

	This is SOP (Standard Operation Procedure) Security Group Creation using CloudFormation Templates.
--	--

## 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 4 tier shared service ( ELB Tier, Web Tier, App Tier and Dbs Tier) AWS Security Group with predefined templates which will create 4 Standard Security groups and that can be used as Shared Services Model in AWS by Multi-tenant environments.

## 2 Tools Required

Tool Name	Tool Location	Tool Description
AWS Console Access	AWs Account	AWS Console can be used to run CloudFormation Templates
		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.

[illegible]

## 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 certification.

## 5 List of Resources will be created

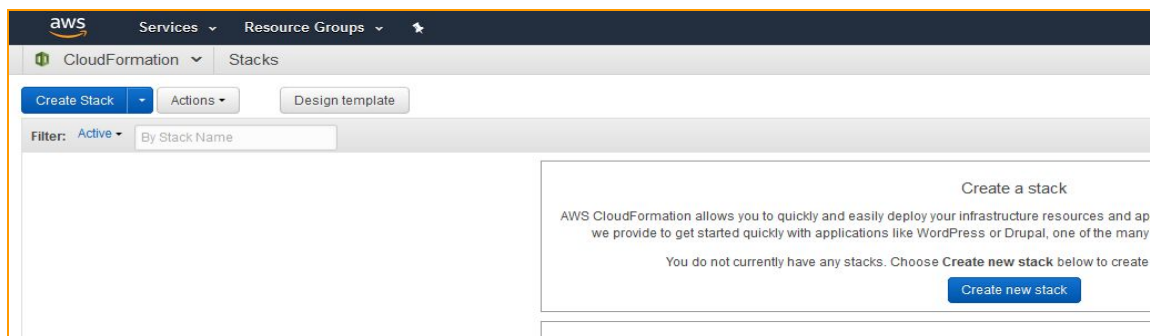
[illegible]

## 6 Produrre

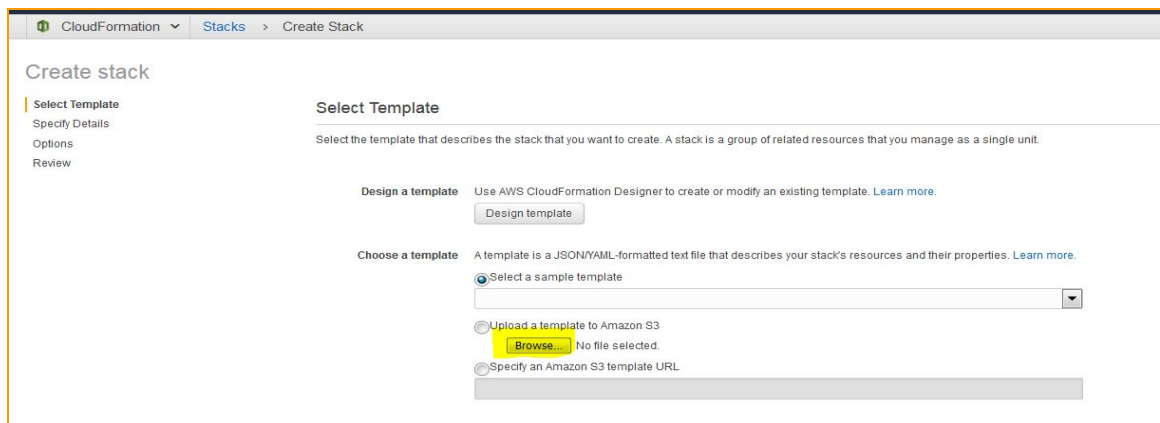
### 6.1 Creating Security Group Using CloudFormation Templates

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 to create Security group along with VPC creation time but here I'm doing each CloudFormation Templates separately.

