

Rubiscape AWS Environment

This Document describes the details about the AWS environment for   
the Production setup of Infrastructure

Infra Details Of Production

**Table of Contents**

[**AWS Environment Structure (MUMBAI) 3**](#_2jig7flnpnzi)

[Networking Architecture](#_e2lywft11e6y) 4

[Routing in AWS](#_rdlg8y5u9nel)5

[VPC](#_2o1qdvbtdyub) 6

[Security Control](#_jy7uhust7stf) 8

[EC2 Instances](#_z5zyyfz8xys3)29

[S3 Bucket:](#_e63aava8h754) 30

[Elastic IP:](#_6oxo9wyi0g5u) 31

[IAM Roles and Policies](#_r925eyq0uvc6) 32

[KMS](#_sefznsl2s7m0) 40

EKS Cluster42

Backup 48

Load Balancers 48

Route 53 51

Lambda 51

SNS 55

[**AWS Environment Structure (SYDNEY)**](#_2jig7flnpnzi) **56**

[Networking Architecture](#_e2lywft11e6y) 56

[Routing in AWS](#_rdlg8y5u9nel)58

[VPC](#_2o1qdvbtdyub)  59

[Security Control](#_jy7uhust7stf) 60

[EC2 Instances](#_z5zyyfz8xys3)67

[S3 Bucket:](#_e63aava8h754) 67

[Elastic IP:](#_6oxo9wyi0g5u) 68

[IAM Roles](#_r925eyq0uvc6) 68

[KMS](#_sefznsl2s7m0) 69

Load Balancers 70

Lambda 71

SNS 72

# **MUMBAI REGION**

# **AWS Environment Structure:**

The new AWS environment setup is done using the AWS native resources only like VPC, subnets, EC2, ECS, Application Load Balancer.

|  |  |
| --- | --- |
| Environment | Description |
| PROD Environment | Production environment |

## 

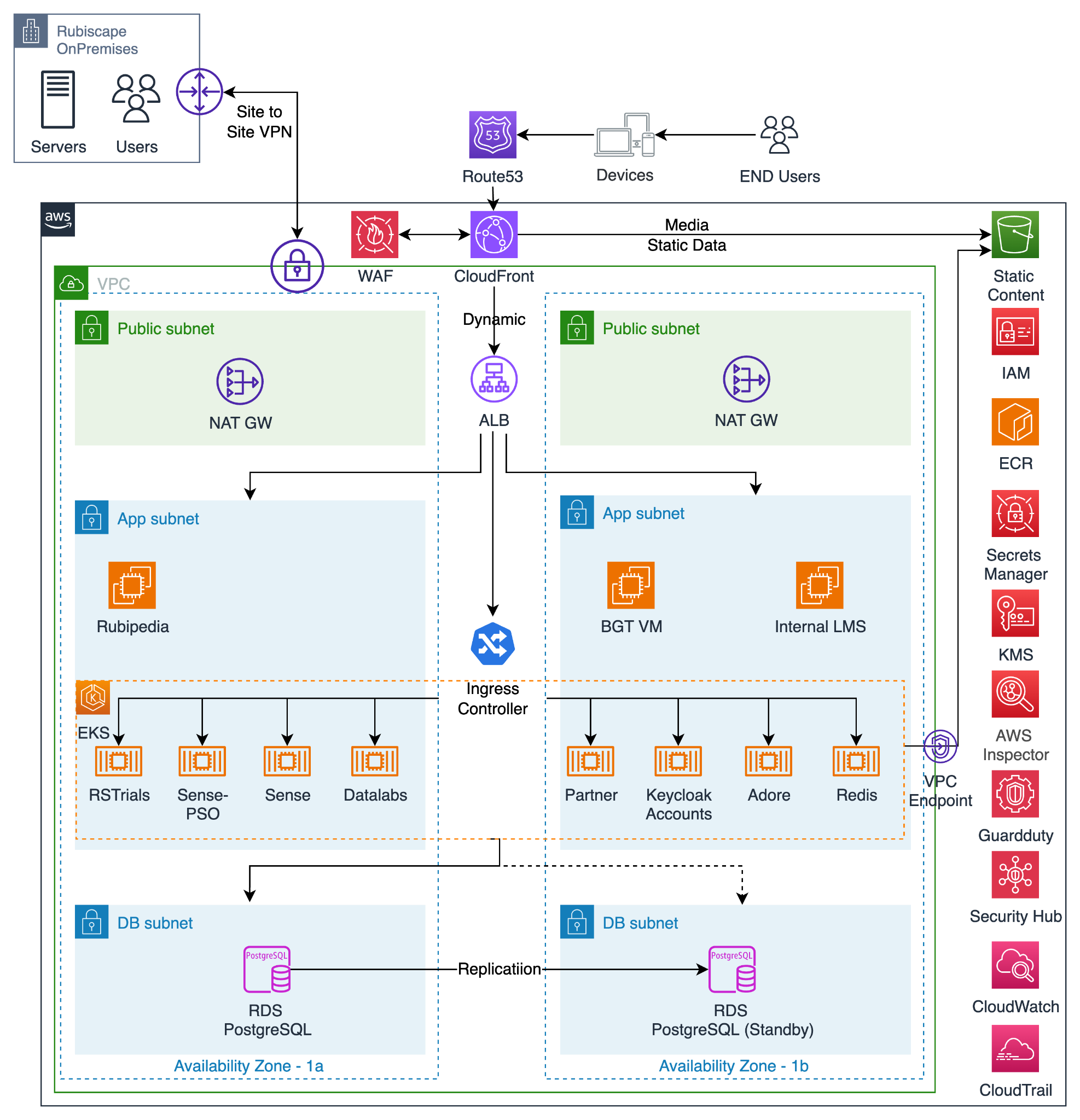
## **Networking Architecture:**

In AWS Virtual Private Cloud (VPC) provides secure Networking for the resources in AWS. Searce team will create the networking based on the below architecture. It will be configured with its own network access control list (NACL), and routing table. The following sections cover a detailed explanation of all components.

Please find the application details about Streamlyn Business Line below.

|  |  |
| --- | --- |
| Environment | Application Name |
| PROD | Adore |
| PROD | BTG VM |
| PROD | Accounts |
| PROD | Jenkins-Prod |
| PROD | rubiscape-pritunl-vpn |
| PROD | Datalabs App EKS |
| PROD | Partner App EKS |
| PROD | Sense App EKS |
| DEV | ZAP |
| DEV | Docker-Backend |
| DEV | DataSync |
| MONITOR | Monitoring-Nodegroup1 |
| MONITOR | Monitoring-Nodegroup2 |

**Architectures:**

****

## **Routing in AWS:**

### **Route Tables:**

A route table contains a set of rules called routes that are used to determine where network traffic is directed. The following tables describe the route table rules and subnet associations.

### **Route Table and Subnet Associations**

A route table contains a set of rules called routes that are used to determine where network traffic is directed.

### **Production VPC Route Tables:**

* **Public RTB:** This RTB is attached to the public subnets that can communicate with the following destination CIDRs.
* **Private RTB:** This RTB is attached to the private subnets that can communicate with the following destination CIDRs.

**Public Route Table ID:** **rtb-0326b88e0aefcd1b9**

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Destination** | **Target** | **Subnet Associations** |
| rubiscape-prod-public-rt | 0.0.0.0/0 172.16.192.0/20  172.31.0.0/16 | [igw-0285931a4ccd1d345](https://ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#igws:internetGatewayId=igw-0285931a4ccd1d345) local  [pcx-05ccb34b6c22996cb](https://ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#PeeringConnections:vpcPeeringConnectionId=pcx-05ccb34b6c22996cb) | rubiscape-prod-public-1b-subnet  rubiscape-prod-public-1a-subnet |

**Private Route Table ID:** **rtb-06e60fe7a694267af**

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Destination** | **Target** | **Subnet Associations** |
| rubiscape-prod-db-rt | 0.0.0.0/0 172.16.192.0/20  172.31.0.0/16 | [nat-0fc27f4629784ff4a](https://ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#NatGateways:natGatewayId=nat-0fc27f4629784ff4a) local  [pcx-05ccb34b6c22996cb](https://ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#PeeringConnections:vpcPeeringConnectionId=pcx-05ccb34b6c22996cb) | rubiscape-prod-db-1a-subnet  rubiscape-prod-db-1b-subnet |

**Private Route Table ID:** **rtb-059fbc0213b7d0fff**

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Destination** | **Target** | **Subnet Associations** |
| rubiscape-prod-app-rt | 0.0.0.0/0 172.16.192.0/20  172.31.0.0/16 | [nat-0d5a76ccdc1ef9028](https://ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#NatGateways:natGatewayId=nat-0d5a76ccdc1ef9028) local  [pcx-05ccb34b6c22996cb](https://ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#PeeringConnections:vpcPeeringConnectionId=pcx-05ccb34b6c22996cb) | rubiscape-prod-app-1b-subnet  rubiscape-prod-app-1a-subnet |

## 

**Private Route Table ID:** **rtb-047e472752fee0caf**

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Destination** | **Target** | **Subnet Associations** |
| - | 172.16.192.0/20 | local | - |

## 

## **VPC:**

Amazon **VPC (Virtual Private Cloud)** is a networking service that allows you to create a **secure, isolated** virtual network within AWS. It enables you to define your own **IP address ranges, subnets, routing, and security settings**, providing full control over your cloud network.

The Production VPC is configured with four-tier architecture.

|  |  |
| --- | --- |
| **Tier** | **Purpose** |
| Public Subnet | This tier is a public subnet that hosts externally facing services that require unique IPs and that are directly accessed. It also hosts the NAT gateway which will be leveraged by all the workload instances to access the internet. |
| Private Subnet | This tier is a private subnet. |

The following tables describe the Security VPC name and VPC ID’s.

### **VPC details:**

|  |  |
| --- | --- |
| **NAME** | **VPC ID** |
| **rubiscape-prod-vpc** | vpc-0166b8961a64fe74a |

### 

### **Subnet IP Ranges:**

Production VPC is provisioned with **172.16.192.0/20** CIDRs and it contains six private and two public subnets. These subnets have been created in **ap-south-1 (Mumbai)** region.

| **Subnets** | **CIDR** |
| --- | --- |
| rubiscape-prod-db-1a-subnet | 172.16.200.0/23 |
| rubiscape-prod-db-1b-subnet | 172.16.202.0/23 |
| rubiscape-prod-app-1a-subnet | 172.16.192.0/22 |
| rubiscape-prod-app-1b-subnet | 172.16.204.0/22 |
| rubiscape-prod-public-1a-subnet | 172.16.196.0/23 |
| rubiscape-prod-public-1b-subnet | 172.16.198.0/23 |

### 

### 

## **Security Control:**

AWS Services like Security Groups and Network Access control can be leveraged to provide firewall capabilities and security control.

### **NACLs:**

NACLs provide stateless firewall capabilities that can only be applied at the subnet level. NACLs are best used for blacklisting ports, services, or hosts for entire subnets. Given their stateless nature, any bi-directional communications would require ingress and Egress NACL (Outbound) rules to be configured. NACLs will be used sparingly as heavy implementation of NACLs can result in unexpected network communication blocks and difficulty to troubleshoot. NACLs will be used as guardrails to blacklist all ingress or egress traffic to subnets that should never occur.

Below is the list of Ingress and Egress rules that will be applied for the NACLs in **Prod and DEV VPCs**.

The following table provides the NACL details in different VPCs.

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Network ACL ID** | **Associated with** | **Default** |
| - | acl-0670db58c68baef38 | All the Subnets in the VPC | YES |

The **NACLs** have the following Ingress and Egress rules.

**Ingress NACL (Inbound)**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Rule** | **Type** | **Protocol** | **Port Range** | **Destination** | **Allow/Deny** |
| 100 | ALL Traffic | ALL | ALL | 0.0.0.0/0 | ALLOW |
| \* | ALL Traffic | ALL | ALL | 0.0.0.0/0 | DENY |

**Note:** In the AWS Console you can see the **Destination** as the **Source.**

Egress NACL (Outbound)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Rule** | **Type** | **Protocol** | **Port Range** | **Destination** | **Allow/Deny** |
| 100 | ALL Traffic | ALL | ALL | 0.0.0.0/0 | ALLOW |
| \* | ALL Traffic | ALL | ALL | 0.0.0.0/0 | DENY |

**Note:** In the AWS Console you can see the **Destination** as the **Source.**

### **Security Groups:**

Security Groups provide stateful firewall capabilities that can be applied directly to AWS resources. Security Groups will be used within the environment to prevent communication between hosts and tiers that do not require direct access.

The security groups can be used to restrict access between Business Unit applications and services as well as between tiers, such as web and app tiers. A standardized Security Group approach is recommended. AWS resources should have a baseline of up to three security groups applied depending on role. The following diagram shows the different security groups that may be applied.



***Figure 2: Security Group Layered Approach***

**Security Group Design:**

In addition to standard port requirements that are configured as part of the base infrastructure, the following application specific ports will be added to the required Security Groups in the Management, Security and Workload VPCs.

