

	Virtual Private Cloud (VPC) SOP (VPC, Subnets, Route Tables, Internet Gateway, NAT Gateway, Security Group etc)
--	--

## Revision History

Date	Version	Changed Sections	Author	Approver
11/19/2017	1.0	Created	Samal Dimdung	

## Document Controller Number

Document Reference	Project

# 1 Purpose

The purpose of the document is to provide guidance on how to use the CloudFormation template to create AWS Cloud Infrastructure with predefined templates such as building whole Network Infrastructure and use the same code/templates repeatedly for multiple environment with no time.

## 2 Tools Required

Tool Name	Tool Location	Tool Description
AWS Console Access	AWs Account	AWS Console can be used to run CloudFormation Templates to create Cloud infrastructure
AWS CLI/AWS SDK		AWS CLI or AWS SDK can be used if you don't want to use AWs Console to run the CloudFormation Templates

## 3 Associated Documents

The follow documents are associated with the Standard Operating Procedure and are required in order to complete it. For Google Docs/Wiki please type the document name and apply hyper link to google doc.

Document Name	Date Entered
Bootstrapping New AWS Account	XX-XX-XXXX
AWS Infrastructure Provisioning	XX-XX-XXXX
IAM and Roles Provisioning	XX-XX-XXXX
CloudFormation Template for VPC	XX-XX-XXXX
CloudFormation Template for Wordpress Stack	XX-XX-XXXX
Nested CloudFormation for deploying full stack with multiple AWS services	XX-XX-XXXX

## 4 Assumptions

The individuals reading this document are assumed to already have worked as AWS Architect or should have a skill for at least AWS Solution Architect - Associate level certifications.

**This includes:**

- Should have Knowledge about the AWS Environment
- Should have Knowledge about the Virtualization
- Should have knowledge about the CIDR and subnetting
- Should have knowledge about the Routing Concepts
- Should have knowledge about the Firewall and NACL
- Should have knowledge about the NAT Gateway or NAT servers