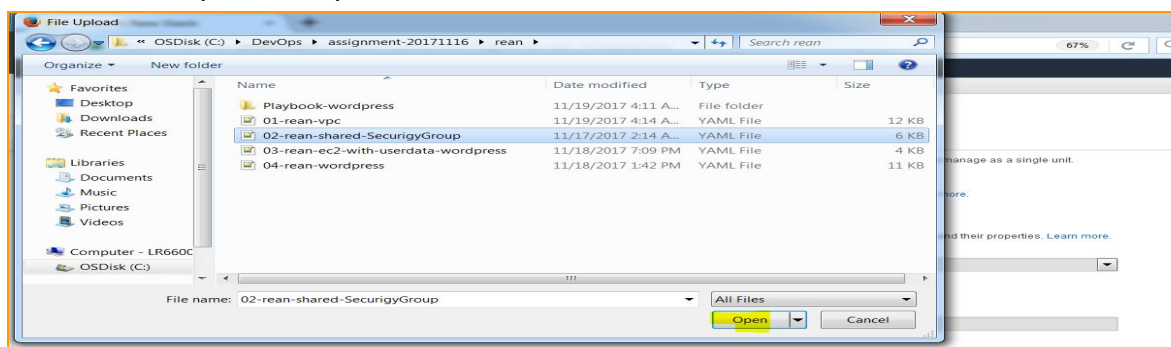
2. Create Stack



3. Browse



4. Select the Templates > Open



## 5. Alter the Value as your needs and Click Next

Create stack

Select Template  
Specify Details  
Options  
Review

### 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

CostCenterTag  Value for the Cost Center Tags

CreatorTag  Value for the Creator Tag

EnvironmentName  An environment name that will be prefixed to resource names

POCTag  Value for the Point of Contact

SecurityLevelTag  Enter the Value of Security Level ( FedRAMP, HIPAA, Standard )

TenantTag  Enter the Tenant Name

VPC  Choose which VPC the security groups should be deployed to

## 6. Leave blank in Options and Click Next ( You can configure Advance if you like to but I'm leaving blank for this demo)

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 <input type="text"/>	<input type="text"/>

#### 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

Enter role arn

Advanced

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

## 7. Review and Make sure all the Parameter you passed is correct and Click Next.

Create stack

Select Template  
Specify Details  
Options  
Review

### Review

#### Template

Template URL <https://s3-external-1.amazonaws.com/cf-templates-1twm056jwz-us-east-1/201732492v-02-rean-shared-SecurityGroup.yaml>

Description This template creates the Shared Security group for All the Tier i.e ELB, Web, App and Dbs for Rean-Cloud Clients

