**AWS Three Tier Setup procedure**

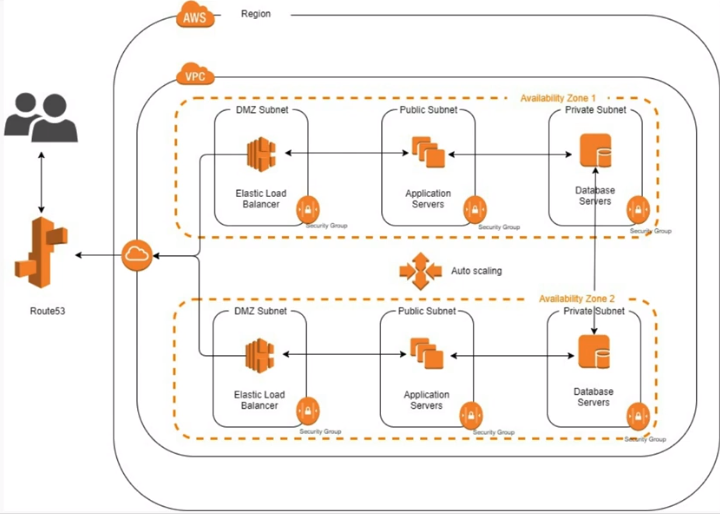
**Overview:**

This procedure will describe the steps needed to set up a three tier scaling AWS environment. It will explain how to set up the environment through the AWS dashboard via the web interface and it will also give the steps needed to set up the same environment through CLI commands. Both processes should produce the same environment and both will utilize AWS CloudFormation.

**Assumptions:**

We will be creating all components throughout this procedure in the us-east-1 AWS region.

**Diagram of the architecture we are trying to achieve:**



**Procedure:**

1. Figure out the range of IP addresses that will be needed for the entire VPC - including all subnets.
   1. We are going to use 192.168.0.0/19. This will give us 8188 usable addresses (8190 total addresses).

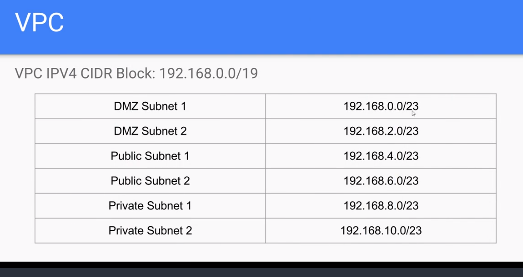
We will need to split this up for six different subnets - two subzones that each have three subnets

After calculating we split it up into 510 IP addresses in each of the six subzones using the mask of /23 for each.

I wanted to use 256 but the calculation forced us to round up to 510.

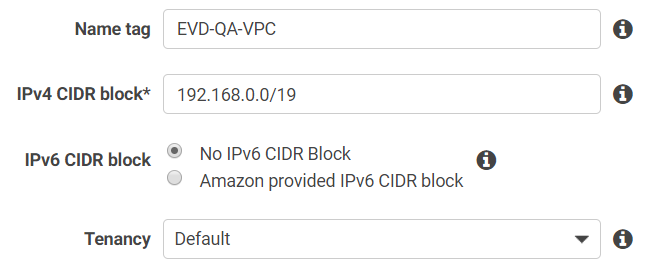
A good site to help calculate this is <http://www.vlsm-calc.net>

**Resulting VPC subnet mapping:**



**Initial VPC Creation**

1. Initial configuration of VPC via the AWS dashboard:
   1. Log into AWS, go to your console and navigate to the VPC dashboard.
   2. Click on “Create VPC”.
   3. Name the VPC – for this procedure we will be using “EVD-QA-VPC”.
   4. Enter the appropriate CIDR block that will encompass all addresses needed for all subnets utilized inside of this VPC.
   5. Check no IPv6 CIDR block, keep the tenancy at default and click Create.



* 1. If successful you should get a message stating that the VPC was created. Click close and you should now see you new VPC displayed on the VPC dashboard.



\*\*You should take note of the ARN identifier of this VPC as you will use it as a reference throughout the procedure.