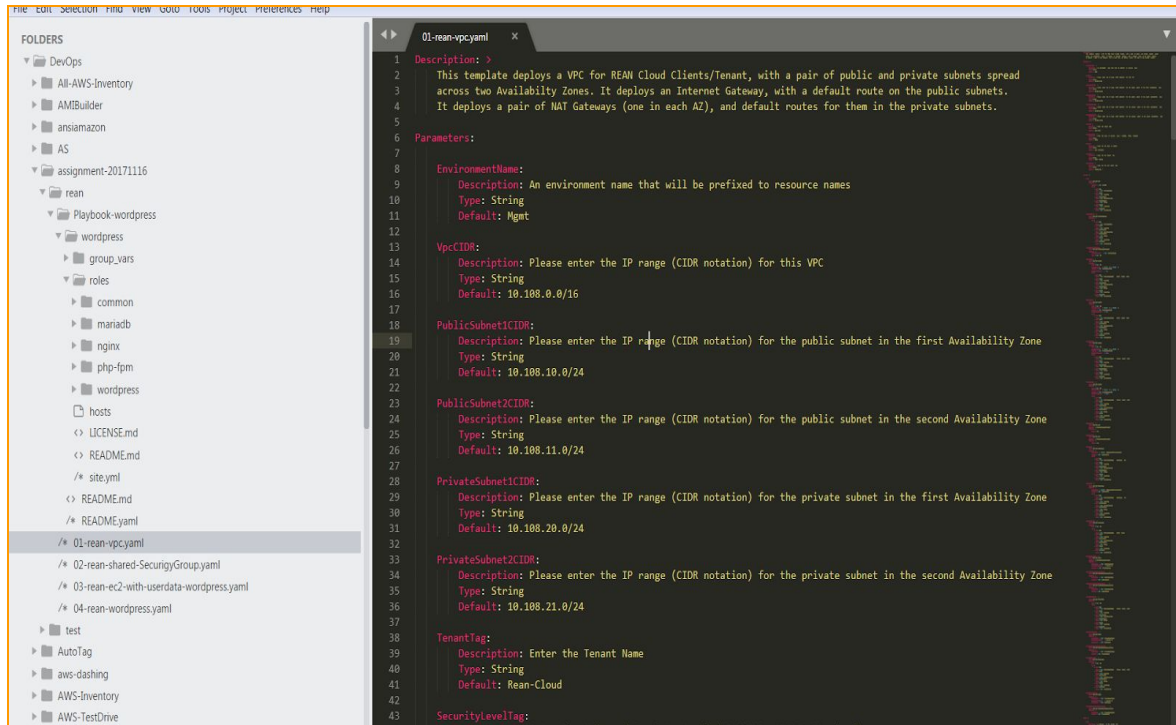
## 5 List of Resources will be created

Numbers	Resource Name	Description
1	VPC	10.108.0.0/16
2	Public Subnets	10.108.10.0/24   10.108.11.0/24
2	Private Subnets	10.108.20.0/24   10.108.21.0/24 with NAT Gateway
2	NAT Gateway	Arbitrary EIP
1	Public Route Table	To Route Traffic to Public Access
2	Private Route Table	To Route Traffic within VPC
1	IGW	To route Traffic to Internet

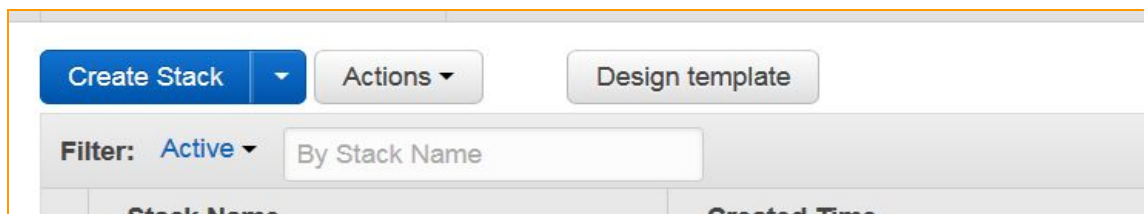
# 6 Produrre

## 6.1 Creating New VPC

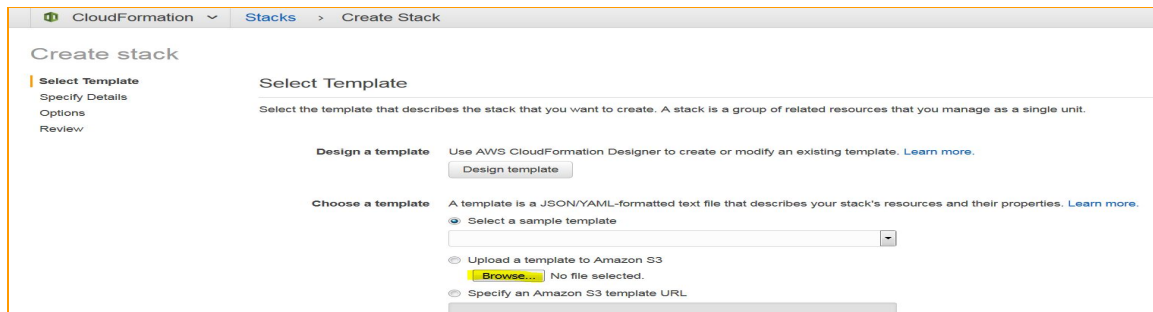
1. Download the CloudFormation Templates on your Local Workstation or CM servers from Github or S3. You can make Nested templates and run the all the CloudFormation Templates but here I'm doing 3 different CloudFormation Templates separately.



