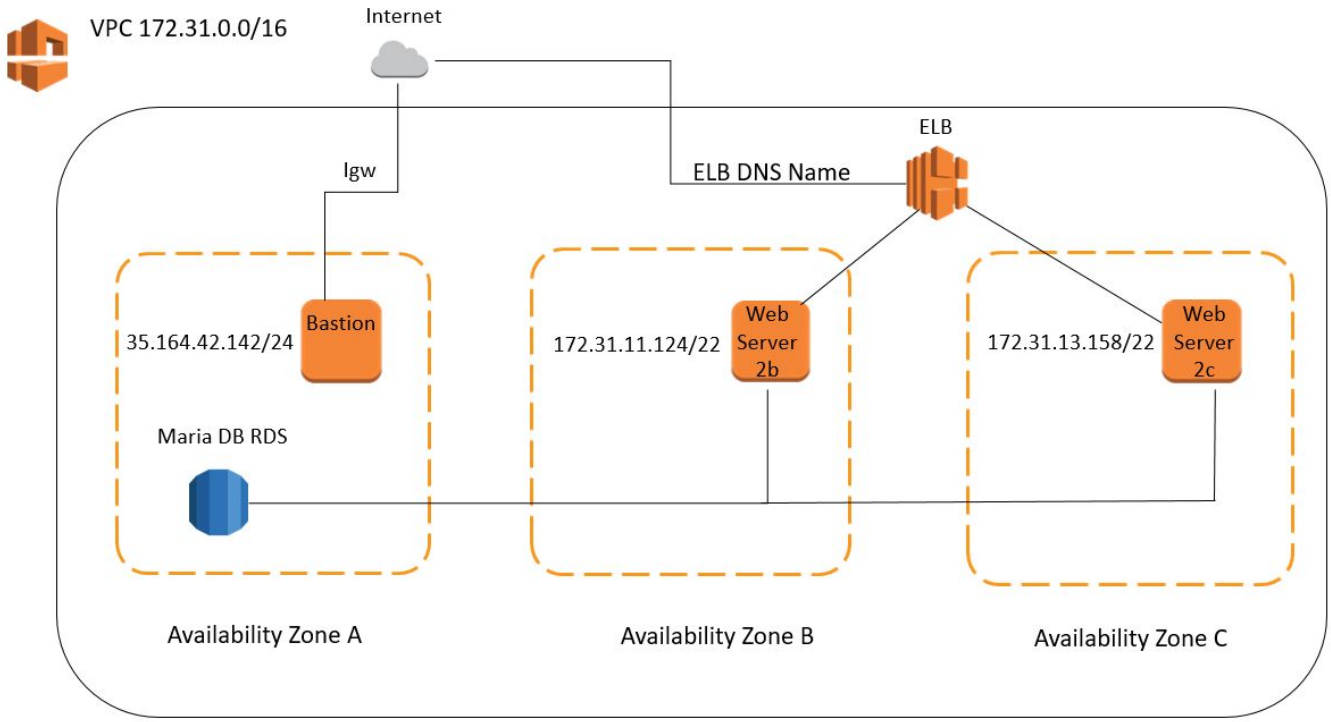
Short Description

Launch two Linux web servers via terraform. Both instances connect to an elastic load balancer which displays a database on a web browser through an ELB DNS name address.

Required Software/Materials

1. *Terraform*
2. *Terraform infra.tf file*
3. *GIT*
4. *Git-Hub account*
5. *Ansible*
6. *SSH capable terminal*
7. *Amazon AWS account*
8. *Amazon EC2 AMI Linux*

Architecture Diagram



Deployment

1. Install GIT on physical machine
    a. To install git type “sudo yum install git”.
    b. Next, clone your git-hub repo to your Bastion instance by typing “git clone https://github.com/UserName/cit-360.git.
2. Install Terraform on your physical machine
    a. Download appropriate terraform file from terraform website.
    b. Unzip terraform file into directory of choice.
    c. Place Terraform file on the path
        i. Navigate to your ~/.profile
        ii. Add “ export PATH=$PATH:/home/your-username/terraform”
    d. Type terraform, the following menu should appear
    e.

```
Usage: terraform [--version] [--help] <command> [args]

The available commands for execution are listed below.
The most common, useful commands are shown first, followed by
less common or more advanced commands. If you're just getting
started with Terraform, stick with the common commands. For the
other commands, please read the help and docs before usage.

Common commands:
    apply              Builds or changes infrastructure
    destroy            Destroy Terraform-managed infrastructure
    fmt                Rewrites config files to canonical format
    get                Download and install modules for the configuration
    graph              Create a visual graph of Terraform resources
    import             Import existing infrastructure into Terraform
    init               Initializes Terraform configuration from a module
    output             Read an output from a state file
    plan               Generate and show an execution plan
    push               Upload this Terraform module to Atlas to run
    refresh            Update local state file against real resources
    remote             Configure remote state storage
    show               Inspect Terraform state or plan
    taint              Manually mark a resource for recreation
    untaint            Manually unmark a resource as tainted
    validate           Validates the Terraform files
    version            Prints the Terraform version

All other commands:
    state              Advanced state management
```

3. Locate the directory where your infra.tf file is located.
    a. Enter “terraform apply”.
    b. Enter your password to build infrastructure.