#### **Prod VPC Security Groups:**

This section describes the Prod VPC security groups and its inbound and outbound rules.

The following table provides the Security group Name and Security-ID details.

|  |  |  |
| --- | --- | --- |
| **Security Group Name** | **Group ID** | **VPCID** |
| k8s-tomcatgroup-9308729354 | [sg-08445262e6190c45e](https://ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#SecurityGroup:groupId=sg-08445262e6190c45e) | vpc-0166b8961a64fe74a |
| rubiscape-prod-zap-ec2-sg | [sg-09afdda5a09410511](https://ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#SecurityGroup:groupId=sg-09afdda5a09410511) | vpc-0166b8961a64fe74a |
| k8s-monitori-promethe-0f81f9213d | [sg-0f937f887641e2106](https://ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#SecurityGroup:groupId=sg-0f937f887641e2106) | vpc-0166b8961a64fe74a |
| launch-wizard-4 | [sg-0f90034f1f2dec37f](https://ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#SecurityGroup:groupId=sg-0f90034f1f2dec37f) | vpc-0166b8961a64fe74a |
| eks-cluster-sg-rubiscape-prod-cluster-100371083 | [sg-00b47e0487df1ad75](https://ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#SecurityGroup:groupId=sg-00b47e0487df1ad75) | vpc-0166b8961a64fe74a |
| k8s-monitori-promethe-314eeb990d | [sg-0857793265b6a40c0](https://ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#SecurityGroup:groupId=sg-0857793265b6a40c0) | vpc-0166b8961a64fe74a |
| docker-test-sg | [sg-0e8be6c87600ef519](https://ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#SecurityGroup:groupId=sg-0e8be6c87600ef519) | vpc-0166b8961a64fe74a |
| rubiscape-prod-efs-sg | [sg-0a4cf47ba41f28b5f](https://ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#SecurityGroup:groupId=sg-0a4cf47ba41f28b5f) | vpc-0166b8961a64fe74a |
| default | [sg-0ce70ca9f9208d7d5](https://ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#SecurityGroup:groupId=sg-0ce70ca9f9208d7d5) | vpc-0166b8961a64fe74a |
| rubiscape-prod-accounts-ec2-sg | [sg-0e1d088909a9eb93e](https://ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#SecurityGroup:groupId=sg-0e1d088909a9eb93e) | vpc-0166b8961a64fe74a |
| rubiscape-prod-adore-ec2-sg | [sg-014960e459ab648e0](https://ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#SecurityGroup:groupId=sg-014960e459ab648e0) | vpc-0166b8961a64fe74a |
| k8s-traffic-rubiscapeprodcluster-48ee223d75 | [sg-009e6aef61225f084](https://ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#SecurityGroup:groupId=sg-009e6aef61225f084) | vpc-0166b8961a64fe74a |
| k8s-sensegroup-8055f9bd5e | [sg-05ef51d1fa712e254](https://ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#SecurityGroup:groupId=sg-05ef51d1fa712e254) | vpc-0166b8961a64fe74a |
| rubiscape-prod-ec2-sg | [sg-01ae8fd2e9e787355](https://ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#SecurityGroup:groupId=sg-01ae8fd2e9e787355) | vpc-0166b8961a64fe74a |
| k8s-datalabgroup-fec27433a7 | [sg-0a1a17e63974260d2](https://ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#SecurityGroup:groupId=sg-0a1a17e63974260d2) | vpc-0166b8961a64fe74a |
| rubiscape-prod-ALB-sg | [sg-0b566f27368c30abd](https://ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#SecurityGroup:groupId=sg-0b566f27368c30abd) | vpc-0166b8961a64fe74a |
| jenkins | [sg-020052f4345f08e3c](https://ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#SecurityGroup:groupId=sg-020052f4345f08e3c) | vpc-0166b8961a64fe74a |
| rubiscape-prod-eks-sg | [sg-0cb25495666abbab7](https://ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#SecurityGroup:groupId=sg-0cb25495666abbab7) | vpc-0166b8961a64fe74a |
| rubiscape-mumbai-pritunl-sg | [sg-0739de8c8562034d9](https://ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#SecurityGroup:groupId=sg-0739de8c8562034d9) | vpc-0166b8961a64fe74a |

##### 

##### **K8s-tomcatgroup-9308729354** **Security Group:**

The following table provides the Security group Name and Security-ID details.

|  |  |  |
| --- | --- | --- |
| **Security Group Name** | **Group ID** | **VPCID** |
| k8s-tomcatgroup-9308729354 | [sg-08445262e6190c45e](https://ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#SecurityGroup:groupId=sg-08445262e6190c45e) | vpc-0166b8961a64fe74a |

The k8s-tomcatgroup-9308729354 has the following inbound and outbound rules.

###### 

###### **Inbound:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Type** | **Protocol** | **Port Range** | **Source** | **Description** |
| HTTP | TCP | 80 | 0.0.0.0/0 | - |
| HTTPS | TCP | 443 | 0.0.0.0/0 | - |

#### 

###### **Outbound**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Type** | **Protocol** | **Port Range** | **Source** | **Description** |
| All traffic | ALL | ALL | 0.0.0.0/0 | Anywhere |

##### 

##### **rubiscape-prod-zap-ec2-sg:**

The following table provides the Security group Name and Security-ID details.

|  |  |  |
| --- | --- | --- |
| **Name** | **Group ID** | **VPCID** |
| rubiscape-prod-zap-ec2-sg | [sg-09afdda5a09410511](https://ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#SecurityGroup:groupId=sg-09afdda5a09410511) | vpc-0166b8961a64fe74a |

The rubiscape-prod-zap-ec2-sg has the following inbound and outbound rules.

###### **Inbound**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Type** | **Protocol** | **Port Range** | **Source** | **Description** |
| SSH | TCP | 22 | 172.16.198.249/32 | - |
| Custom TCP | TCP | 8080 | [sg-0b566f27368c30abd / rubiscape-prod-ALB-sg](https://ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#SecurityGroup:groupId=sg-0b566f27368c30abd) | - |

###### **Outbound**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Type** | **Protocol** | **Port Range** | **Source** | **Description** |
| All traffic | ALL | ALL | 0.0.0.0/0 | Anywhere |

##### **K8s-monitori-promethe-0f81f9213d Security Group:**

The following table provides the Security group Name and Security-ID details.

|  |  |  |
| --- | --- | --- |
| **Name** | **Group ID** | **VPCID** |
| k8s-monitori-promethe-0f81f9213d | [sg-0f937f887641e2106](https://ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#SecurityGroup:groupId=sg-0f937f887641e2106) | vpc-0166b8961a64fe74a |

###### **Inbound**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Type** | **Protocol** | **Port Range** | **Source** | **Description** |
| HTTP | TCP | 80 | 0.0.0.0/0 | Allow inbound traffic from internet |

#### 

###### **Outbound**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Type** | **Protocol** | **Port Range** | **Source** | **Description** |
| All traffic | ALL | ALL | 0.0.0.0/0 | Anywhere |

##### 

##### **Sg-0f90034f1f2dec37f Security Group:**

The following table provides the Security group Name and Security-ID details.

|  |  |  |
| --- | --- | --- |
| **Name** | **Group ID** | **VPCID** |
| launch-wizard-4 | [sg-0f90034f1f2dec37f](https://ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#SecurityGroup:groupId=sg-0f90034f1f2dec37f) | vpc-0166b8961a64fe74a |

#### 

###### **Inbound**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Type** | **Protocol** | **Port Range** | **Source** | **Description** |
| All traffic | ALL | ALL | 0.0.0.0/0 | Anywhere |

###### **Outbound**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Type** | **Protocol** | **Port Range** | **Source** | **Description** |
| All traffic | ALL | ALL | 0.0.0.0/0 | Anywhere |

##### **eks-cluster-sg-rubiscape-prod-cluster-100371083 Security Group:**

The following table provides the Security group Name and Security-ID details.

|  |  |  |
| --- | --- | --- |
| **Name** | **Group ID** | **VPCID** |
| eks-cluster-sg-rubiscape-prod-cluster-100371083 | [sg-00b47e0487df1ad75](https://ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#SecurityGroup:groupId=sg-00b47e0487df1ad75) | vpc-0166b8961a64fe74a |

###### **Inbound**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Type** | **Protocol** | **Port Range** | **Source** | **Description** |
| Custom TCP | TCP | 3000-32590 | * [sg-009e6aef61225f084 / k8s-traffic-rubiscapeprodcluster-48ee223d75](https://ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#SecurityGroup:groupId=sg-009e6aef61225f084) | - |
| ALL TRAFFIC | ALL | ALL | [sg-00b47e0487df1ad75 / eks-cluster-sg-rubiscape-prod-cluster-100371083](https://ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#SecurityGroup:groupId=sg-00b47e0487df1ad75) | - |
| ALL TRAFFIC | ALL | ALL | 172.16.192.0/20 |  |

###### **Outbound**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Type** | **Protocol** | **Port Range** | **Source** | **Description** |
| All traffic | ALL | ALL | 0.0.0.0/0 | Anywhere |

##### **k8s-monitori-promethe-314eeb990d Group:**

The following table provides the Security group Name and Security-ID details.

|  |  |  |
| --- | --- | --- |
| **Name** | **Group ID** | **VPCID** |
| k8s-monitori-promethe-314eeb990d | [sg-0857793265b6a40c0](https://ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#SecurityGroup:groupId=sg-0857793265b6a40c0) | vpc-0166b8961a64fe74a |

#### 

###### **Inbound**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Type** | **Protocol** | **Port Range** | **Source** | **Description** |
| HTTP | TCP | 80 | 0.0.0.0/0 | - |

###### **Outbound**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Type** | **Protocol** | **Port Range** | **Source** | **Description** |
| All traffic | ALL | ALL | 0.0.0.0/0 | Anywhere |

### 

##### **Docker-test-sg** **Security Group:**

The following table provides the Security group Name and Security-ID details.

|  |  |  |
| --- | --- | --- |
| **Name** | **Group ID** | **VPCID** |
| docker-test-sg | [sg-0e8be6c87600ef519](https://ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#SecurityGroup:groupId=sg-0e8be6c87600ef519) | vpc-0166b8961a64fe74a |

###### **Inbound**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Type** | **Protocol** | **Port Range** | **Source** | **Description** |
| HTTP | TCP | 80 | 0.0.0.0/0 | - |
| SSH | TCP | 22 | 61.95.158.116/32 | - |
| ALL TRAFFIC | ALL | ALL | * 172.16.192.0/20 | - |
| SSH | TCP | 22 | * 49.37.133.79/32 | Nagababu Home IP |

#### 

###### **Outbound**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Type** | **Protocol** | **Port Range** | **Source** | **Description** |
| All traffic | ALL | ALL | 0.0.0.0/0 | Anywhere |

##### **rubiscape-prod-efs-sg Security Group:**

The following table provides the Security group Name and Security-ID details.

|  |  |  |
| --- | --- | --- |
| **Name** | **Group ID** | **VPCID** |
| rubiscape-prod-efs-sg | [sg-0a4cf47ba41f28b5f](https://ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#SecurityGroup:groupId=sg-0a4cf47ba41f28b5f) | vpc-0166b8961a64fe74a |

#### 

###### **Inbound**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Type** | **Protocol** | **Port Range** | **Source** | **Description** |
| NFS | TCP | 2049 | * [sg-0cb25495666abbab7 / rubiscape-prod-eks-sg](https://ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#SecurityGroup:groupId=sg-0cb25495666abbab7) | - |
| NFS | TCP | 2049 | * 172.16.192.0/20 | VPC CIDR |

###### **Outbound:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Type** | **Protocol** | **Port Range** | **Source** | **Description** |
| All traffic | ALL | ALL | 0.0.0.0/0 | OUTBOUND RULE |

### 

##### **default Security Group:**

The following table provides the Security group Name and Security-ID details.

|  |  |  |
| --- | --- | --- |
| **Name** | **Group ID** | **VPCID** |
| default | [sg-0ce70ca9f9208d7d5](https://ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#SecurityGroup:groupId=sg-0ce70ca9f9208d7d5) | vpc-0166b8961a64fe74a |

###### **Inbound:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Type** | **Protocol** | **Port Range** | **Source** | **Description** |
| NFS | TCP | 2049 | * 0.0.0.0/0 | - |
| ALL TRAFFIC | ALL | ALL | * 0.0.0.0/0 | - |

###### **Outbound**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Type** | **Protocol** | **Port Range** | **Source** | **Description** |
| All traffic | ALL | ALL | 0.0.0.0/0 | Anywhere |

##### **rubiscape-prod-accounts-ec2-sg Security Group:**

The following table provides the Security group Name and Security-ID details.

|  |  |  |
| --- | --- | --- |
| **Name** | **Group ID** | **VPCID** |
| rubiscape-prod-accounts-ec2-sg | [sg-0e1d088909a9eb93e](https://ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#SecurityGroup:groupId=sg-0e1d088909a9eb93e) | vpc-0166b8961a64fe74a |