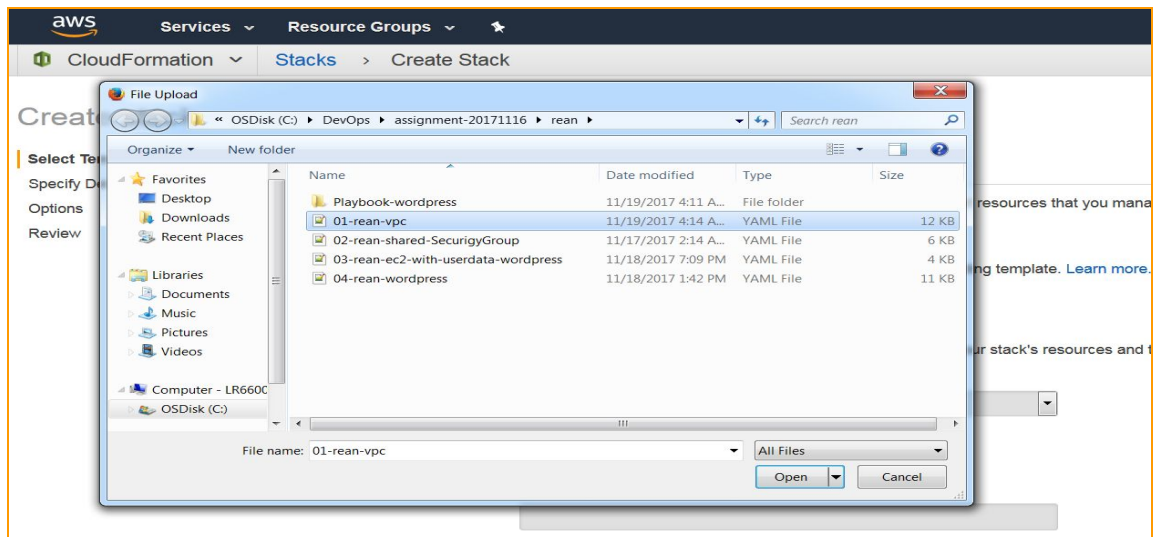
2. Once you download the CloudFormation Template from the S3 or Github, you have multiple choice to run the CloudFormation Templates. By Login into AWS Console using AWS Console user/credentials or you can use AWS CLI or AWS-SDK if you have access and secret key for your users.
3. I'm using AWS Console, because you can see all the parameter which I'm going to pass while I create the Virtual Private Cloud in AWS using CloudFormation Templates to automate the provisioning.
4. All Services > Management Tools > CloudFormation
5. Create Stack



## 6. Select Template: Browse



## 7. Select the CloudFormation Templates files > Open > Next



## 8. Specify Details : Verify the Parameters, if you want to change enter the new values and Next.

**Specify Details**

Specify a stack name and parameter values. You can use or change the default parameter values, which are defined in the AWS CloudFormation template. [Learn more.](#)

**Stack name**

**Parameters**

<b>CostCenterTag</b>	<input type="text" value="DevOps-108"/>	Value for the Cost Center Tags
<b>CreatorTag</b>	<input type="text" value="Samal Dindung"/>	Value for the Creator Tag
<b>EnvironmentName</b>	<input type="text" value="Mgmt"/>	An environment name that will be prefixed to resource names
<b>POCTag</b>	<input type="text" value="Nick Martinelli"/>	Value for the Point of Contact
<b>PrivateSubnet1CIDR</b>	<input type="text" value="10.108.20.0/24"/>	Please enter the IP range (CIDR notation) for the private subnet in the first Availability Zone
<b>PrivateSubnet2CIDR</b>	<input type="text" value="10.108.21.0/24"/>	Please enter the IP range (CIDR notation) for the private subnet in the second Availability Zone
<b>PublicSubnet1CIDR</b>	<input type="text" value="10.108.10.0/24"/>	Please enter the IP range (CIDR notation) for the public subnet in the first Availability Zone
<b>PublicSubnet2CIDR</b>	<input type="text" value="10.108.11.0/24"/>	Please enter the IP range (CIDR notation) for the public subnet in the second Availability Zone
<b>SecurityLevelTag</b>	<input type="text" value="HIPAA"/>	Enter the Value of Security Level ( FedRAMP, HIPAA, Standard)
<b>TenantTag</b>	<input type="text" value="Rean-Cloud"/>	Enter the Tenant Name
<b>VpcCIDR</b>	<input type="text" value="10.108.0.0/16"/>	Please enter the IP range (CIDR notation) for this VPC

## 9. Option - Leave Blank and Next

The screenshot shows the 'Create Stack' page in the AWS CloudFormation console, specifically the 'Options' tab. The left sidebar has links for 'Select Template', 'Specify Details', 'Options' (selected), and 'Review'. The main content area is titled 'Options' and includes sections for 'Tags', 'Permissions', and 'Advanced'. The 'Tags' section has a table with columns 'Key' and 'Value'. The 'Permissions' section has a dropdown for 'IAM Role' and a text input for 'Enter role arn'. The 'Advanced' section is currently collapsed. At the bottom right, there are 'Cancel', 'Previous', and 'Next' buttons.