Estimate cost Cost

#### Details

Stack name: cf-rean-sg-samai

CostCenterTag DevOps-108

CreatorTag Samal Dimdung

EnvironmentName Mgmt

POCTag Nick Martinelli

SecurityLevelTag HIPAA

TenantTag Rean-Cloud

VPC vpc-c5ed7abd

#### Options

#### Tags

No tags provided

#### Advanced

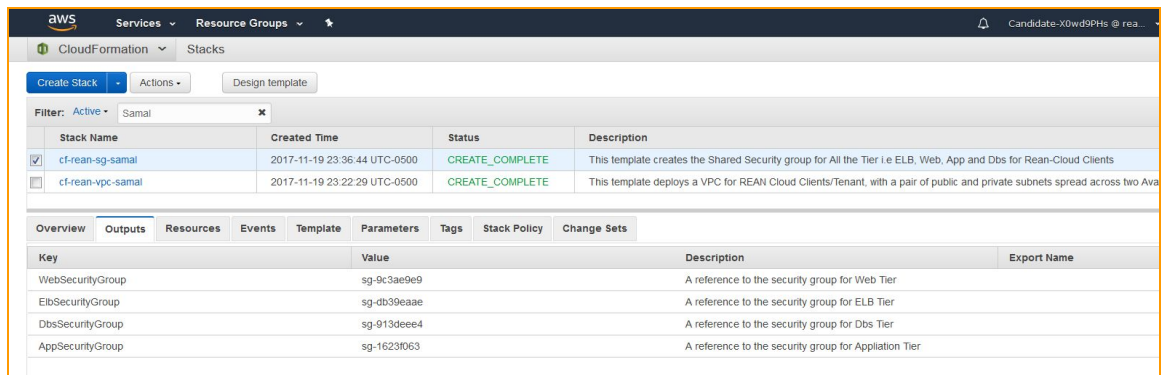
Notification

Termination Protection Disabled

Timeout none

Rollback on failure Yes

8. Once it completed you can see below details



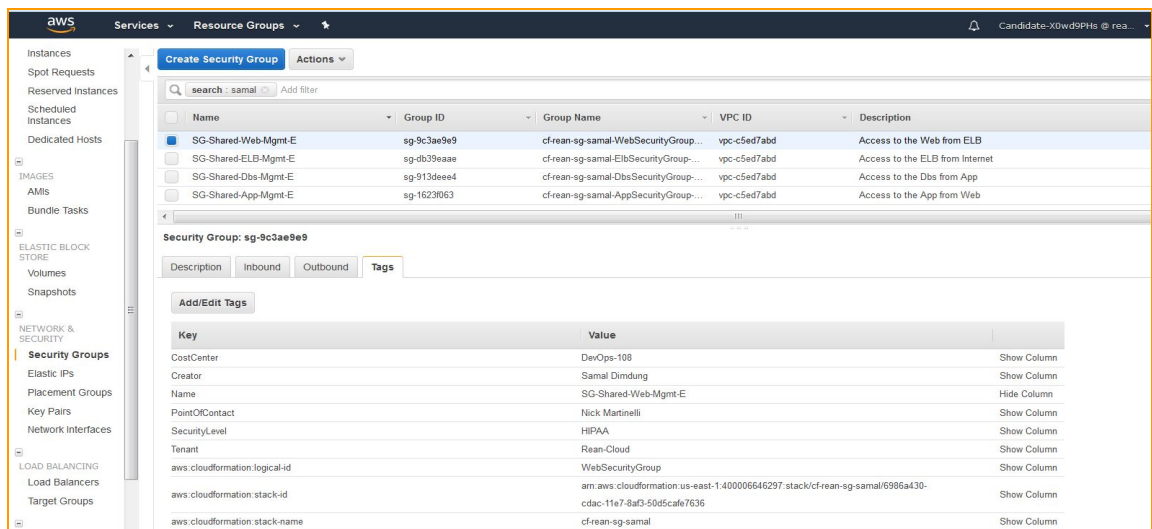
The screenshot shows the AWS CloudFormation console. The 'Stacks' section is active, and the filter is set to 'Active'. Two stacks are listed: 'cf-rean-sg-samal' and 'cf-rean-vpc-samal', both with a status of 'CREATE\_COMPLETE'. Below the list, the 'Outputs' tab is selected, showing a table with four outputs: 'WebSecurityGroup', 'ElbSecurityGroup', 'DbsSecurityGroup', and 'AppSecurityGroup', each with a value and a description.

Stack Name	Created Time	Status	Description
cf-rean-sg-samal	2017-11-19 23:36:44 UTC-0500	CREATE_COMPLETE	This template creates the Shared Security group for All the Tier i.e ELB, Web, App and Dbs for Rean-Cloud Clients
cf-rean-vpc-samal	2017-11-19 23:22:29 UTC-0500	CREATE_COMPLETE	This template deploys a VPC for REAN Cloud Clients/Tenant, with a pair of public and private subnets spread across two Ava

Key	Value	Description	Export Name
WebSecurityGroup	sg-9c3ae9e9	A reference to the security group for Web Tier	
ElbSecurityGroup	sg-db39eaae	A reference to the security group for ELB Tier	
DbsSecurityGroup	sg-913deee4	A reference to the security group for Dbs Tier	
AppSecurityGroup	sg-1623f063	A reference to the security group for Application Tier	

9. If you go the AWS Console, ec2 > Security Group sections you will see below. The Cools things is The Security Group also have tags