###### 

###### **Inbound:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Type** | **Protocol** | **Port Range** | **Source** | **Description** |
| SSH | TCP | 22 | * 172.16.198.249/32 | - |
| Custom TCP | TCP | 9091 | * [sg-0b566f27368c30abd / rubiscape-prod-ALB-sg](https://ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#SecurityGroup:groupId=sg-0b566f27368c30abd) | - |

###### **Outbound**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Type** | **Protocol** | **Port Range** | **Source** | **Description** |
| All traffic | ALL | ALL | 0.0.0.0/0 | Anywhere |

##### 

##### 

##### 

##### **rubiscape-prod-adore-ec2-sg Group:**

The following table provides the Security group Name and Security-ID details.

|  |  |  |
| --- | --- | --- |
| **Name** | **Group ID** | **VPCID** |
| rubiscape-prod-adore-ec2-sg | [sg-014960e459ab648e0](https://ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#SecurityGroup:groupId=sg-014960e459ab648e0) | vpc-0166b8961a64fe74a |

###### **Inbound:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Type** | **Protocol** | **Port Range** | **Source** | **Description** |
| SSH | TCP | 22 | 172.16.198.249/32 | - |
| CUSTOM TCP | TCP | 8123 | 172.16.198.249/32 | - |
| CUSTOM TCP | TCP | 8123 | [sg-0b566f27368c30abd / rubiscape-prod-ALB-sg](https://ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#SecurityGroup:groupId=sg-0b566f27368c30abd) | - |
| CUSTOM TCP | TCP | 8124 | [sg-0b566f27368c30abd / rubiscape-prod-ALB-sg](https://ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#SecurityGroup:groupId=sg-0b566f27368c30abd) | - |
| CUSTOM TCP | TCP | 8888 | [sg-0b566f27368c30abd / rubiscape-prod-ALB-sg](https://ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#SecurityGroup:groupId=sg-0b566f27368c30abd) | - |
| CUSTOM TCP | TCP | 9999 | [sg-0b566f27368c30abd / rubiscape-prod-ALB-sg](https://ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#SecurityGroup:groupId=sg-0b566f27368c30abd) | - |

#### 

###### **Outbound:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Type** | **Protocol** | **Port Range** | **Source** | **Description** |
| All traffic | ALL | ALL | 0.0.0.0/0 | OUTBOUND RULE |

##### **k8s-traffic-rubiscapeprodcluster-48ee223d75 security group:**

The following table provides the Security group Name and Security-ID details.

|  |  |  |
| --- | --- | --- |
| **Name** | **Group ID** | **VPCID** |
| k8s-traffic-rubiscapeprodcluster-48ee223d75 | [sg-009e6aef61225f084](https://ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#SecurityGroup:groupId=sg-009e6aef61225f084) | vpc-0166b8961a64fe74a |

###### **Inbound:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Type** | **Protocol** | **Port Range** | **Source** | **Description** |
| - | - | - | * - | - |

#### 

###### **Outbound:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Type** | **Protocol** | **Port Range** | **Source** | **Description** |
| All traffic | ALL | ALL | 0.0.0.0/0 | OUTBOUND RULE |

##### 

##### **k8s-sensegroup-8055f9bd5e Security Group:**

The following table provides the Security group Name and Security-ID details.

|  |  |  |
| --- | --- | --- |
| **Name** | **Group ID** | **VPCID** |
| k8s-sensegroup-8055f9bd5e | [sg-05ef51d1fa712e254](https://ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#SecurityGroup:groupId=sg-05ef51d1fa712e254) | vpc-0166b8961a64fe74a |

###### 

###### **Inbound:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Type** | **Protocol** | **Port Range** | **Source** | **Description** |
| HTTP | TCP | 80 | * 0.0.0.0/0 | - |
| HTTPS | TCP | 443 | * 0.0.0.0/0 | - |

###### **Outbound:**

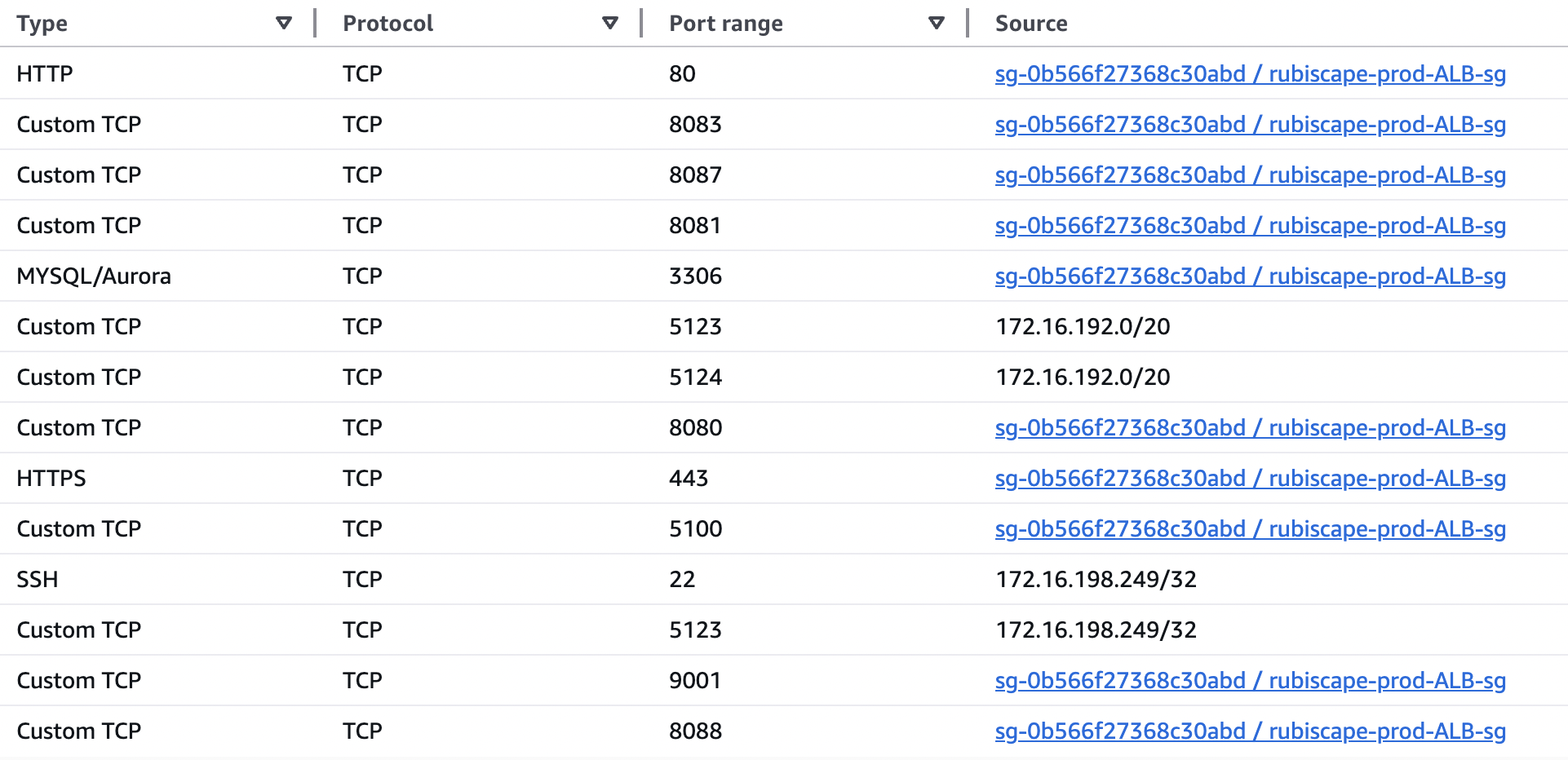
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Type** | **Protocol** | **Port Range** | **Source** | **Description** |
| All traffic | ALL | ALL | 0.0.0.0/0 | Anywhere |

##### **rubiscape-prod-ec2-sg Security Group:**

The following table provides the Security group Name and Security-ID details.

|  |  |  |
| --- | --- | --- |
| **Name** | **Group ID** | **VPCID** |
| rubiscape-prod-ec2-sg | [sg-01ae8fd2e9e787355](https://ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#SecurityGroup:groupId=sg-01ae8fd2e9e787355) | vpc-0166b8961a64fe74a |

**INBOUND:**



###### **Outbound:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Type** | **Protocol** | **Port Range** | **Source** | **Description** |
| All traffic | ALL | ALL | 0.0.0.0/0 | Anywhere |

##### **k8s-datalabgroup-fec27433a7 Security Group:**

The following table provides the Security group Name and Security-ID details.

|  |  |  |
| --- | --- | --- |
| **Name** | **Group ID** | **VPCID** |
| k8s-datalabgroup-fec27433a7 | [sg-0a1a17e63974260d2](https://ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#SecurityGroup:groupId=sg-0a1a17e63974260d2) | vpc-0166b8961a64fe74a |

**INBOUND:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Type** | **Protocol** | **Port Range** | **Source** | **Description** |
| HTTP | TCP | 80 | 0.0.0.0/0 | Anywhere |
| HTTPS | TCP | 443 | 0.0.0.0/0 | Anywhere |

###### **Outbound:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Type** | **Protocol** | **Port Range** | **Source** | **Description** |
| All traffic | ALL | ALL | 0.0.0.0/0 | Anywhere |

##### 

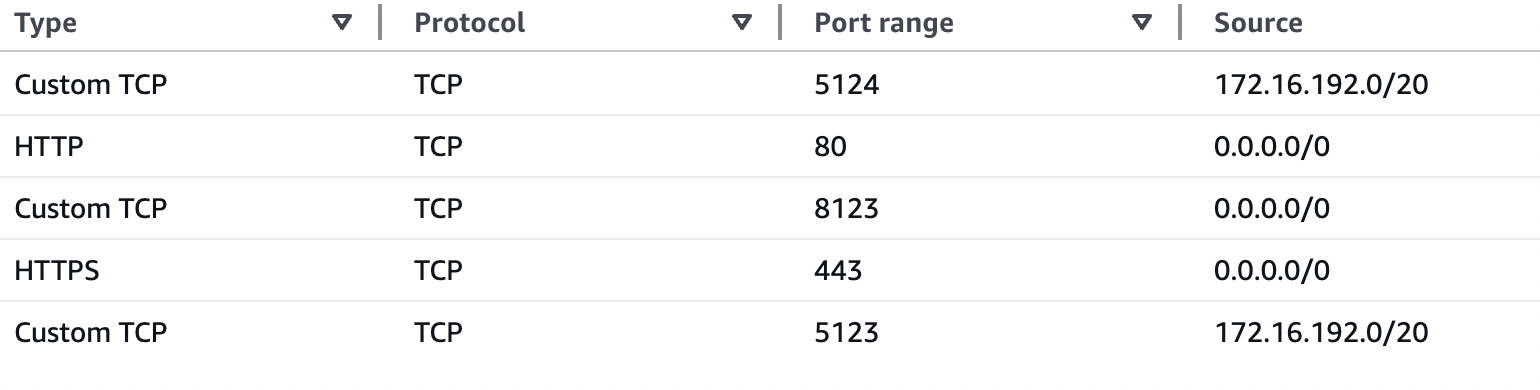
##### 

##### **rubiscape-prod-ALB-sg Security Group:**

The following table provides the Security group Name and Security-ID details.

|  |  |  |
| --- | --- | --- |
| **Name** | **Group ID** | **VPCID** |
| rubiscape-prod-ALB-sg | [sg-0b566f27368c30abd](https://ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#SecurityGroup:groupId=sg-0b566f27368c30abd) | vpc-0166b8961a64fe74a |

**INBOUND:**



###### **Outbound:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Type** | **Protocol** | **Port Range** | **Source** | **Description** |
| All traffic | ALL | ALL | 0.0.0.0/0 | Anywhere |

##### 

##### 

##### **Jenkins Security Group:**

The following table provides the Security group Name and Security-ID details.

|  |  |  |
| --- | --- | --- |
| **Name** | **Group ID** | **VPCID** |
| jenkins | [sg-020052f4345f08e3c](https://ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#SecurityGroup:groupId=sg-020052f4345f08e3c) | vpc-0166b8961a64fe74a |

**INBOUND:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Type** | **Protocol** | **Port Range** | **Source** | **Description** |
| SSH | TCP | 22 | [sg-0739de8c8562034d9 / rubiscape-mumbai-pritunl-sg](https://ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#SecurityGroup:groupId=sg-0739de8c8562034d9) | - |
| HTTP | TCP | 80 | [sg-0739de8c8562034d9 / rubiscape-mumbai-pritunl-sg](https://ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#SecurityGroup:groupId=sg-0739de8c8562034d9) | - |
| CUSTOM TCP | TCP | 8080 | [sg-0739de8c8562034d9 / rubiscape-mumbai-pritunl-sg](https://ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#SecurityGroup:groupId=sg-0739de8c8562034d9) | - |

###### **Outbound:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Type** | **Protocol** | **Port Range** | **Source** | **Description** |
| All traffic | ALL | ALL | 0.0.0.0/0 | Anywhere |

##### **Rubiscape-prod-eks-sg** **Security Group:**

The following table provides the Security group Name and Security-ID details.