1. Initial configuration of VPC via the CLI and CloudFormation scripts:
   1. Create a directory that will be specifically used for the entirety of this project and cd into it.
   2. Create a YAML file that will be used as the CloudFormation template.
      1. For this procedure we will name it “vpc.yml”.
   3. Add the following text to the vpc.yml file and save it:

**AWSTemplateFormatVersion**: 2010-09-09  
**Description**: 'A CloudFormation template to form a VPC for our tutorial'**Resources**:  
 **VPC**:  
 **Type**: AWS::EC2::VPC  
 **Properties**:  
 **CidrBlock**: 192.168.0.0/19  
 **EnableDnsSupport**: false  
 **EnableDnsHostnames**: false  
 **InstanceTenancy**: default  
 **Tags**:  
 - **Key**: Name  
 **Value**: EVD-QA-CLI-VPC  
 - **Key**: Owner  
 **Value**: Ernie Van Duyne  
 - **Key**: Environment  
 **Value**: QA

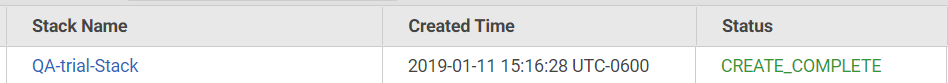
* 1. Run the following command in the same directory that the “vpc.yml” file is in:

*aws cloudformation create-stack --stack-name QA-trial-Stack --template-body file://vpc.yml --region us-east-1*

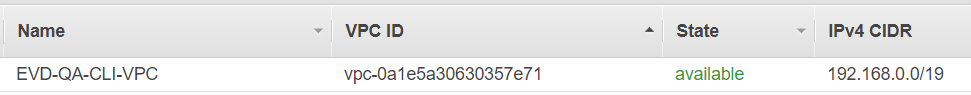
* 1. Upon successful completion of the command you should receive outout similar to the following:

*"StackId": "arn:aws:cloudformation:us-east-1:499000881936:stack/QA-trial-Stack/28e86110-15e6-11e9-8a86-0a9fca2e6786"*

* 1. In the AWS CloudFormation dashboard you should now see an entry for the stack that was just created.

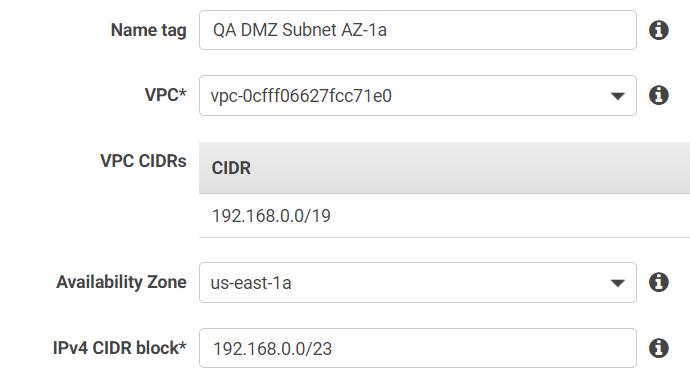


* 1. In the AWS VPC dashboard you should see an entry for the VPC that was just created through the CloudFormation script.

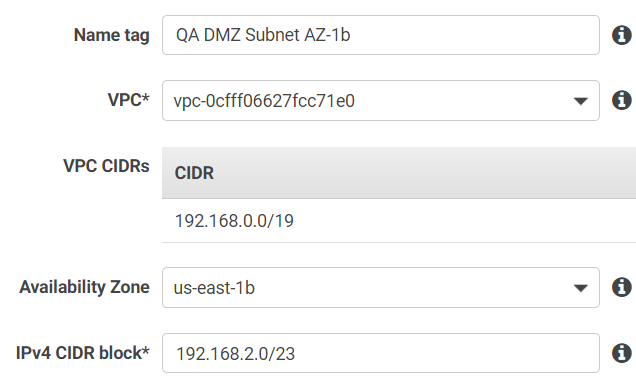


**Subnet Creation**

1. Create subnets through the AWS dashboard:
   1. Click on “Subnets” in the VPC Dashboard menu then click on “Create New Subnet”.
   2. In the name tag field create the name for the DMZ subnet for availability zone 1a.
      1. For this procedure we will name it “QA DMZ Subnet AZ-1a”.
   3. Under “VPC” select the same VPC that was just created in the AWS dashboard steps. Make sure that the ARN of this VPC matches the one created in the AWS dashboard steps.
   4. Select the Availability zone “us-east-1a”.
   5. Enter the IPv4 CIDR block 192.168.0.0/23 and then click create.



* 1. Follow the same steps outlined from b through e but use “QA DMZ Subnet AZ-1b” as the name and “192.168.2.0/23 for the CIDR block.



\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Network setup tutorial notes**

DMZ - demilitarized zone - public facing.

In computer security, a DMZ or demilitarized zone (sometimes referred to as a perimeter network or screened subnet) is a physical or logical subnetwork

that contains and exposes an organization's external-facing services to an untrusted network, usually a larger network such as the Internet.

A website that helps you calculate IPV4 subnets - http://www.vlsm-calc.net/

CloudFormation tutorial - https://blog.boltops.com/2018/02/14/aws-cloudformation-declarative-infrastructure-code-tutorial

VPC CloudFormation templates - https://sookocheff.com/post/aws/how-to-create-a-vpc-using-cloudformation/