CloudFormation > Stacks > Create Stack

### Create stack

Select Template  
Specify Details  
**Options**  
Review

#### Options

##### Tags

You can specify tags (key-value pairs) for resources in your stack. You can add up to 50 unique key-value pairs for each stack. [Learn more.](#)

Key (127 characters maximum)	Value (255 characters maximum)
1	

+

##### Permissions

You can choose an IAM role that CloudFormation uses to create, modify, or delete resources in the stack. If you don't choose a role, CloudFormation uses the permissions defined in your account. [Learn more.](#)

IAM Role: Choose a role (optional)

Enter role arn:

Advanced

You can set additional options for your stack, like notification options and a stack policy. [Learn more.](#)

Cancel Previous Next

## 10. Review - Just Click on Create.

The screenshot shows the 'Create Stack' page in the AWS CloudFormation console, specifically the 'Review' tab. The left sidebar has links for 'Select Template', 'Specify Details', 'Options', and 'Review' (selected). The main content area is titled 'Review' and includes sections for 'Template', 'Details', 'Options', and 'Advanced'. The 'Template' section shows the 'Template URL' and 'Description'. The 'Details' section shows the 'Stack name' and various tags. The 'Options' section shows 'Tags' and 'Advanced' options. At the bottom, there are 'Notification', 'Termination Protection', 'Timeout', and 'Rollback on failure' options. At the bottom right, there are 'Cancel', 'Previous', and 'Next' buttons.

### Create stack

Select Template  
Specify Details  
Options  
**Review**

#### Review

##### Template

Template URL: <https://s3-external-1.amazonaws.com/cf-templates-1tvmf058jwz-us-east-1/2017324Y93-01-rean-vpc.yaml>  
Description: This template deploys a VPC for REAN Cloud Clients/Tenant, with a pair of public and private subnets spread across two Availability Zones. It deploys an Internet Gateway, with a default route on the public subnets. It deploys a pair of NAT Gateways (one in each AZ), and default routes for them in the private subnets.  
Estimate cost: Cost

##### Details

Stack name: cf-rean-vpc-samal

CostCenterTag: DevOps-108  
CreatorTag: Samal Dindung  
EnvironmentName: Mgmt  
POCTag: Nick Martirelli  
PrivateSubnet1CIDR: 10.108.20.0/24  
PrivateSubnet2CIDR: 10.108.21.0/24  
PublicSubnet1CIDR: 10.108.10.0/24  
PublicSubnet2CIDR: 10.108.11.0/24  
SecurityLevelTag: HIPAA  
TenantTag: Rean-Cloud  
VpcCIDR: 10.108.0.0/16

##### Options

##### Tags

No tags provided

##### Advanced

Notification: Disabled  
Termination Protection: none  
Timeout: none  
Rollback on failure: Yes

Cancel Previous Next

## 11. VPC creation in progress

The screenshot shows the 'Stacks' page in the AWS CloudFormation console. The top bar shows 'AWS Services', 'Resource Groups', and 'Candidate-X0wd9PHs @ rea...'. The main content area shows a list of stacks. The 'cf-rean-vpc-samal' stack is selected and its details are shown. The stack is in the 'CREATE\_IN\_PROGRESS' state. The 'Resources' tab is selected, showing a list of resources and their status.

CloudFormation > Stacks

Create Stack Actions Design template

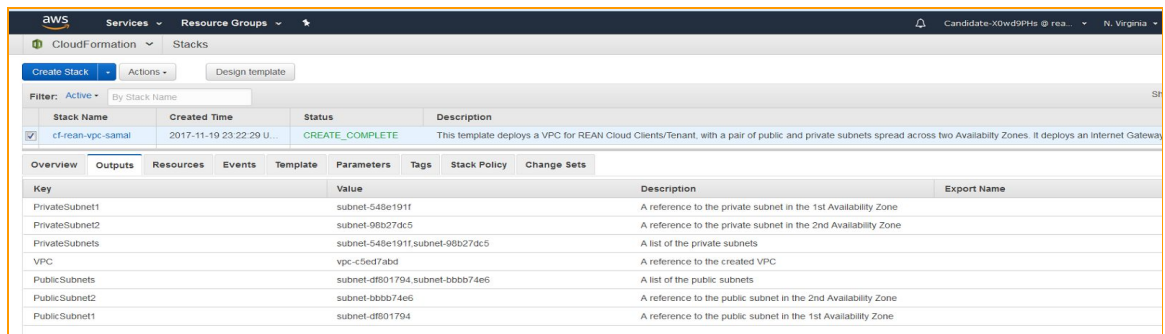
Filter: Active By Stack Name Showing 26 stacks

Stack Name	Created Time	Status	Description
cf-rean-vpc-samal	2017-11-19 23:22:29 U...	CREATE_IN_PROGRE...	This template deploys a VPC for REAN Cloud Clients/Tenant, with a pair of public and private subnets spread across two Availability Zone...