|  |  |  |
| --- | --- | --- |
| **Name** | **Group ID** | **VPCID** |
| rubiscape-prod-eks-sg | [sg-0cb25495666abbab7](https://ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#SecurityGroup:groupId=sg-0cb25495666abbab7) | vpc-0166b8961a64fe74a |

**INBOUND:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Type** | **Protocol** | **Port Range** | **Source** | **Description** |
| ALL TRAFFIC | ALL | ALL | 172.16.192.0/20 | - |
| HTTPS | TCP | 443 | 0.0.0.0/0 | - |
| NFS | TCP | 2049 | 172.16.192.0/20 | - |
| HTTP | TCP | 80 | 0.0.0.0/0 | - |

###### **Outbound:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Type** | **Protocol** | **Port Range** | **Source** | **Description** |
| All traffic | ALL | ALL | 0.0.0.0/0 | Anywhere |

##### **Rubiscape-mumbai-pritunl-sg** **Security Group:**

The following table provides the Security group Name and Security-ID details.

|  |  |  |
| --- | --- | --- |
| **Name** | **Group ID** | **VPCID** |
| rubiscape-mumbai-pritunl-sg | [sg-0739de8c8562034d9](https://ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#SecurityGroup:groupId=sg-0739de8c8562034d9) | vpc-0166b8961a64fe74a |

**INBOUND:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Type** | **Protocol** | **Port Range** | **Source** | **Description** |
| CUSTOM UDP | UDP | 1194 | 0.0.0.0/0 | - |
| HTTP | TCP | 80 | 0.0.0.0/0 | - |
| SSH | TCP | 22 | [sg-0739de8c8562034d9 / rubiscape-mumbai-pritunl-sg](https://ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#SecurityGroup:groupId=sg-0739de8c8562034d9) | - |
| HTTPS | TCP | 443 | 0.0.0.0/0 | - |

###### **Outbound:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Type** | **Protocol** | **Port Range** | **Source** | **Description** |
| All traffic | ALL | ALL | 0.0.0.0/0 | Anywhere |

## **EC2 Instances:**

Amazon **EC2 (Elastic Compute Cloud)** is a cloud-based virtual server service that provides scalable compute capacity. It allows users to launch, configure, and manage virtual machines (instances) on demand, without needing physical hardware.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Name** | **Private IP address** | **Instance ID** | **Subnet ID** | **Security Group** |
| Adore | 172.16.193.125 | i-02163d68b88dd568a | subnet-070fd67d2a115c9ce | sg-014960e459ab648e0 |
| BTG VM | 172.16.204.126 | i-08876557175430aa4 | subnet-0ac94039fa7e074a1 | sg-01ae8fd2e9e787355 |
| Accounts | 172.16.207.157 | i-0afbf0e45b1c12acc | subnet-0ac94039fa7e074a1 | sg-0e1d088909a9eb93e |
| Jenkins Prod Server | 172.16.207.184 | i-05262ea2a5ef7ba95 | subnet-0ac94039fa7e074a1 | sg-020052f4345f08e3c |
| rubiscape-pritunl-vpn | 172.16.198.249 | i-092cdbf8b32b92daf | subnet-04a79cae9dbb0cdb7 | sg-0739de8c8562034d9 |
| Datalabs App EKS | 172.16.193.16  172.16.192.112  172.16.192.48 | i-07a850440a9e321e0 | subnet-070fd67d2a115c9ce | sg-00b47e0487df1ad75 |
| Partner App EKS | 172.16.193.35  172.16.192.240  172.16.193.49 | i-0fb81fab70b76fceb | subnet-070fd67d2a115c9ce | sg-00b47e0487df1ad75 |
| Sense App EKS | 172.16.194.80  172.16.194.173 | i-080582ea6122905f9 | subnet-070fd67d2a115c9ce | sg-00b47e0487df1ad75 |
| ZAP | 172.16.207.41 | i-00eb7181ee3bc16fa | subnet-0ac94039fa7e074a1 | sg-09afdda5a09410511 |
| Docker-Backend | 172.16.199.210 | i-0effa097006c7873a | subnet-04a79cae9dbb0cdb7 | sg-0739de8c8562034d9 |
| DataSync | 172.16.199.242 | i-079ddc1b66fa58f69 | subnet-04a79cae9dbb0cdb7 | sg-0f90034f1f2dec37f |
| Monitoring-Nodegroup1 | 172.16.206.12  172.16.204.96  172.16.205.208 | i-01a3f1c14c24c38c5 | subnet-0ac94039fa7e074a1 | sg-00b47e0487df1ad75 |
| Monitoring-Nodegroup2 | 172.16.204.139  172.16.204.19 | i-0b1dd2b174f9f1ca9 | subnet-0ac94039fa7e074a1 | sg-00b47e0487df1ad75 |

## **S3 Bucket:**

Amazon S3 (Simple Storage Service) is an object storage service provided by AWS that allows users to store and retrieve any amount of data at any time. It is designed for scalability, security, durability, and performance, making it ideal for storing backup files, logs, media files, and data lakes.

### **Types of S3 Buckets (Storage Classes):**

1. S3 Standard
2. S3 Intelligent-Tiering
3. S3 Standard-IA (Infrequent Access)
4. S3 One Zone-IA
5. S3 Glacier
6. S3 Glacier Deep Archive

|  |  |
| --- | --- |
| **Bucket Name** | **Bucket Arn** |
| [cf-templates-19mc2jynp9tpm-ap-south-1](https://ap-south-1.console.aws.amazon.com/s3/buckets/cf-templates-19mc2jynp9tpm-ap-south-1?region=ap-south-1) | arn:aws:s3:::cf-templates-19mc2jynp9tpm-ap-south-1 |
| [db-backups-main](https://ap-south-1.console.aws.amazon.com/s3/buckets/db-backups-main?region=ap-south-1&bucketType=general) | arn:aws:s3:::db-backups-main |
| [dummybackup1](https://ap-south-1.console.aws.amazon.com/s3/buckets/dummybackup1?region=ap-south-1&bucketType=general) | arn:aws:s3:::dummybackup1 |
| [rubiscape-builds-prod](https://ap-south-1.console.aws.amazon.com/s3/buckets/rubiscape-builds-prod?region=ap-south-1&bucketType=general) | arn:aws:s3:::rubiscape-builds-prod |
| [rubiscapebackupdata](https://ap-south-1.console.aws.amazon.com/s3/buckets/rubiscapebackupdata?region=ap-south-1&bucketType=general) | arn:aws:s3:::rubiscapebackupdata |
| [rubiscapedevs3bucket](https://ap-south-1.console.aws.amazon.com/s3/buckets/rubiscapedevs3bucket?region=ap-south-1&bucketType=general) | arn:aws:s3:::rubiscapedevs3bucket |
| [sense-prod-bucket](https://ap-south-1.console.aws.amazon.com/s3/buckets/sense-prod-bucket?region=ap-south-1&bucketType=general) | arn:aws:s3:::sense-prod-bucket |

## **Elastic IP:**

An **Elastic IP (EIP)** is a static, public IPv4 address provided by AWS for use in Amazon EC2 instances. Unlike regular public IPs assigned to EC2 instances, Elastic IPs remain constant even if an instance is stopped or restarted.

|  |  |
| --- | --- |
| **EIP Name** | **Public IP** |
| rubiscape-prod-nat1-eip | 3.6.231.45 |
| rubiscape-prod-nat2-eip | 13.203.31.200 |

## 

## **IAM Roles:**

**IAM (Identity and Access Management) Roles** are a way to grant **temporary** permissions to AWS resources without needing to share long-term credentials (such as access keys). Unlike IAM users, IAM roles are **not associated with a specific user** but can be assumed by AWS services, applications, or other AWS accounts.

Below table suggests IAM role created for account to be used by all the instances:

|  |  |  |
| --- | --- | --- |
| **Role Name** | **Policies attached** | **ARN** |
| [alertmanager\_role](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles/details/alertmanager_role) | [SNSPublishPolicy](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles/details/alertmanager_role/editPolicy/SNSPublishPolicy?step=addPermissions) | arn:aws:iam::155727836473:role/alertmanager\_role |
| [Amazon\_EventBridge\_Scheduler\_LAMBDA](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles/details/Amazon_EventBridge_Scheduler_LAMBDA) | [Amazon-EventBridge-Scheduler-Execution-Policy-c171a518-415a-47ac-bec7-8f317713c17d](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3A155727836473%3Apolicy%2Fservice-role%2FAmazon-EventBridge-Scheduler-Execution-Policy-c171a518-415a-47ac-bec7-8f317713c17d) | arn:aws:iam::155727836473:role/service-role/Amazon\_EventBridge\_Scheduler\_LAMBDA |
| [Amazon\_EventBridge\_Scheduler\_LAMBDA\_start](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles/details/Amazon_EventBridge_Scheduler_LAMBDA_start) | [Amazon-EventBridge-Scheduler-Execution-Policy-357d9e8c-03f9-49b2-ada5-7359a45cef3f](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3A155727836473%3Apolicy%2Fservice-role%2FAmazon-EventBridge-Scheduler-Execution-Policy-357d9e8c-03f9-49b2-ada5-7359a45cef3f) | arn:aws:iam::155727836473:role/service-role/Amazon\_EventBridge\_Scheduler\_LAMBDA\_start |
| [AmazonEKS\_EFS\_CSI\_DriverRole](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles/details/AmazonEKS_EFS_CSI_DriverRole) | Trusted Entity | arn:aws:iam::155727836473:role/AmazonEKS\_EFS\_CSI\_DriverRole |
| [AmazonEKSLoadBalancerControllerRole](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles/details/AmazonEKSLoadBalancerControllerRole) | [AWSLoadBalancerControllerIAMPolicy](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3A155727836473%3Apolicy%2FAWSLoadBalancerControllerIAMPolicy)  [listener](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles/details/AmazonEKSLoadBalancerControllerRole/editPolicy/listener?step=addPermissions) | arn:aws:iam::155727836473:role/AmazonEKSLoadBalancerControllerRole |
| [AWS-QuickSetup-StackSet-Local-AdministrationRole](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles/details/AWS-QuickSetup-StackSet-Local-AdministrationRole) | [AssumeRole-AWS-QuickSetup-StackSet-Local-ExecutionRole](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles/details/AWS-QuickSetup-StackSet-Local-AdministrationRole/editPolicy/AssumeRole-AWS-QuickSetup-StackSet-Local-ExecutionRole?step=addPermissions) | arn:aws:iam::155727836473:role/AWS-QuickSetup-StackSet-Local-AdministrationRole |
| [AWS-QuickSetup-StackSet-Local-ExecutionRole](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles/details/AWS-QuickSetup-StackSet-Local-ExecutionRole) | [AdministratorAccess](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2FAdministratorAccess) | arn:aws:iam::155727836473:role/AWS-QuickSetup-StackSet-Local-ExecutionRole |
| [AWSBackupDefaultServiceRole](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles/details/AWSBackupDefaultServiceRole) | [AWSBackupServiceRolePolicyForBackup](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2Fservice-role%2FAWSBackupServiceRolePolicyForBackup)  [AWSBackupServiceRolePolicyForRestores](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2Fservice-role%2FAWSBackupServiceRolePolicyForRestores) | arn:aws:iam::155727836473:role/service-role/AWSBackupDefaultServiceRole |
| [AWSDataSyncS3BucketAccess-sense-prod-bucket-f83dd](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles/details/AWSDataSyncS3BucketAccess-sense-prod-bucket-f83dd) | [AWSDataSyncS3BucketAccess-sense-prod-bucket-f83dd](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3A155727836473%3Apolicy%2Fservice-role%2FAWSDataSyncS3BucketAccess-sense-prod-bucket-f83dd) | arn:aws:iam::155727836473:role/service-role/AWSDataSyncS3BucketAccess-sense-prod-bucket-f83dd |
| [AWSDataSyncS3BucketAccess-sensedata1-d165b](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles/details/AWSDataSyncS3BucketAccess-sensedata1-d165b) | [AWSDataSyncS3BucketAccess-sensedata1-d165b](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3A155727836473%3Apolicy%2Fservice-role%2FAWSDataSyncS3BucketAccess-sensedata1-d165b) | arn:aws:iam::155727836473:role/service-role/AWSDataSyncS3BucketAccess-sensedata1-d165b |
| [AWSDataSyncTaskReportS3BucketAccess-dummybackup1-ap-south--df9e6](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles/details/AWSDataSyncTaskReportS3BucketAccess-dummybackup1-ap-south--df9e6) | [AWSDataSyncTaskReportS3BucketAccess-dummybackup1-ap-south--df9e6](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3A155727836473%3Apolicy%2Fservice-role%2FAWSDataSyncTaskReportS3BucketAccess-dummybackup1-ap-south--df9e6) | arn:aws:iam::155727836473:role/service-role/AWSDataSyncTaskReportS3BucketAccess-dummybackup1-ap-south--df9e6 |
| [AWSGlueServiceRole-athenasetup](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles/details/AWSGlueServiceRole-athenasetup) | [AWSGlueServiceRole](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2Fservice-role%2FAWSGlueServiceRole)  [AWSGlueServiceRole-athenasetup-EZCRC-s3Policy](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3A155727836473%3Apolicy%2Fservice-role%2FAWSGlueServiceRole-athenasetup-EZCRC-s3Policy) | arn:aws:iam::155727836473:role/service-role/AWSGlueServiceRole-athenasetup |
| [AWSServiceRoleForAmazonEKS](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles/details/AWSServiceRoleForAmazonEKS) | [AmazonEKSServiceRolePolicy](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2Faws-service-role%2FAmazonEKSServiceRolePolicy) | [AmazonEKSServiceRolePolicy](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2Faws-service-role%2FAmazonEKSServiceRolePolicy) |
| [AWSServiceRoleForAmazonEKSNodegroup](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles/details/AWSServiceRoleForAmazonEKSNodegroup) | [AWSServiceRoleForAmazonEKSNodegroup](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2Faws-service-role%2FAWSServiceRoleForAmazonEKSNodegroup) | arn:aws:iam::155727836473:role/aws-service-role/eks-nodegroup.amazonaws.com/AWSServiceRoleForAmazonEKSNodegroup |
| [AWSServiceRoleForAmazonElasticFileSystem](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles/details/AWSServiceRoleForAmazonElasticFileSystem) | [AmazonElasticFileSystemServiceRolePolicy](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2Faws-service-role%2FAmazonElasticFileSystemServiceRolePolicy) | arn:aws:iam::155727836473:role/aws-service-role/elasticfilesystem.amazonaws.com/AWSServiceRoleForAmazonElasticFileSystem |
| [AWSServiceRoleForAutoScaling](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles/details/AWSServiceRoleForAutoScaling) | [AutoScalingServiceRolePolicy](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2Faws-service-role%2FAutoScalingServiceRolePolicy) | arn:aws:iam::155727836473:role/aws-service-role/autoscaling.amazonaws.com/AWSServiceRoleForAutoScaling |
| [AWSServiceRoleForBackup](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles/details/AWSServiceRoleForBackup) | [AWSBackupServiceLinkedRolePolicyForBackup](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2Faws-service-role%2FAWSBackupServiceLinkedRolePolicyForBackup) | arn:aws:iam::155727836473:role/aws-service-role/backup.amazonaws.com/AWSServiceRoleForBackup |
| [AWSServiceRoleForElasticLoadBalancing](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles/details/AWSServiceRoleForElasticLoadBalancing) | [AWSElasticLoadBalancingServiceRolePolicy](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2Faws-service-role%2FAWSElasticLoadBalancingServiceRolePolicy) | arn:aws:iam::155727836473:role/aws-service-role/elasticloadbalancing.amazonaws.com/AWSServiceRoleForElasticLoadBalancing |
| [AWSServiceRoleForGlobalAccelerator](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles/details/AWSServiceRoleForGlobalAccelerator) | [AWSGlobalAcceleratorSLRPolicy](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2Faws-service-role%2FAWSGlobalAcceleratorSLRPolicy) | arn:aws:iam::155727836473:role/aws-service-role/globalaccelerator.amazonaws.com/AWSServiceRoleForGlobalAccelerator |
| [AWSServiceRoleForOrganizations](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles/details/AWSServiceRoleForOrganizations) | [AWSOrganizationsServiceTrustPolicy](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2Faws-service-role%2FAWSOrganizationsServiceTrustPolicy) | arn:aws:iam::155727836473:role/aws-service-role/organizations.amazonaws.com/AWSServiceRoleForOrganizations |
| [AWSServiceRoleForSupport](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles/details/AWSServiceRoleForSupport) | [AWSSupportServiceRolePolicy](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2Faws-service-role%2FAWSSupportServiceRolePolicy) | arn:aws:iam::155727836473:role/aws-service-role/support.amazonaws.com/AWSServiceRoleForSupport |
| [AWSServiceRoleForTrustedAdvisor](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles/details/AWSServiceRoleForTrustedAdvisor) | [AWSTrustedAdvisorServiceRolePolicy](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2Faws-service-role%2FAWSTrustedAdvisorServiceRolePolicy) | arn:aws:iam::155727836473:role/aws-service-role/trustedadvisor.amazonaws.com/AWSServiceRoleForTrustedAdvisor |
| [datalabs-postgres-backup-role](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles/details/datalabs-postgres-backup-role) | [datalabs-postgres-backup-policy](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3A155727836473%3Apolicy%2Fdatalabs-postgres-backup-policy) | arn:aws:iam::155727836473:role/datalabs-postgres-backup-role |
| [DockerStatus-sns-function-role-oflr30u0](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles/details/DockerStatus-sns-function-role-oflr30u0) | [AWSLambdaBasicExecutionRole-806fd1ce-ffbf-43c7-8bf1-ca0f969c9f78](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3A155727836473%3Apolicy%2Fservice-role%2FAWSLambdaBasicExecutionRole-806fd1ce-ffbf-43c7-8bf1-ca0f969c9f78) | arn:aws:iam::155727836473:role/service-role/DockerStatus-sns-function-role-oflr30u0 |
| [DockerStatus-sns-Lambda-role-kn8ucpzn](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles/details/DockerStatus-sns-Lambda-role-kn8ucpzn) | [AmazonSNSFullAccess](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2FAmazonSNSFullAccess)  [AmazonSSMFullAccess](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2FAmazonSSMFullAccess)  [AWSLambdaBasicExecutionRole](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2Fservice-role%2FAWSLambdaBasicExecutionRole)  [AWSLambdaBasicExecutionRole-65d8438f-edd3-4832-a36c-3b75e0fcb8b8](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3A155727836473%3Apolicy%2Fservice-role%2FAWSLambdaBasicExecutionRole-65d8438f-edd3-4832-a36c-3b75e0fcb8b8)  [CloudWatchAgentAdminPolicy](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2FCloudWatchAgentAdminPolicy)  [CloudWatchAgentServerPolicy](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2FCloudWatchAgentServerPolicy)  [CloudWatchFullAccessV2](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2FCloudWatchFullAccessV2)  [CloudWatchLogsFullAccess](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2FCloudWatchLogsFullAccess) | arn:aws:iam::155727836473:role/service-role/DockerStatus-sns-Lambda-role-kn8ucpzn |
| [eksctl-rubiscape-prod-cluster-addon-iamservic-Role1-mm7r6oaJHi3Z](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles/details/eksctl-rubiscape-prod-cluster-addon-iamservic-Role1-mm7r6oaJHi3Z) | [AmazonEBSCSIDriverPolicy](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2Fservice-role%2FAmazonEBSCSIDriverPolicy) | arn:aws:iam::155727836473:role/eksctl-rubiscape-prod-cluster-addon-iamservic-Role1-mm7r6oaJHi3Z |
| [InstanceState-sns-Lambda-role-04n6i7bg](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles/details/InstanceState-sns-Lambda-role-04n6i7bg) | [AmazonSNSFullAccess](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2FAmazonSNSFullAccess)  [AmazonSSMFullAccess](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2FAmazonSSMFullAccess)  [AWSLambdaBasicExecutionRole-8af21ccf-48d4-46d5-b3b9-7598a09b16ac](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3A155727836473%3Apolicy%2Fservice-role%2FAWSLambdaBasicExecutionRole-8af21ccf-48d4-46d5-b3b9-7598a09b16ac)  [CloudWatchFullAccessV2](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2FCloudWatchFullAccessV2)  [CloudWatchFullAccess](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2FCloudWatchFullAccess) | arn:aws:iam::155727836473:role/service-role/InstanceState-sns-Lambda-role-04n6i7bg |
| [Jenkins-role](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles/details/Jenkins-role) | [AdministratorAccess](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2FAdministratorAccess) | arn:aws:iam::155727836473:role/Jenkins-role |
| [KarpenterControllerRole-rubiscape-prod-cluster](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles/details/KarpenterControllerRole-rubiscape-prod-cluster) | [KarpenterControllerPolicy-rubiscape-prod-cluster](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles/details/KarpenterControllerRole-rubiscape-prod-cluster/editPolicy/KarpenterControllerPolicy-rubiscape-prod-cluster?step=addPermissions) | arn:aws:iam::155727836473:role/KarpenterControllerRole-rubiscape-prod-cluster |
| [KarpenterNodeRole-rubiscape-prod-cluster](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles/details/KarpenterNodeRole-rubiscape-prod-cluster) | [AmazonEC2ContainerRegistryReadOnly](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2FAmazonEC2ContainerRegistryReadOnly)  [AmazonEKS\_CNI\_Policy](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2FAmazonEKS_CNI_Policy)  [AmazonEKSWorkerNodePolicy](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2FAmazonEKSWorkerNodePolicy)  [AmazonSSMManagedInstanceCore](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2FAmazonSSMManagedInstanceCore) | arn:aws:iam::155727836473:role/KarpenterNodeRole-rubiscape-prod-cluster |
| [Lambda](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles/details/Lambda) | [AmazonEC2FullAccess](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2FAmazonEC2FullAccess)  [AmazonEC2ReadOnlyAccess](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2FAmazonEC2ReadOnlyAccess)  [ec\_start\_stop](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3A155727836473%3Apolicy%2Fec_start_stop) | arn:aws:iam::155727836473:role/Lambda |
| [Lambda-full](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles/details/Lambda-full) | [AmazonEC2FullAccess](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2FAmazonEC2FullAccess)  [ec\_start\_stop](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3A155727836473%3Apolicy%2Fec_start_stop) | arn:aws:iam::155727836473:role/Lambda-full |
| [partner-postgres-backup-role](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles/details/partner-postgres-backup-role) | [partner-postgres-backup-policy](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3A155727836473%3Apolicy%2Fpartner-postgres-backup-policy) | arn:aws:iam::155727836473:role/partner-postgres-backup-role |
| [Rubiscape-Prod-Cloudwatch-MonitoringInstanceProfile](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles/details/Rubiscape-Prod-Cloudwatch-MonitoringInstanceProfile) | [AdministratorAccess](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2FAdministratorAccess)  [AmazonSNSFullAccess](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2FAmazonSNSFullAccess)  [AmazonSSMFullAccess](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2FAmazonSSMFullAccess)  [AWSLambda\_FullAccess](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2FAWSLambda_FullAccess)  [AWSLambdaBasicExecutionRole-65d8438f-edd3-4832-a36c-3b75e0fcb8b8](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3A155727836473%3Apolicy%2Fservice-role%2FAWSLambdaBasicExecutionRole-65d8438f-edd3-4832-a36c-3b75e0fcb8b8)  [AWSLambdaBasicExecutionRole-8af21ccf-48d4-46d5-b3b9-7598a09b16ac](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3A155727836473%3Apolicy%2Fservice-role%2FAWSLambdaBasicExecutionRole-8af21ccf-48d4-46d5-b3b9-7598a09b16ac)  [CloudWatchAgentServerPolicy](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2FCloudWatchAgentServerPolicy)  [CloudWatchFullAccessV2](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2FCloudWatchFullAccessV2)  [CloudWatchLogsFullAccess](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2FCloudWatchLogsFullAccess) | arn:aws:iam::155727836473:role/Rubiscape-Prod-Cloudwatch-MonitoringInstanceProfile |
| [rubiscape-prod-mumbai-cf-EKSClusterRole-4rWkg8MsWDb3](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles/details/rubiscape-prod-mumbai-cf-EKSClusterRole-4rWkg8MsWDb3) | [AmazonEFSCSIDriverPolicy](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2Fservice-role%2FAmazonEFSCSIDriverPolicy)  [AmazonEKSClusterPolicy](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2FAmazonEKSClusterPolicy) | arn:aws:iam::155727836473:role/rubiscape-prod-mumbai-cf-EKSClusterRole-4rWkg8MsWDb3 |
| [rubiscape-prod-mumbai-cf-NodeInstanceRole-YDVbq6V0vhBp](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles/details/rubiscape-prod-mumbai-cf-NodeInstanceRole-YDVbq6V0vhBp) | [AdministratorAccess](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2FAdministratorAccess)  [AmazonEC2ContainerRegistryPullOnly](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2FAmazonEC2ContainerRegistryPullOnly)  [AmazonEC2ContainerRegistryReadOnly](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2FAmazonEC2ContainerRegistryReadOnly)  [AmazonEFSCSIDriverPolicy](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2Fservice-role%2FAmazonEFSCSIDriverPolicy)  [AmazonEKS\_CNI\_Policy](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2FAmazonEKS_CNI_Policy)  [AmazonEKSWorkerNodePolicy](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2FAmazonEKSWorkerNodePolicy)  [AmazonSNSFullAccess](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2FAmazonSNSFullAccess)  [Assume\_alertmanager\_role\_policy](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles/details/rubiscape-prod-mumbai-cf-NodeInstanceRole-YDVbq6V0vhBp/editPolicy/assume_alertmanager_role_policy?step=addPermissions)  [assuming\_alertmanager\_role\_policy](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles/details/rubiscape-prod-mumbai-cf-NodeInstanceRole-YDVbq6V0vhBp/editPolicy/assuming_alertmanager_role_policy?step=addPermissions) | arn:aws:iam::155727836473:role/rubiscape-prod-mumbai-cf-NodeInstanceRole-YDVbq6V0vhBp |
| [sense-postgres-backup-role](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles/details/sense-postgres-backup-role) | [sense-postgres-backup-policy](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3A155727836473%3Apolicy%2Fsense-postgres-backup-policy) | arn:aws:iam::155727836473:role/sense-postgres-backup-role |
| [ssm\_cwagent](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles/details/ssm_cwagent) | [AmazonEC2FullAccess](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2FAmazonEC2FullAccess)  [AmazonSSMFullAccess](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2FAmazonSSMFullAccess)  [AmazonSSMManagedInstanceCore](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2FAmazonSSMManagedInstanceCore)  [CloudWatchAgentAdminPolicy](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2FCloudWatchAgentAdminPolicy)  [CloudWatchAgentServerPolicy](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2FCloudWatchAgentServerPolicy)  [CloudWatchFullAccessV2](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2FCloudWatchFullAccessV2) | arn:aws:iam::155727836473:role/ssm\_cwagent |
| [test-role](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/roles/details/test-role) | [AdministratorAccess](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2FAdministratorAccess)  [AmazonEC2ContainerRegistryFullAccess](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2FAmazonEC2ContainerRegistryFullAccess)  [AmazonEKSClusterPolicy](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2FAmazonEKSClusterPolicy)  [AmazonEKSServicePolicy](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2FAmazonEKSServicePolicy) | arn:aws:iam::155727836473:role/test-role |