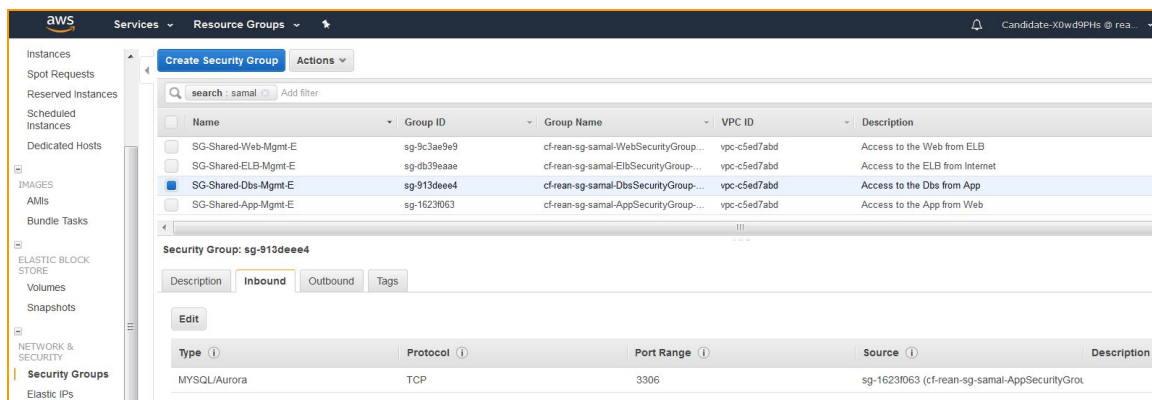
The screenshot shows the AWS Security Groups console. A list of security groups is displayed, including 'SG-Shared-Web-Mgmt-E', 'SG-Shared-ELB-Mgmt-E', 'SG-Shared-Dbs-Mgmt-E', and 'SG-Shared-App-Mgmt-E'. Below the list, the details for 'Security Group: sg-9c3ae9e9' are shown, including tabs for 'Description', 'Inbound', 'Outbound', and 'Tags'. The 'Tags' tab is active, showing a table of tags for the security group.

Name	Group ID	Group Name	VPC ID	Description
SG-Shared-Web-Mgmt-E	sg-9c3ae9e9	cf-rean-sg-samal-WebSecurityGroup...	vpc-c5ed7abd	Access to the Web from ELB
SG-Shared-ELB-Mgmt-E	sg-db39eaae	cf-rean-sg-samal-ElbSecurityGroup...	vpc-c5ed7abd	Access to the ELB from Internet
SG-Shared-Dbs-Mgmt-E	sg-913deee4	cf-rean-sg-samal-DbsSecurityGroup...	vpc-c5ed7abd	Access to the Dbs from App
SG-Shared-App-Mgmt-E	sg-1623f063	cf-rean-sg-samal-AppSecurityGroup...	vpc-c5ed7abd	Access to the App from Web

Key	Value	
CostCenter	DevOps-108	Show Column
Creator	Samal Dimdung	Show Column
Name	SG-Shared-Web-Mgmt-E	Hide Column
PointOfContact	Nick Martinelli	Show Column
SecurityLevel	HIPAA	Show Column
Tenant	Rean-Cloud	Show Column
aws:cloudformation:logical-id	WebSecurityGroup	Show Column
aws:cloudformation:stack-id	arn:aws:cloudformation:us-east-1:400006646297:stack/cf-rean-sg-samal/6986a430-cdac-11e7-8af3-50d5cafe7636	Show Column
aws:cloudformation:stack-name	cf-rean-sg-samal	Show Column

10. Inbound traffic for Dbs is only allowed for 3306 from App Security Groups, you can add or remove any number of ports for the Security Groups..



The screenshot shows the AWS Security Groups console. The 'Inbound' tab is selected for the security group 'sg-913deee4'. It shows a table of inbound rules, including a rule for 'MySQL/Aurora' on port 3306, allowing traffic from 'sg-1623f063'.

Type	Protocol	Port Range	Source	Description
MySQL/Aurora	TCP	3306	sg-1623f063 (cf-rean-sg-samal-AppSecurityGro...	

11. Done, now you can start using ..