Overview Outputs Resources Events Template Parameters Tags Stack Policy Change Sets

Logical ID	Physical ID	Type	Status	Status Reason
DefaultPublicRoute	cf-re-Defau-1ACE2KF9DPPRE	AWS::EC2::Route	CREATE_COMPLETE	
InternetGateway	igw-d60d9ea7	AWS::EC2::InternetGateway	CREATE_COMPLETE	
InternetGatewayAttachment	cf-re-Inter-53Q46OT7MN0S	AWS::EC2::VPCGatewayAttachment	CREATE_COMPLETE	
NatGateway1	nat-0d0b01e6c7adb0775	AWS::EC2::NatGateway	CREATE_IN_PROGRESS	Resource creation initiated

12. Once it complet, you will see below details

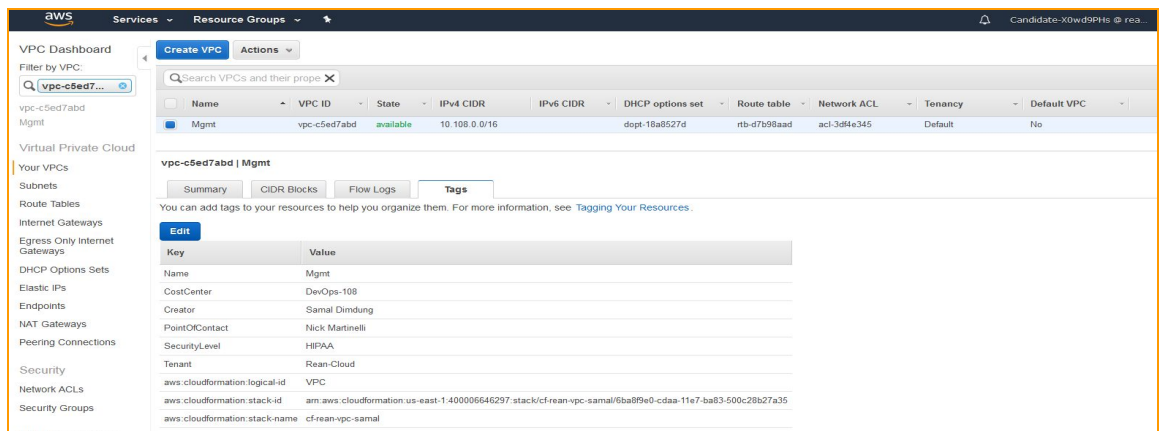


The screenshot shows the AWS CloudFormation console. The top navigation bar includes 'aws', 'Services', 'Resource Groups', and a user profile. The main header shows 'CloudFormation' and 'Stacks'. Below this, there are buttons for 'Create Stack', 'Actions', and 'Design template'. A filter bar shows 'Active' and 'By Stack Name'. The stack list table has columns for 'Stack Name', 'Created Time', 'Status', and 'Description'. One stack is listed: 'cf-rean-vpc-samal' with a status of 'CREATE\_COMPLETE' and a description: 'This template deploys a VPC for REAN Cloud Clients/Tenant, with a pair of public and private subnets spread across two Availability Zones. It deploys an Internet Gateway'. Below the stack list, there are tabs for 'Overview', 'Outputs', 'Resources', 'Events', 'Template', 'Parameters', 'Tags', 'Stack Policy', and 'Change Sets'. The 'Outputs' tab is selected, showing a table with columns 'Key', 'Value', 'Description', and 'Export Name'. The outputs listed are: PrivateSubnet1 (subnet-545e191f), PrivateSubnet2 (subnet-08b27dc5), PrivateSubnets (subnet-545e191f,subnet-08b27dc5), VPC (vpc-c5ed7abd), PublicSubnets (subnet-df801794,subnet-bbb74e6), PublicSubnet2 (subnet-bbb74e6), and PublicSubnet1 (subnet-df801794).