## 

## **CUSTOMER MANAGED POLICIES FOR THE ROLE:**

|  |  |  |
| --- | --- | --- |
| **Policy Name** | **Permissions** | **ARN** |
| [Amazon-EventBridge-Scheduler-Execution-Policy-357d9e8c-03f9-49b2-ada5-7359a45cef3f](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3A155727836473%3Apolicy%2Fservice-role%2FAmazon-EventBridge-Scheduler-Execution-Policy-357d9e8c-03f9-49b2-ada5-7359a45cef3f) | Lambda -  Limited: Write | arn:aws:iam::155727836473:policy/service-role/Amazon-EventBridge-Scheduler-Execution-Policy-357d9e8c-03f9-49b2-ada5-7359a45cef3f |
| [Amazon-EventBridge-Scheduler-Execution-Policy-c171a518-415a-47ac-bec7-8f317713c17d](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3A155727836473%3Apolicy%2Fservice-role%2FAmazon-EventBridge-Scheduler-Execution-Policy-c171a518-415a-47ac-bec7-8f317713c17d) | Lambda -  Limited: Write | arn:aws:iam::155727836473:policy/service-role/Amazon-EventBridge-Scheduler-Execution-Policy-c171a518-415a-47ac-bec7-8f317713c17d |
| [AmazonEKS\_EFS\_CSI\_Driver\_Policy](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3A155727836473%3Apolicy%2FAmazonEKS_EFS_CSI_Driver_Policy) | EC2 - Limited: List  EFS - Limited: List, Read, Write, Tagging | arn:aws:iam::155727836473:policy/AmazonEKS\_EFS\_CSI\_Driver\_Policy |
| [AthenaGlueAccessPolicy](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3A155727836473%3Apolicy%2FAthenaGlueAccessPolicy) | Athena - Full Access  Glue - Full Access  S3 - Limited: List, Read, Write | arn:aws:iam::155727836473:policy/AthenaGlueAccessPolicy |
| [AWSDataSyncS3BucketAccess-sense-prod-bucket-f83dd](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3A155727836473%3Apolicy%2Fservice-role%2FAWSDataSyncS3BucketAccess-sense-prod-bucket-f83dd) | S3 - Limited: List, Read, Write, Tagging | arn:aws:iam::155727836473:policy/service-role/AWSDataSyncS3BucketAccess-sense-prod-bucket-f83dd |
| [AWSDataSyncS3BucketAccess-sensedata1-d165b](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3A155727836473%3Apolicy%2Fservice-role%2FAWSDataSyncS3BucketAccess-sensedata1-d165b) | S3 - Limited: List, Read, Write, Tagging | arn:aws:iam::155727836473:policy/service-role/AWSDataSyncS3BucketAccess-sensedata1-d165b |
| [AWSDataSyncTaskReportS3BucketAccess-dummybackup1-ap-south--df9e6](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3A155727836473%3Apolicy%2Fservice-role%2FAWSDataSyncTaskReportS3BucketAccess-dummybackup1-ap-south--df9e6) | S3 - Limited: Write | arn:aws:iam::155727836473:policy/service-role/AWSDataSyncTaskReportS3BucketAccess-dummybackup1-ap-south--df9e6 |
| [AWSGlueServiceRole-athenasetup-EZCRC-s3Policy](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3A155727836473%3Apolicy%2Fservice-role%2FAWSGlueServiceRole-athenasetup-EZCRC-s3Policy) | S3 - Limited: Read, Write | arn:aws:iam::155727836473:policy/service-role/AWSGlueServiceRole-athenasetup-EZCRC-s3Policy |
| [AWSLambdaBasicExecutionRole-65d8438f-edd3-4832-a36c-3b75e0fcb8b8](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3A155727836473%3Apolicy%2Fservice-role%2FAWSLambdaBasicExecutionRole-65d8438f-edd3-4832-a36c-3b75e0fcb8b8) | Cloudwatch Logs - Limited: Write | arn:aws:iam::155727836473:policy/service-role/AWSLambdaBasicExecutionRole-65d8438f-edd3-4832-a36c-3b75e0fcb8b8 |
| [AWSLambdaBasicExecutionRole-806fd1ce-ffbf-43c7-8bf1-ca0f969c9f78](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3A155727836473%3Apolicy%2Fservice-role%2FAWSLambdaBasicExecutionRole-806fd1ce-ffbf-43c7-8bf1-ca0f969c9f78) | Cloudwatch Logs - Limited: Write | arn:aws:iam::155727836473:policy/service-role/AWSLambdaBasicExecutionRole-806fd1ce-ffbf-43c7-8bf1-ca0f969c9f78 |
| [AWSLambdaBasicExecutionRole-8af21ccf-48d4-46d5-b3b9-7598a09b16ac](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3A155727836473%3Apolicy%2Fservice-role%2FAWSLambdaBasicExecutionRole-8af21ccf-48d4-46d5-b3b9-7598a09b16ac) | Cloudwatch Logs - Limited: Write | arn:aws:iam::155727836473:policy/service-role/AWSLambdaBasicExecutionRole-8af21ccf-48d4-46d5-b3b9-7598a09b16ac |
| [AWSLoadBalancerControllerIAMPolicy](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3A155727836473%3Apolicy%2FAWSLoadBalancerControllerIAMPolicy) | Certificate Manager - Full: List Limited: Read  Cognito User Pools - Limited: Read  EC2 - Full: Tagging Limited: List, Read, Write  Elb - Full: List, Tagging Limited: Read, Write  ELB v2 - Full: Tagging Limited: Read, Write  IAM - Limited: List, Read, Write  Shield - Limited: Read, Write  WAF Regional - Limited: Read, Write  WAF v2 - Limited: Read, Write | arn:aws:iam::155727836473:policy/AWSLoadBalancerControllerIAMPolicy |
| [CloudShellAccessPolicy](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3A155727836473%3Apolicy%2FCloudShellAccessPolicy) | CloudShell - Limited: Read, Write | arn:aws:iam::155727836473:policy/CloudShellAccessPolicy |
| [datalabs-postgres-backup-policy](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3A155727836473%3Apolicy%2Fdatalabs-postgres-backup-policy) | S3 - Limited: List, Read, Write | arn:aws:iam::155727836473:policy/datalabs-postgres-backup-policy |
| [ec\_start\_stop](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3A155727836473%3Apolicy%2Fec_start_stop) | Cloudwatch Logs - Limited: Write  Ec2 - Limited: Read, Write | arn:aws:iam::155727836473:policy/ec\_start\_stop |
| [eks\_full\_access](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3A155727836473%3Apolicy%2Feks_full_access) | EKS - Full access | arn:aws:iam::155727836473:policy/eks\_full\_access |
| [partner-postgres-backup-policy](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3A155727836473%3Apolicy%2Fpartner-postgres-backup-policy) | S3 - Limited: List, Read, Write | arn:aws:iam::155727836473:policy/partner-postgres-backup-policy |
| [sense-postgres-backup-policy](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-south-1#/policies/details/arn%3Aaws%3Aiam%3A%3A155727836473%3Apolicy%2Fsense-postgres-backup-policy) | Limited: List, Read, Write | arn:aws:iam::155727836473:policy/sense-postgres-backup-policy |

## 

## **KMS:**

AWS **Key Management Service (KMS)** is a managed service that allows you to create, manage, and control encryption keys used to secure your data across AWS services and applications. It simplifies key management while ensuring strong security and compliance.

These are the encryption keys used to encrypt EBS Volumes of EC2 Servers and RDS Instance.

|  |  |  |
| --- | --- | --- |
| **Key Name** | **Description** | **ARN** |
| aws/s3 | Default key that protects my S3 objects when no other key is defined | arn:aws:kms:ap-south-1:155727836473:key/28d43b86-da3e-479e-ad16-a43b35126439 |
| aws/redshift | Default key that protects my Redshift clusters when no other key is defined | arn:aws:kms:ap-south-1:155727836473:key/294329b9-bf03-4e3c-b7ef-ff28b46dd38f |
| aws/sns | Default key that protects my SNS data when no other key is defined | arn:aws:kms:ap-south-1:155727836473:key/2a284195-e399-43c2-a395-49bd5281d352 |
| aws/dynamodb | Default key that protects my DynamoDB data when no other key is defined | arn:aws:kms:ap-south-1:155727836473:key/34c6c557-d780-4d91-a98b-694683582d50 |
| aws/ecr | Default key that protects my ECR data when no other key is defined | arn:aws:kms:ap-south-1:155727836473:key/4f70751b-635e-4ce2-9284-e37d8a3715d1 |
| aws/backup | Default key that protects my Backup data when no other key is defined | arn:aws:kms:ap-south-1:155727836473:key/a4306d28-64f5-47bd-9f95-1495b2deea87 |
| aws/ebs | Default master key that protects my EBS volumes when no other key is defined | arn:aws:kms:ap-south-1:155727836473:key/b5c7a67c-7309-41a5-bdbf-e069b45944c3 |
| aws/lightsail | Default master key that protects my Lightsail signing keys when no other key is defined | arn:aws:kms:ap-south-1:155727836473:key/c5a438a5-140d-49ec-ae97-29f44fa59f29 |
| aws/acm | Default key that protects my ACM private keys when no other key is defined | arn:aws:kms:ap-south-1:155727836473:key/defa2e45-131f-482c-8888-fa03e8cd24be |
| aws/elasticfilesystem | Default key that protects my EFS filesystems when no other key is defined | arn:aws:kms:ap-south-1:155727836473:key/e724c1d1-dffd-43b1-90de-3a0c3f181f8d |
| rubiscape-prod-ebs-keys | rubiscape-prod-ebs-vol-encryption-key | arn:aws:kms:ap-south-1:155727836473:key/71486276-a41b-4bc5-a9e4-538fe178568a |

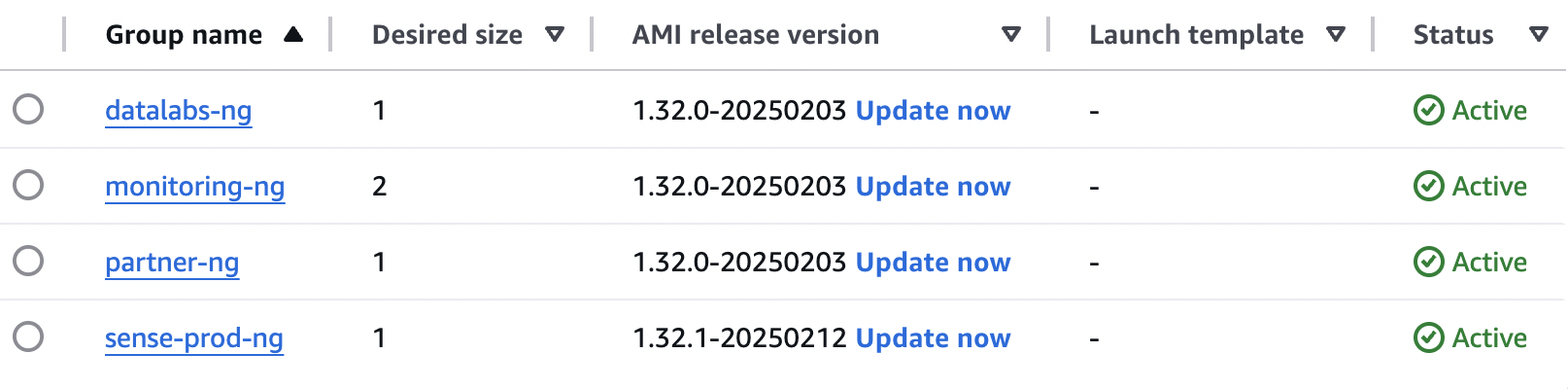
**EKS Cluster:**

Amazon Elastic Kubernetes Service (Amazon EKS) is a managed service that makes it easy for you to run Kubernetes on AWS without needing to stand up or maintain your own Kubernetes control plane. Kubernetes is an open-source system for automating the deployment, scaling, and management of containerized applications.