4. Next ssh into your bastion EC2 instance using your cit360.pem file
    a. $ ssh -i ~/.ssh/cit360.pem ec2-user@ec2-##-###-###-###.us-west-2.compute.amazonaws.com
    b. Your Bastion instance is up and running if you see the following splash screen.
    c.

```
The authenticity of host 'ec2-35-164-42-142.us-west-2.compute.amazonaws.com (35.
164.42.142)' can't be established.
ECDSA key fingerprint is SHA256:Cx9IR1d/JFYtL9WR1ryekEtfVpaDxj0e7S+jGsHnWPM.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'ec2-35-164-42-142.us-west-2.compute.amazonaws.com,35
.164.42.142' (ECDSA) to the list of known hosts.

       __|  __|_  )
       _|  (     /   Amazon Linux AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-ami/2016.09-release-notes/
6 package(s) needed for security, out of 11 available
Run "sudo yum update" to apply all updates.
[ec2-user@ip-172-31-0-137 ~]$
```

5. Install GIT on EC2 Amazon Linux instance
    a. To install git type “sudo yum install git”.
    b. Next, clone your git-hub repo to your Bastion instance by typing “git clone https://github.com/UserName/cit-360.git”
6. Configure your hosts.ini, db.yml and web.yml playbook with the correct ip address and rds information.
    a. In your hosts.ini file be sure to add your correct web server ip addresses.
    b.

```
[web]
172.31.11.124 ansible_ssh_private_key_file=~/.ssh/cit360.pem
172.31.13.158 ansible_ssh_private_key_file=~/.ssh/cit360.pem
```

    c. Add your RDS endpoint to your your db.yml.
    d.

```
    - name: Create rds database
      become: yes
      command: ./make_databases.sh "{{ db_password }}" tf-201612141834
32565670898u4w.cxvytcpxrmgm.us-west-2.rds.amazonaws.com chdir=~/db
      ignore_errors: True
```

    e. Also add your RDS endpoint to your your Web.yml
    f.

```
    service_version: 1.0
    app_env: test
    db_host: tf-20161214183432565670898u4w.cxvytcpxrmgm.us-west-2.rds.
amazonaws.com
    db_database: curriculum
```

7. Install Ansible on EC2 Amazon Linux instance
    a. Install Ansible by typing “sudo pip install ansible”.
    b. Run db.yml by typing “ansible-playbook -i hosts.ini db.yml --ask-vault-pass”.
    c. Run web.yml ansible by typing “ansible-playbook -i hosts.ini web.yml --ask-vault-pass”.

8. EC2 Load Balancer
    a. Navigate to your Amazon EC2 Dash, select “load balancers” and copy your DNS Name.
    b. In a web browser, paste your ELB DNS name.

Issues

Title: *Failed to connect to the host via ssh*

```
Are you sure you want to continue connecting (yes/no)? yes
fatal: [localhost]: UNREACHABLE! => {"changed": false, "msg": "Failed to connect
 to the host via ssh: Warning: Permanently added 'localhost' (ECDSA) to the list
 of known hosts.\r\nno such identity: /home/ec2-user/.ssh/cit360.pem: No such fi
le or directory\r\nPermission denied (publickey).\r\n", "unreachable": true}
```

Description: *The host not able to communicate with the control machine*
Remediation Steps:

- *Ensure that your cit360.pem file is inside of the instance’s ~/.ssh directory*.

Title: *Permissions 0664 for '/home/ec2-user/.ssh/cit360.pem' are too open*

```
fatal: [localhost]: UNREACHABLE! => {"changed": false, "msg": "Failed to connect
 to the host via ssh: @@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@\r\n@         WARNING: UNPROTECTED PRIVATE KEY FILE!          @\r\n@@@@@@@@@@@@@
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@\r\nPermissions 0664 for '/home/e
c2-user/.ssh/cit360.pem' are too open.\r\nIt is required that your private key f
iles are NOT accessible by others.\r\nThis private key will be ignored.\r\nbad p
ermissions: ignore key: /home/ec2-user/.ssh/cit360.pem\r\nPermission denied (pub
lickey).\r\n", "unreachable": true}
```

Description: *Permissions for your cit360.pem files are not secure enough*
Remediation Steps:

- *cd into your ~/.ssh file and chmod your cit360.pem file with 0600 permissons*