Stack Name	Created Time	Status	Description
cf-rean-vpc-samal	2017-11-19 23 22:29 U...	CREATE_COMPLETE	This template deploys a VPC for REAN Cloud Clients/Tenant, with a pair of public and private subnets spread across two Availability Zones. It deploys an Internet Gateway

Key	Value	Description	Export Name
PrivateSubnet1	subnet-545e191f	A reference to the private subnet in the 1st Availability Zone	
PrivateSubnet2	subnet-08b27dc5	A reference to the private subnet in the 2nd Availability Zone	
PrivateSubnets	subnet-545e191f,subnet-08b27dc5	A list of the private subnets	
VPC	vpc-c5ed7abd	A reference to the created VPC	
PublicSubnets	subnet-df801794,subnet-bbb74e6	A list of the public subnets	
PublicSubnet2	subnet-bbb74e6	A reference to the public subnet in the 2nd Availability Zone	
PublicSubnet1	subnet-df801794	A reference to the public subnet in the 1st Availability Zone	

13. VPC named as Mgmt

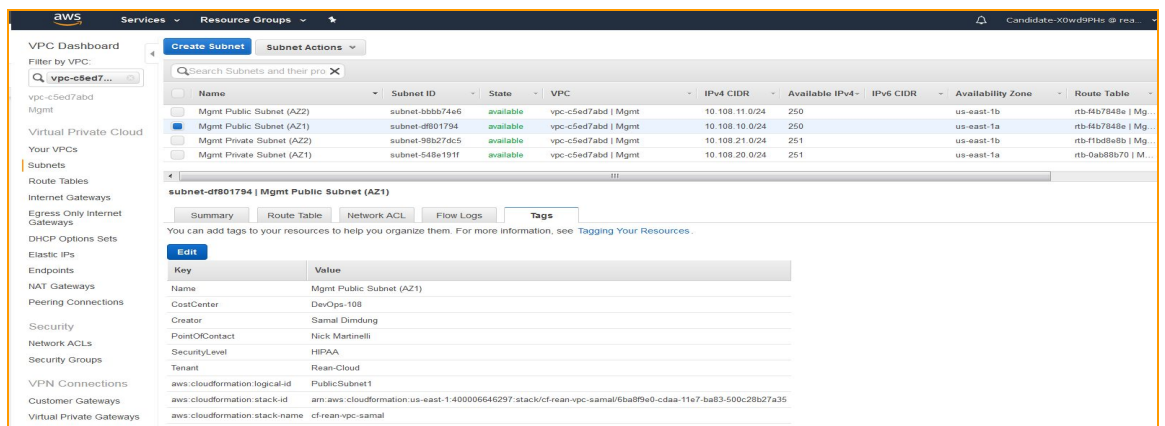


The screenshot shows the AWS VPC Dashboard. The top navigation bar includes 'aws', 'Services', 'Resource Groups', and a user profile. The main header shows 'VPC Dashboard'. Below this, there are buttons for 'Create VPC' and 'Actions'. A search bar is present. A table lists VPCs with columns: 'Name', 'VPC ID', 'State', 'IPv4 CIDR', 'IPv6 CIDR', 'DHCP options set', 'Route table', 'Network ACL', 'Tenancy', and 'Default VPC'. One VPC is listed: 'Mgmt' with VPC ID 'vpc-c5ed7abd', state 'available', and IPv4 CIDR '10.108.0.0/16'. Below the table, there are tabs for 'Summary', 'CIDR Blocks', 'Flow Logs', and 'Tags'. The 'Tags' tab is selected, showing a table with columns 'Key' and 'Value'. The tags listed are: Name (Mgmt), CostCenter (DevOps-108), Creator (Samal Dimdung), PointOfContact (Nick Martinelli), SecurityLevel (HIPAA), Tenant (Rean-Cloud), aws:cloudformation:logical-id (VPC), aws:cloudformation:stack-id (arn:aws:cloudformation:us-east-1:400006646297:stack/cf-rean-vpc-samal/6ba89e0-cdaa-11e7-ba83-500c28b27a35), and aws:cloudformation:stack-name (cf-rean-vpc-samal).

Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	DHCP options set	Route table	Network ACL	Tenancy	Default VPC
Mgmt	vpc-c5ed7abd	available	10.108.0.0/16		dopt-18a8527d	rtb-d7b9baad	acl-3d8e345	Default	No

Key	Value
Name	Mgmt
CostCenter	DevOps-108
Creator	Samal Dimdung
PointOfContact	Nick Martinelli
SecurityLevel	HIPAA
Tenant	Rean-Cloud
aws:cloudformation:logical-id	VPC
aws:cloudformation:stack-id	arn:aws:cloudformation:us-east-1:400006646297:stack/cf-rean-vpc-samal/6ba89e0-cdaa-11e7-ba83-500c28b27a35
aws:cloudformation:stack-name	cf-rean-vpc-samal

14. Subnets Public and Private, Public both has Internet Gateway attached and private with Nat Gateway.

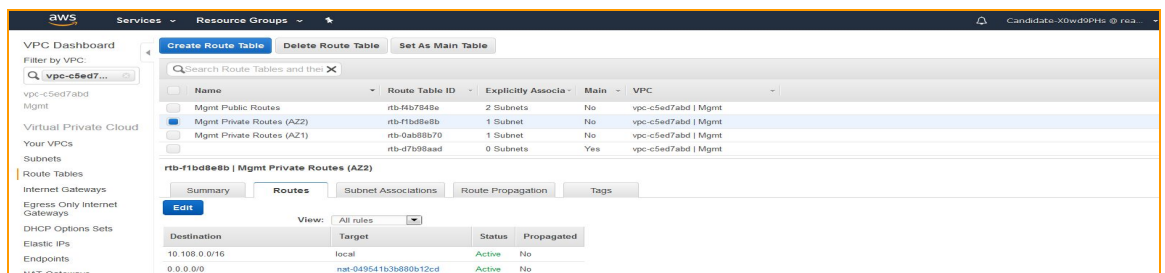


The screenshot shows the AWS VPC Dashboard. The top navigation bar includes 'aws', 'Services', 'Resource Groups', and a user profile. The main header shows 'VPC Dashboard'. Below this, there are buttons for 'Create Subnet' and 'Subnet Actions'. A search bar is present. A table lists subnets with columns: 'Name', 'Subnet ID', 'State', 'VPC', 'IPv4 CIDR', 'Available IPv4', 'IPv6 CIDR', 'Availability Zone', and 'Route Table'. Four subnets are listed: 'Mgmt Public Subnet (AZ2)', 'Mgmt Public Subnet (AZ1)', 'Mgmt Private Subnet (AZ2)', and 'Mgmt Private Subnet (AZ1)'. Below the table, there are tabs for 'Summary', 'Route Table', 'Network ACL', 'Flow Logs', and 'Tags'. The 'Tags' tab is selected, showing a table with columns 'Key' and 'Value'. The tags listed are: Name (Mgmt Public Subnet (AZ1)), CostCenter (DevOps-108), Creator (Samal Dimdung), PointOfContact (Nick Martinelli), SecurityLevel (HIPAA), Tenant (Rean-Cloud), aws:cloudformation:logical-id (PublicSubnet1), aws:cloudformation:stack-id (arn:aws:cloudformation:us-east-1:400006646297:stack/cf-rean-vpc-samal/6ba89e0-cdaa-11e7-ba83-500c28b27a35), and aws:cloudformation:stack-name (cf-rean-vpc-samal).

Name	Subnet ID	State	VPC	IPv4 CIDR	Available IPv4	IPv6 CIDR	Availability Zone	Route Table
Mgmt Public Subnet (AZ2)	subnet-bbb74e6	available	vpc-c5ed7abd   Mgmt	10.108.11.0/24	250		us-east-1b	rtb-bb7848e   Mgmt
Mgmt Public Subnet (AZ1)	subnet-df801794	available	vpc-c5ed7abd   Mgmt	10.108.10.0/24	250		us-east-1a	rtb-bb7848e   Mgmt
Mgmt Private Subnet (AZ2)	subnet-98b27dc5	available	vpc-c5ed7abd   Mgmt	10.108.21.0/24	251		us-east-1b	rtb-f1bd8e8b   Mgmt
Mgmt Private Subnet (AZ1)	subnet-545e191f	available	vpc-c5ed7abd   Mgmt	10.108.20.0/24	251		us-east-1a	rtb-0ab88b70   Mgmt

