

Only you can see this message



This story's distribution setting is on. You're in the Partner Program, so this story is eligible to earn money. [Learn more](#)

# Setting up a simple cloud in AWS



Craig Godden-Payne

Oct 26, 2018 · 4 min read ★



## Setting up a simple cloud

I do a lot of terraform configuration at work, but never had a chance to look at how to provision stuff within the AWS management console, so I've working to understand the basics of AWS architecture, to improve my knowledge and skills.

## What is a Virtual Private Cloud?

A VPC is a logically isolate network within the AWS global network. It is the primary subnet, that can be split into multiple smaller subnets, and allows you to control all your network infrastructure.

It allows for enhanced security against everything that sits within it, and is typically secured using network control lists (NCLs). You can also use a VPC to internetwork with other organisations or accounts, using VPC peering, to join VPCs together. You can also assign public IP addresses from within the VPC (in AWS these are termed Elastic IP addresses), you can also setup hybrid clouds, using site-to-site VPN. VPC is free within AWS, as it is everything else inside, which you pay for.

## VPC Elements

In the AWS console, there are various things you can setup, such as:

- Subnets
- Route Tables
- Internet Gateways
- Elastic IPs
- Endpoints
- NAT Gateways
- Peering Connections
- Network ACLs
- Security Groups
- VPNs



## VPC Characteristics

When setting up a subnet within a VPC, there are a few quirks that are good to be aware of.

- AWS reserves 5 IP addresses per subnet, which is typically the first 4 and the last 1. These are used for management purposes. Also a subnet can either be made Public,

## Private or VPN only

- Subnets cannot span availability zones (as they sit within a single AZ).
- VPCs span across a single region, but can span across multiple availability zones.
- When specifying a CIDR block, you can only specify between 16 and 28 (no more or less).
- You can specify the IP Prefix within the VPC.

## VPC Security

There are pros and cons for applying different security measures in AWS against a VPC. The two types of security you can apply are Security Groups, and Access Control lists.

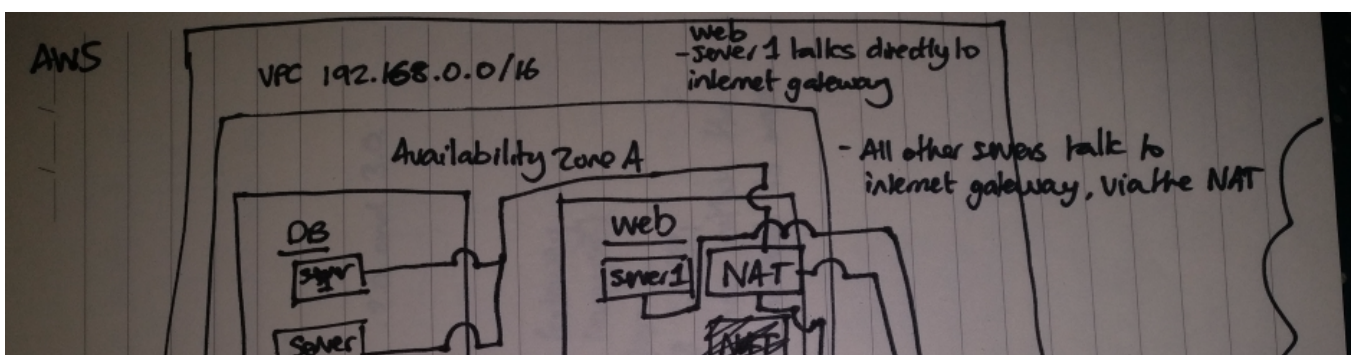
Security Groups feature:

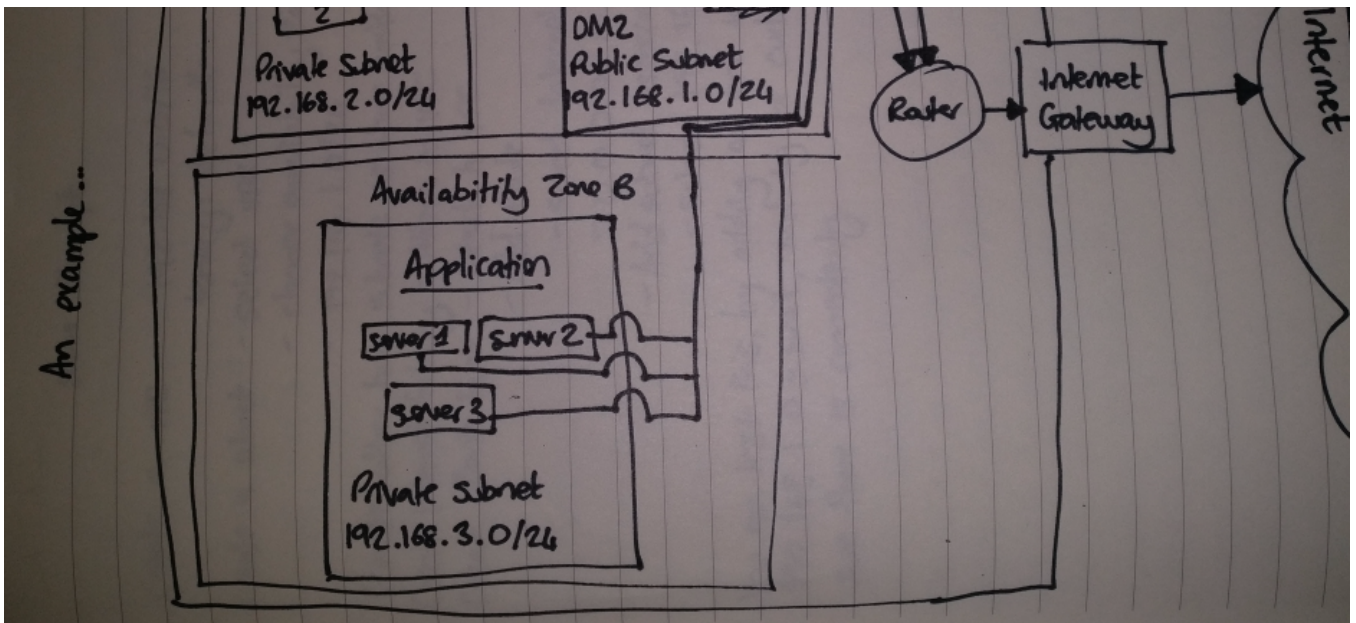
- Resource level traffic firewall, meaning you can block by resource such as Instance, ELB etc.
- Ingress and Egress rules combined
- Is stateful (return traffic is allowed)

Access Control Lists feature:

- Source and protocol filtering
- Subnet level traffic firewall
- Ingress and Egress rules are separate
- Is stateless (traffic is strictly filtered and return traffic has to be specified.)

## An Example of setting up a simple VPC





In this example I am designing a simple cloud structure.

It's going to have a DMZ subnet where the Web servers are located, and a subnet for dB servers, and one for application servers. The dB and application servers will talk to the Internet via a Nat Gateway.

First you need to create the VPC, and set the IP prefix to something like `192.168.0.0/16` and set the tenancy to default.

Name tag  ⓘ

IPv4 CIDR block\*  ⓘ

IPv6 CIDR block\* ☒ No IPv6 CIDR Block ⓘ  
☐ Amazon provided IPv6 CIDR block

Tenancy  ⓘ

You then want to create 3 subnets, and set the CIDR block to be `192.168.1.0/24`, `192.168.2.0/24` and `192.168.3.0/24` respectively.

Name tag  ⓘ

VPC  ⓘ

VPC CIDRs

CIDR	Status	Status Reason
192.168.0.0/16	<span style="color: green;">●</span> associated	

Availability Zone us-east-2a ⓘ

IPv4 CIDR block 192.168.1.0/24 ⓘ

We are going to treat 1.0 as our DMZ containing our web servers and NATs, 2.0 as our DB server, and 3.0 as our Application servers.

Next add an Internet Gateway and attach to the VPC

☒ CraigsIGW CraigsIGW igw-e917e581 detached

- Delete internet gateway
- Attach to VPC
- Detach from VPC
- Add/Edit Tags

Then add a new Route Table and attach to the VPC

Next add a route to the route table, selecting the internet gateway, and assign it to everyone 0.0.0.0/0.

#### rtb-a44e73cc | CraigsRouteTable

Summary Routes Subnet Associations Route Propagation Tags

Cancel Save

View: All rules





Destination	Target	Status	Propagated	Remove
192.168.0.0/16	local	Active	No	
<input type="text" value="0.0.0.0/0"/>	<input type="text" value="igw-e917e581"/>	No	No	<input checked="" type="button" value="x"/>

Add another route

Then add a subnet association, and select our DMZ subnet, 192.168.1.0/24

If you bring up an EC2 instance within the 192.168.1.0 subnet, and run a curl command, you should find that the box has internet traffic.

Launch Instance  Actions

	Name ▾	Instance ID ▾	Instance Type ▾	Availability Zone ▾	Instance State ▾	Status Checks ▾
	CraigsWeb	i-02fc9f257e1d6c887	t2.micro	us-east-2a	 pending	 Initializing

Written on May 7, 2018.

Originally published on <https://craig.goddenpayne.co.uk/aws-simple-cloud-setup/>

[AWS](#) [Vpc](#) [Cloud](#)

[About](#) [Help](#) [Legal](#)

Get the Medium app