Applications running on Amazon EKS are fully compatible with applications running on any standard Kubernetes environment, whether running in on-premises data centers or public clouds.

|  |  |  |
| --- | --- | --- |
| **Cluster Name** | **Kubernetes version** | **Cluster ARN** |
| rubiscape-prod-cluster | 1.32 | arn:aws:eks:ap-south-1:155727836473:cluster/rubiscape-prod-cluster |

**Node Groups:**

****

**EKS Deployment steps:**

1. **Ensure you are connected to your EKS cluster:**

aws eks update-kubeconfig --region <your-region> --name <your-cluster-name>

1. **Apply a specific deployment file:**

kubectl apply -f <deployment-file>.yaml

**[or]**

**Apply with a namespace:**

kubectl apply -f <deployment-file>.yaml -n <namespace>

1. **Check if pods are running:**

kubectl get pods

**[or]**

**Describe a deployment for more details:**

kubectl describe deploy <deployment-name>

1. **View logs of a specific pod:**

kubectl logs <pod-name>

1. **Check if services are running:**

kubectl get svc

**Apply an Ingress configuration (if applicable):**

kubectl apply -f ingress.yaml

1. **Monitor pod status:**

watch kubectl get pods

**Kubectl basic commands:**

**Namespace Management:**

kubectl get ns # List all namespaces

kubectl create ns <namespace> # Create a new namespace

kubectl delete ns <namespace> # Delete a namespace

**Pod Management:**

kubectl get po # List all pods in the default namespace

kubectl get po -n <namespace> # List pods in a specific namespace

kubectl get po -o wide # List pods with more details (Node, IP, etc.)

kubectl get po --all-namespaces # List pods across all namespaces

kubectl describe po <pod-name> # Show detailed information about a pod

kubectl logs <pod-name> # Fetch logs from a pod

kubectl logs -f <pod-name> # Stream pod logs in real-time

kubectl logs <pod-name> -c <container> # Get logs from a specific container in a pod

kubectl delete po <pod-name> # Delete a pod

kubectl exec -it <pod-name> -- sh # Access a pod’s shell (for Alpine-based images)

kubectl exec -it <pod-name> -- bash # Access a pod’s shell (for Ubuntu-based images)

**Deployment Management:**

kubectl get deploy # List deployments

kubectl get deploy -n <namespace> # List deployments in a specific namespace

kubectl describe deploy <deploy-name> # Get details of a deployment

kubectl rollout status deploy <deploy-name> # Check rollout status

kubectl rollout restart deploy <deploy-name> # Restart a deployment

kubectl scale deploy <deploy-name> --replicas=3 # Scale deployment replicas

kubectl delete deploy <deploy-name> # Delete a deployment

**Service Management:**

kubectl get svc # List services

kubectl get svc -n <namespace> # List services in a namespace

kubectl describe svc <svc-name> # Get details of a service

kubectl delete svc <svc-name> # Delete a service

**Ingress & Networking:**

kubectl get ingress # List all ingress resources

kubectl describe ingress <ingress-name># Get details of an ingress

kubectl get nodes # List cluster nodes

kubectl get endpoints # Show endpoints of services

kubectl get networkpolicy # List all network policies

**Persistent Volume (PV) & Persistent Volume Claim (PVC):**

kubectl get pv # List persistent volumes

kubectl get pvc # List persistent volume claims

kubectl describe pv <pv-name> # Get details of a persistent volume

kubectl describe pvc <pvc-name> # Get details of a persistent volume claim

kubectl delete pvc <pvc-name> # Delete a PVC

**Resource Usage & Monitoring:**

kubectl top nodes # View CPU and memory usage of nodes

kubectl top pods # View CPU and memory usage of pods

kubectl get events # Show recent cluster events

**Apply & Patch Configuration:**

kubectl apply -f <file.yaml> # Deploy resources from a YAML file

kubectl delete -f <file.yaml> # Delete resources defined in a YAML file

kubectl patch deploy <deploy-name> -p '{"spec": {"replicas": 3}}' # Patch a deployment

**Watch for Real-time Changes:**

watch kubectl get po # Continuously watch pod status

watch kubectl get nodes # Continuously watch node status

watch kubectl get deploy # Watch deployment updates

**Debugging & Troubleshooting:**

kubectl get events --sort-by=.metadata.creationTimestamp # Show events sorted by time

kubectl describe po <pod-name> # Detailed pod information

kubectl get rs # Check ReplicaSets

kubectl get ds # Check DaemonSets

kubectl get all # Get all resources in a namespace

kubectl logs <pod-name> # View pod logs

kubectl exec -it <pod-name> -- sh # Access pod shell

## **Understanding our Manifests files**

**Persistent Volume deployment**

**#Create PV**

apiVersion: v1

kind: PersistentVolume

metadata:

name: partner-pv

spec:

capacity:

storage: 5Gi

volumeMode: Filesystem

accessModes:

- ReadWriteMany

persistentVolumeReclaimPolicy: Retain

storageClassName: efs-sc

csi:

driver: efs.csi.aws.com

volumeHandle: fs-01e04ed2b6a62cdc2 **# Replace with your EFS File System ID**



This code is creating a Persistent Volume (PV) in a Kubernetes environment. Think of a Persistent Volume as a shared storage space that different applications can use to store and access data, even if they restart or move around.

Here's what each part does in simple terms:

* apiVersion: v1 & kind: PersistentVolume → This tells Kubernetes that we're creating a storage unit that will be shared across applications.
* metadata: name: partner-pv → Names the storage unit as "partner-pv" so it can be referenced later.
* spec: → Defines the storage details:  
  + capacity: storage: 5Gi → This storage unit has 5 gigabytes of space.
  + volumeMode: Filesystem → The storage works like a regular file system (like a folder on your computer).
  + accessModes: ReadWriteMany → Multiple applications can read and write to this storage at the same time.
  + persistentVolumeReclaimPolicy: Retain → Even if the application using this storage is deleted, the data remains.
  + storageClassName: efs-sc → Specifies a storage class to manage this volume (in this case, AWS EFS).
  + csi: → Defines AWS EFS (Elastic File System) as the backend storage provider:  
    - driver: efs.csi.aws.com → Uses Amazon's EFS storage system.
    - volumeHandle: fs-01e04ed2b6a62cdc2 → This is a unique ID that points to a specific AWS EFS storage system.

**Persistent Volume Claim deployment**

#Create PVC

apiVersion: v1

kind: PersistentVolumeClaim

metadata:

name: partner-pvc

spec:

accessModes:

- ReadWriteMany

volumeMode: Filesystem

storageClassName: efs-sc

resources:

requests:

storage: 5Gi



* apiVersion: v1 & kind: PersistentVolumeClaim → This tells Kubernetes that we're requesting storage from an existing Persistent Volume (PV).
* metadata: name: partner-pvc → Names the storage request as "partner-pvc", so applications can refer to it.
* spec: → Defines the storage request details:
* accessModes: ReadWriteMany → The storage can be used by multiple applications at the same time.
* volumeMode: Filesystem → The storage behaves like a regular file system (like a folder on a computer).
* storageClassName: efs-sc → Requests storage from a storage class named "efs-sc", which is linked to AWS EFS.
* resources:  
  + requests: storage: 5Gi → Requests 5GB of storage from an available Persistent Volume (PV).

**Deployment file**

#Create Deployment

apiVersion: apps/v1

kind: Deployment

metadata:

name: partner-backend

spec:

replicas: 1

selector:

matchLabels:

app: partner-backend

template:

metadata:

labels:

app: partner-backend

spec:

containers:

- name: partner-backend

image: 155727836473.dkr.ecr.ap-south-1.amazonaws.com/rubiscape-prod-ecr-image-repo:backendnew

ports:

- containerPort: 8085

env:

- name: JAVA\_OPTS

value: '-Xms512m -Xmx1g'

volumeMounts:

- name: partner-pv-storage

mountPath: "/home/ubuntu/Rubics" # Path inside the container where you want the volume mounted

subPath: "Rubics"

- name: partner-pv-storage

mountPath: "/home/ubuntu/Storage\_Rubiscape"

subPath: "Storage\_Rubiscape"

volumes:

- name: partner-pv-storage

persistentVolumeClaim:

claimName: partner-pvc # The PVC name that you created for EFS or your desired PV

nodeSelector: # Added node selector

application: partner

**Key Parts of the Deployment:**

**replicas: 1**

* Only one instance of this application will run.

**Container Setup (containers:)**

* Runs a container named partner-backend.
* Uses a Docker image from AWS ECR (rubiscape-prod-ecr-image-repo:backendnew).
* Exposes port 8085 for communication.
* Environment variable (JAVA\_OPTS) is set to manage Java memory (512MB min, 1GB max).

**Storage (volumeMounts: & volumes:)**

* Mounts a Persistent Volume (partner-pv-storage) inside the container.
* Two mount points:
  + /home/ubuntu/Rubics → Maps to Rubics in the persistent volume.
  + /home/ubuntu/Storage\_Rubiscape → Maps to Storage\_Rubiscape in the persistent volume.
* Uses a Persistent Volume Claim (PVC) named partner-pvc to request storage.

**Node Selector (nodeSelector:)**

* Ensures this deployment runs on a specific node labeled application: partner.

**Service for the deployment**

#Create SVC

apiVersion: v1

kind: Service

metadata:

name: partner-backend-service

namespace: partner

labels:

app: partner

spec:

ports:

- port: 8085

protocol: TCP

selector:

app: partner-backend

type: NodePort



kind: Service

* Defines a service that connects to the partner-backend application.

metadata:

* The service is named partner-backend-service and belongs to the partner namespace.

ports:

* The service listens on port 8085 and uses TCP for communication.

selector:

* This service will find and route traffic to Pods labeled app: partner-backend.

type: NodePort

* Exposes the service on a high-numbered port on each Kubernetes node.
* This allows external access to the backend app via NodeIP:NodePort.

**Backup:**

AWS Backup is a fully managed backup service that centralizes and automates data protection across AWS services. It allows you to schedule, manage, and restore backups for various AWS resources, ensuring data availability and compliance.

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Frequency** | **Resource** | **Retention** |
| [prod-daily-backup](https://ap-south-1.console.aws.amazon.com/backup/home?region=ap-south-1#backupplan/details/ee91780f-767b-4e59-bb0e-2c02c4cf965e/version/NjYxYWE3YjYtYjQxZi00ZGZlLWEzYTktMDZmYzkxYzJlMTFm/rules/35dab47e-3df7-4f70-b76b-5b47fdd3e3fa) | Daily  At 06:00 AM IST | **EC2**  arn:aws:ec2:ap-south-1:155727836473:instance/i-0effa097006c7873a    **Stored in s3:**  arn:aws:s3:::db-backups-main | 10 days |

**Load Balancers:**

Elastic Load Balancing scales your load balancer capacity automatically in response to changes in incoming traffic.