Key	Value
Name	Mgmt Public Subnet (AZ1)
CostCenter	DevOps-108
Creator	Samal Dimdung
PointOfContact	Nick Martinelli
SecurityLevel	HIPAA
Tenant	Rean-Cloud
aws:cloudformation:logical-id	PublicSubnet1
aws:cloudformation:stack-id	arn:aws:cloudformation:us-east-1:400006646297:stack/cf-rean-vpc-samal/6ba89e0-cdaa-11e7-ba83-500c28b27a35
aws:cloudformation:stack-name	cf-rean-vpc-samal

15. Private Subnet with NAT Gateway attached to routing traffic to Internet



The screenshot shows the AWS VPC Dashboard. The top navigation bar includes 'aws', 'Services', 'Resource Groups', and a user profile. The main header shows 'VPC Dashboard'. Below this, there are buttons for 'Create Route Table', 'Delete Route Table', and 'Set As Main Table'. A search bar is present. A table lists route tables with columns: 'Name', 'Route Table ID', 'Explicitly Associa', 'Main', and 'VPC'. Three route tables are listed: 'Mgmt Public Routes', 'Mgmt Private Routes (AZ2)', and 'Mgmt Private Routes (AZ1)'. Below the table, there are tabs for 'Summary', 'Routes', 'Subnet Associations', 'Route Propagation', and 'Tags'. The 'Routes' tab is selected, showing a table with columns 'Destination', 'Target', 'Status', and 'Propagated'. The routes listed are: '10.108.0.0/16' with target 'local' and status 'Active', and '0.0.0.0/0' with target 'nat-049541b3b880b12cd' and status 'Active'.

Name	Route Table ID	Explicitly Associa	Main	VPC
Mgmt Public Routes	rtb-bb7848e	2 Subnets	No	vpc-c5ed7abd   Mgmt
Mgmt Private Routes (AZ2)	rtb-f1bd8e8b	1 Subnet	No	vpc-c5ed7abd   Mgmt
Mgmt Private Routes (AZ1)	rtb-0ab88b70	1 Subnet	No	vpc-c5ed7abd   Mgmt
	rtb-d7b9baad	0 Subnets	Yes	vpc-c5ed7abd   Mgmt

Destination	Target	Status	Propagated
10.108.0.0/16	local	Active	No
0.0.0.0/0	nat-049541b3b880b12cd	Active	No



## 16. IGW with Proper tags

**Internet Gateway: igw-de0d9ea7 | Mgmt**

Summary | **Tags**

You can add tags to your resources to help you organize them. For more information, see [Tagging Your Resources](#).

**Edit**

Key	Value
Name	Mgmt
CostCenter	DevOps-108
Creator	Samal Dimdung
PointOfContact	Nick Martinelli
SecurityLevel	HIPAA
Tenant	Rean-Cloud
aws:cloudformation:logical-id	InternetGateway
aws:cloudformation:stack-id	arn:aws:cloudformation:us-east-1:400006646297:stack/cf-rean-vc-samal/6ba89e0-cdaa-11e7-ba83-500c28b27a35
aws:cloudformation:stack-name	cf-rean-vc-samal

## 17. Two Nat Gateway for redundancy ..

**NAT Gateway: nat-0d0b01e6c7ad6275**

Details | **Tags**

**Add/Edit Tags**

Key	Value
CostCenter	DevOps-108
Creator	Samal Dimdung
Name	Mgmt NatGateway One
PointOfContact	Nick Martinelli
SecurityLevel	HIPAA
Tenant	Rean-Cloud
aws:cloudformation:logical-id	NatGateway1
aws:cloudformation:stack-id	arn:aws:cloudformation:us-east-1:400006646297:stack/cf-rean-vc-samal/6ba89e0-cdaa-11e7-ba83-500c28b27a35
aws:cloudformation:stack-name	cf-rean-vc-samal

**NAT Gateway: nat-049541b3b80b12cd**

Details | **Tags**

**Add/Edit Tags**

Key	Value
CostCenter	DevOps-108
Creator	Samal Dimdung
Name	Mgmt NatGateway Two
PointOfContact	Nick Martinelli
SecurityLevel	HIPAA
Tenant	Rean-Cloud
aws:cloudformation:logical-id	NatGateway2
aws:cloudformation:stack-id	arn:aws:cloudformation:us-east-1:400006646297:stack/cf-rean-vc-samal/6ba89e0-cdaa-11e7-ba83-500c28b27a35
aws:cloudformation:stack-name	cf-rean-vc-samal



## 7 VPC Architecture

