CommIT VPC Setup Information

DRAFT (in progress document)

Summary

This page describes the steps to setup from scratch the VPC for the CommIT environment. A lot of these steps do not need to be repeated again once it is setup. However, it is provided as a record of what is needed in order to setup the VPC for CommIT.

Steps

1.) Create a new VPC in the AWS Acount with a subnet of '172.16.0.0/16':

VPC ID: vpc-f67abf93 (172.16.0.0/16)

2.) After the VPC is created, create a new Internet Gateway and attach it to the new VPC:

Gateway ID: igw-a4c334c1

Name: CommIT-VPC-Internet-Default-Gateway

3.) Create a security group for a NAT instance that will be launched in the next ste (if you did not launch a NAT instance during the VPC creation). Instructions for how to set this group up can be found at: http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_NAT_Instance.html#NATSG . Be sure to include your IP address initially to allow SSH access until a Bastion Server is configured. Using the default rules found on the instruction page will suffice for servers using this NAT instance to access the Internet.

4.) If you did not have the VPC creation launch a NAT instance for the Private subnet, please do so now. Instructions for completing this step can be found at: http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_NAT_Instance.html

Note: As of 08-28-14 the AMI ID is 'ami-f032acc0'. It was launched as a t1.micro instance. Assign it to a Public Subnet that has been created (in this case the Development Zone A subnet). Enable termination protection for the instance. Do not assign public IP.

TAG: Name=CommIT VPC Default Nat Instance

KeyPair: commit-vpc-keypair

5.) After the NAT instance is launched, allocate an Elastic IP address to use for the new NAT instance and assign it to that instance. Be sure to allocate the Elastic IP address for the VPC and **not** EC2.

6.) Edit the 'Main' route table for the new VPC and add a default gateway for the route table to use the NAT Instance created in step #4. This will be the default route table used by instances in the private subnets.

Tag: Name=CommIT-VPC-Main-Route-Table

Route Table ID: *rtb-4422e321*

Destination	Target	Status	Propagated
172.16.0.0/16	local	Active	No
0.0.0.0/0	i-11aefc1c	Active	No

** Note: when adding this route, you will need to use a Target=<instance id of NAT instance>. When you view the table, it will also add in the Elastic Network interface of the instance.

7.) Create a **new** route table for use by the Public subnets of the VPC. This will allow the instances in the Private VPC to use the NAT instance interface for initiating traffic to the Internet:

Name: CommIT-VPC-Public-Subnet-Route-Table

VPC: 172.16.0.0/16

Route Table ID: rtb-71a16214

Destination	Target	Status	Propagated
172.16.0.0/16	local	Active	No

0.0.0.0/0	igw-a4c334c1	Active	No

8.) Next, assign the proper subnets to the one of the two routing tables created above. Public subnets should use the 'Public' route table, and the Private subnets should use the 'Main' route table. Note that this simply defines the routing for a subnet and not the act of allowing/blocking traffic between the subnets.

9.) Prior to launching instances in the VPC, the proper Security groups should be defined, created, and associated with the VPC for use inside of the VPC. The table below is a list of security groups that have been created (the actual rules in the group are described in another area):

Security Group Name	Function
commit-vpc-dev-idp-public-elb	Allow traffic to the IDP Dev Public ELB
commit-vpc-dev-cpr-public-elb	Allow traffic to the CPR Dev Public ELB
commit-vpc-bastion-server	Allow traffic to the Bastion Server
commit-vpc-dev-idp-servers	Allow traffic to/from the private Dev IDP instances
commit-vpc-dev-cpr-servers	Allow traffic to/from the private Dev CPR instances
commit-vpc-dev-ldap-servers	Allow traffic to/from the private Dev LDAP instances
commit-vpc-dev-salt-master	Allow traffic to/from the Salt Master for the Dev environment
commit-vpc-prod-salt-master	Allow traffic to/from the Salt Master for the Prod environment
commit-vpc-dev-log-server	Allow traffic to/from the central Dev Rsyslog server
commit-vpc-prod-log-server	Allow traffic to/from the central Prod Rsyslog server

10.) Launch instances into the VPC to setup the proper environment (e.g. Dev, QA, Prod, etc.). This can be done maually, or through a CloudFormation template. Ensure that only the ELB and Bastion server reside in the Public Subnet. All other instances should reside in a private subnet. Instances should be launched in the 'CommIT VPC'. Details about each enviornment requirements are below:

General

AWS Resource	Tag: Name	Security Group	Subnet	Zone	Notes
t2.micro	CommIT-VPC-Bastion-Server	commit-vpc-bastion-server	172.16.0.0/24	us-west-2a	This server is accessible via SSH key from anywhere and can connect to the private instances. Once launched and Elastic IP should be assigned to it for use by the server.

Dev (only uses 1 AZ)

AWS Resource	Tag: Name	Security Group	Subnet	Zone	Notes
m3.medium	CommIT-VPC-Dev-IDP-1	commit-vpc-dev-idp-servers	172.16.100.0/24	us-west-2a	ami-d13845e1
m3.medium	CommIT-VPC-Dev-IDP-2	commit-vpc-dev-idp-servers	172.16.100.0/24	us-west-2a	ami-d13845e1
m3.medium	CommIT-VPC-Dev-CPR-1	commit-vpc-dev-cpr-servers	172.16.100.0/24	us-west-2a	ami-d13845e1
m3.medium	CommIT-VPC-Dev-CPR-2	commit-vpc-dev-cpr-servers	172.16.100.0/24	us-west-2a	ami-d13845e1
ELB	CommIT-VPC-Dev-IDP-ELB	commit-vpc-dev-idp-public-elb	172.16.0.0/24	us-west-2a	Listener for 80 and 443; Health thresholds are 2 each; Disable connection draining; Enable Cross-Zone Load balancing; Add Dev IDP instances
ELB	CommIT-VPC-Prod-IDP-ELB	commit-vpc-dev-cpr-public-elb	172.16.0.0/24	us-west-2a	Listener for 80 and 443; Health thresholds are 2 each; Disable connection draining; Enable Cross-Zone Load balancin; Add Dev CPR instances
m3.medium	CommIT-VPC-Dev-LDAP-1	commit-vpc-dev-ldap-servers	172.16.100.0/24	us-west-2a	ami-d13845e1
m3.medium	CommIT-VPC-Dev-LDAP-2	commit-vpc-dev-ldap-servers	172.16.100.0/24	us-west-2a	ami-d13845e1
m3.medium	CommIT-VPC-Dev-Salt-Master	commit-vpc-dev-salt-master	172.16.100.0/24	us-west-2a	ami-d13845e1

m3.medium	CommIT-VPC-Dev-Rsyslog	commit-vpc-dev-log-server	172.16.100.0/24	us-west-2a	ami-d13845e1

Production (to be filled in when launched)

AWS Resource	Tag: Name	Security Group	Subnet	Zone	Notes

11.) Configure the Bastion server to allow Agent Forwarding so that administrators do not need to store their private key on the server itself to communicate with the other systems.

- Edit /etc/ssh/sshd-config and uncomment the following line:
  AllowAgentForwarding yes
- Restart the SSH Daemon
- Ensure that your local machine is running the SSH daemon and that it has had the 'ForwardAgent yes' line uncommented for all hosts (or you can specify which hosts to use agent forwarding as well).

12.) Initially, no accounts will exist on the instances other than 'ec2-user'. To access the private servers you will need to add the SSH private key of the KeyPair that was launched with the instances (eg. for Dev this would be 'commit-vpc-keypair'). To add the key to your **own** local SSH so that the agent will recognize it for use in forwarding use this command on your local box:

ssh-add <private key name>

13.) Once you add the key, you should now SSH to the bastion server as the 'ec2-user' (no need to use a specific key file as you took care of that in the previous step).

14.) Once you are logged into the bastion server, you can SSH to the private instances as 'ec2-user' using their Private IP address. Later on, after the Salt Master has deployed accounts users can use their regular account name and key as they will then exist on the servers.