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **DNS Name** | **Load Balancer ARN** | **Availability Zones** |
| [rubiscape-prod-lb](https://ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#LoadBalancer:loadBalancerArn=arn:aws:elasticloadbalancing:ap-south-1:155727836473:loadbalancer/app/rubiscape-prod-lb/804b98ede1ab2480;tab=listeners) | rubiscape-prod-lb-1968340750.ap-south-1.elb.amazonaws.com | arn:aws:elasticloadbalancing:ap-south-1:155727836473:loadbalancer/app/rubiscape-prod-lb/804b98ede1ab2480 | [Subnet-04a79cae9dbb0cdb7](https://ap-south-1.console.aws.amazon.com/vpc/home?region=ap-south-1#SubnetDetails:subnetId=subnet-04a79cae9dbb0cdb7)  [subnet-0c26b58d5b2dd8388](https://ap-south-1.console.aws.amazon.com/vpc/home?region=ap-south-1#SubnetDetails:subnetId=subnet-0c26b58d5b2dd8388) |
| [tomcat-alb](https://ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#LoadBalancer:loadBalancerArn=arn:aws:elasticloadbalancing:ap-south-1:155727836473:loadbalancer/app/tomcat-alb/43c2eb8f21e680b8;tab=listeners) | tomcat-alb-458614862.ap-south-1.elb.amazonaws.com | arn:aws:elasticloadbalancing:ap-south-1:155727836473:loadbalancer/app/tomcat-alb/43c2eb8f21e680b8 | [subnet-04a79cae9dbb0cdb7](https://ap-south-1.console.aws.amazon.com/vpc/home?region=ap-south-1#SubnetDetails:subnetId=subnet-04a79cae9dbb0cdb7)  [subnet-0c26b58d5b2dd8388](https://ap-south-1.console.aws.amazon.com/vpc/home?region=ap-south-1#SubnetDetails:subnetId=subnet-0c26b58d5b2dd8388) |
| [datalab-alb](https://ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#LoadBalancer:loadBalancerArn=arn:aws:elasticloadbalancing:ap-south-1:155727836473:loadbalancer/app/datalab-alb/9e52ca77b3f3ae63;tab=listeners) | datalab-alb-1984302783.ap-south-1.elb.amazonaws.com | arn:aws:elasticloadbalancing:ap-south-1:155727836473:loadbalancer/app/datalab-alb/9e52ca77b3f3ae63 | [subnet-04a79cae9dbb0cdb7](https://ap-south-1.console.aws.amazon.com/vpc/home?region=ap-south-1#SubnetDetails:subnetId=subnet-04a79cae9dbb0cdb7)  [subnet-0c26b58d5b2dd8388](https://ap-south-1.console.aws.amazon.com/vpc/home?region=ap-south-1#SubnetDetails:subnetId=subnet-0c26b58d5b2dd8388) |
| [k8s-monitori-promethe-577be11017](https://ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#LoadBalancer:loadBalancerArn=arn:aws:elasticloadbalancing:ap-south-1:155727836473:loadbalancer/app/k8s-monitori-promethe-577be11017/d1cb4006de5c5cb2;tab=listeners) | k8s-monitori-promethe-577be11017-689715089.ap-south-1.elb.amazonaws.com | arn:aws:elasticloadbalancing:ap-south-1:155727836473:loadbalancer/app/k8s-monitori-promethe-577be11017/d1cb4006de5c5cb2 | [subnet-04a79cae9dbb0cdb7](https://ap-south-1.console.aws.amazon.com/vpc/home?region=ap-south-1#SubnetDetails:subnetId=subnet-04a79cae9dbb0cdb7)  [subnet-0c26b58d5b2dd8388](https://ap-south-1.console.aws.amazon.com/vpc/home?region=ap-south-1#SubnetDetails:subnetId=subnet-0c26b58d5b2dd8388) |
| [k8s-monitori-promethe-653bea9db2](https://ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#LoadBalancer:loadBalancerArn=arn:aws:elasticloadbalancing:ap-south-1:155727836473:loadbalancer/app/k8s-monitori-promethe-653bea9db2/3b0c731b021fd99b;tab=listeners) | k8s-monitori-promethe-653bea9db2-1020543346.ap-south-1.elb.amazonaws.com | arn:aws:elasticloadbalancing:ap-south-1:155727836473:loadbalancer/app/k8s-monitori-promethe-653bea9db2/3b0c731b021fd99b | [subnet-04a79cae9dbb0cdb7](https://ap-south-1.console.aws.amazon.com/vpc/home?region=ap-south-1#SubnetDetails:subnetId=subnet-04a79cae9dbb0cdb7)  [subnet-0c26b58d5b2dd8388](https://ap-south-1.console.aws.amazon.com/vpc/home?region=ap-south-1#SubnetDetails:subnetId=subnet-0c26b58d5b2dd8388) |
| [sense-alb](https://ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#LoadBalancer:loadBalancerArn=arn:aws:elasticloadbalancing:ap-south-1:155727836473:loadbalancer/app/sense-alb/832569a774e5ea92;tab=listeners) | sense-alb-959612549.ap-south-1.elb.amazonaws.com | arn:aws:elasticloadbalancing:ap-south-1:155727836473:loadbalancer/app/sense-alb/832569a774e5ea92 | [subnet-04a79cae9dbb0cdb7](https://ap-south-1.console.aws.amazon.com/vpc/home?region=ap-south-1#SubnetDetails:subnetId=subnet-04a79cae9dbb0cdb7)  [subnet-0c26b58d5b2dd8388](https://ap-south-1.console.aws.amazon.com/vpc/home?region=ap-south-1#SubnetDetails:subnetId=subnet-0c26b58d5b2dd8388) |

**STEPS TO ADD NEW PORTS TO EXISTING LOAD BALANCER:**

**Identify the Load Balancer:**

* Open **AWS Management Console** > Navigate to **EC2** > **Load Balancers**.
* Select the **Load Balancer** where you want to add the new port.

**Create a New Target Group (if not already created):**

* Go to **EC2** > **Target Groups**.
* Click **Create Target Group**.
* Choose **Target Type** (Instance, IP, Lambda).
* Set **Protocol** (HTTP, HTTPS, TCP) and **Port** (e.g., 8080).
* Select the **VPC** where instances are running.
* Click **Next**, select instances, and register them.
* Click **Create**.

**Add a New Listener to the Load Balancer:**

* Go to **EC2** > **Load Balancers**.
* Select the **Load Balancer** and navigate to the **Listeners** tab.
* Click **Add Listener**.
* Choose **Protocol** (HTTP, HTTPS, TCP) and specify the **Port** (e.g., 8080).
* Under **Default Action**, select **Forward to Target Group** and choose the target group created earlier.
* Click **Add**.

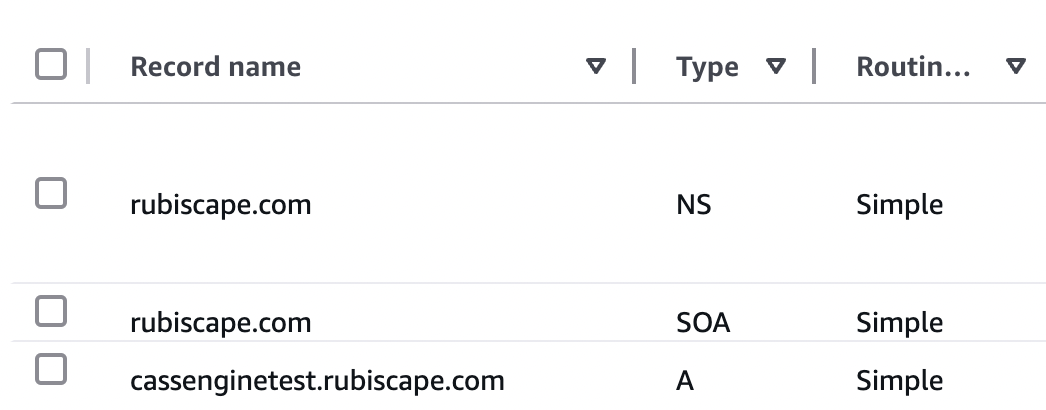
**Update Security Groups:**

* Go to **EC2** > **Security Groups**.
* Locate the security group associated with the Load Balancer.
* Edit the **Inbound Rules**:
  + Add a new rule allowing traffic on the new port (e.g., **8080**).
  + Choose **Source**: Anywhere (0.0.0.0/0) or a specific IP range.
* Click **Save rules**.

**Route 53:**

Amazon Route 53 is a scalable and highly available Domain Name System (DNS) web service that translates domain names into IP addresses. It also provides domain registration, traffic routing, and health checking for applications hosted on AWS or elsewhere.

**Hosted Zone:** rubiscape.com



# 

# **LAMBDA:**

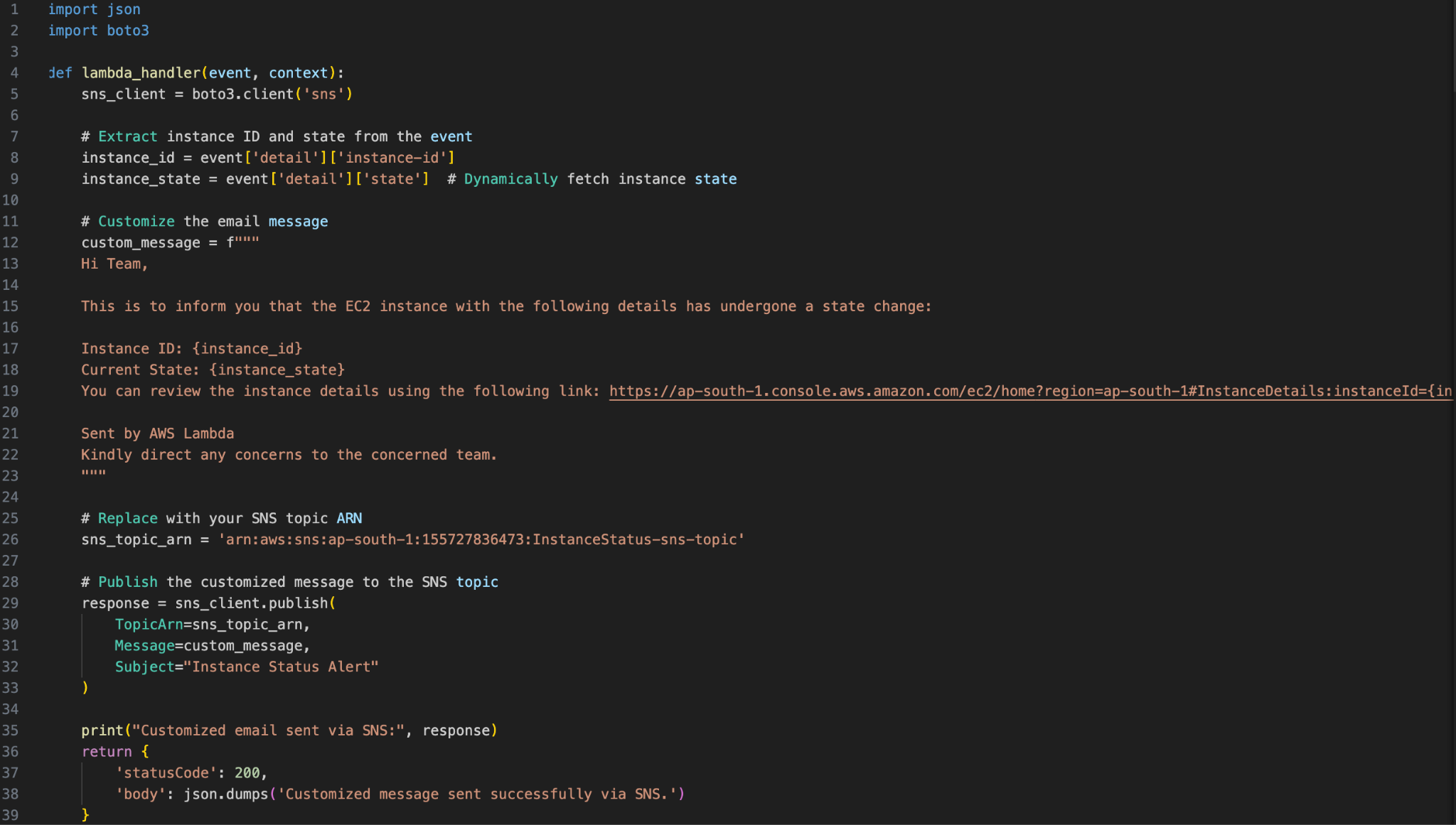
AWS Lambda is a serverless compute service that automatically runs your code in response to events and scales as needed. You only pay for the execution time, making it cost-effective for event-driven applications.

|  |  |  |  |
| --- | --- | --- | --- |
| **Function Name** | **Role Attached** | **Trigger** | **Destination** |
| [InstanceState-sns-Lambda](https://ap-south-1.console.aws.amazon.com/lambda/home?region=ap-south-1#/functions/InstanceState-sns-Lambda) | [InstanceState-sns-Lambda-role-04n6i7bg](https://ap-south-1.console.aws.amazon.com/go/view?arn=arn%3Aaws%3Aiam%3A%3A155727836473%3Arole%2Fservice-role%2FInstanceState-sns-Lambda-role-04n6i7bg&source=lambda) | EventBridge (Cloudwatch Events) | - |
| [startEc2](https://ap-south-1.console.aws.amazon.com/lambda/home?region=ap-south-1#/functions/startEc2) | [Lambda](https://ap-south-1.console.aws.amazon.com/go/view?arn=arn%3Aaws%3Aiam%3A%3A155727836473%3Arole%2FLambda&source=lambda) | - | - |
| [StopEc2](https://ap-south-1.console.aws.amazon.com/lambda/home?region=ap-south-1#/functions/StopEc2) | [Lambda](https://ap-south-1.console.aws.amazon.com/go/view?arn=arn%3Aaws%3Aiam%3A%3A155727836473%3Arole%2FLambda&source=lambda) | - | - |
| [start-ec2-full](https://ap-south-1.console.aws.amazon.com/lambda/home?region=ap-south-1#/functions/start-ec2-full) | [Lambda-full](https://ap-south-1.console.aws.amazon.com/go/view?arn=arn%3Aaws%3Aiam%3A%3A155727836473%3Arole%2FLambda-full&source=lambda) | - | - |
| [DockerStatus-sns-function](https://ap-south-1.console.aws.amazon.com/lambda/home?region=ap-south-1#/functions/DockerStatus-sns-function) | [DockerStatus-sns-Lambda-role-kn8ucpzn](https://ap-south-1.console.aws.amazon.com/go/view?arn=arn%3Aaws%3Aiam%3A%3A155727836473%3Arole%2Fservice-role%2FDockerStatus-sns-Lambda-role-kn8ucpzn&source=lambda) | EventBridge (Cloudwatch Events) | - |

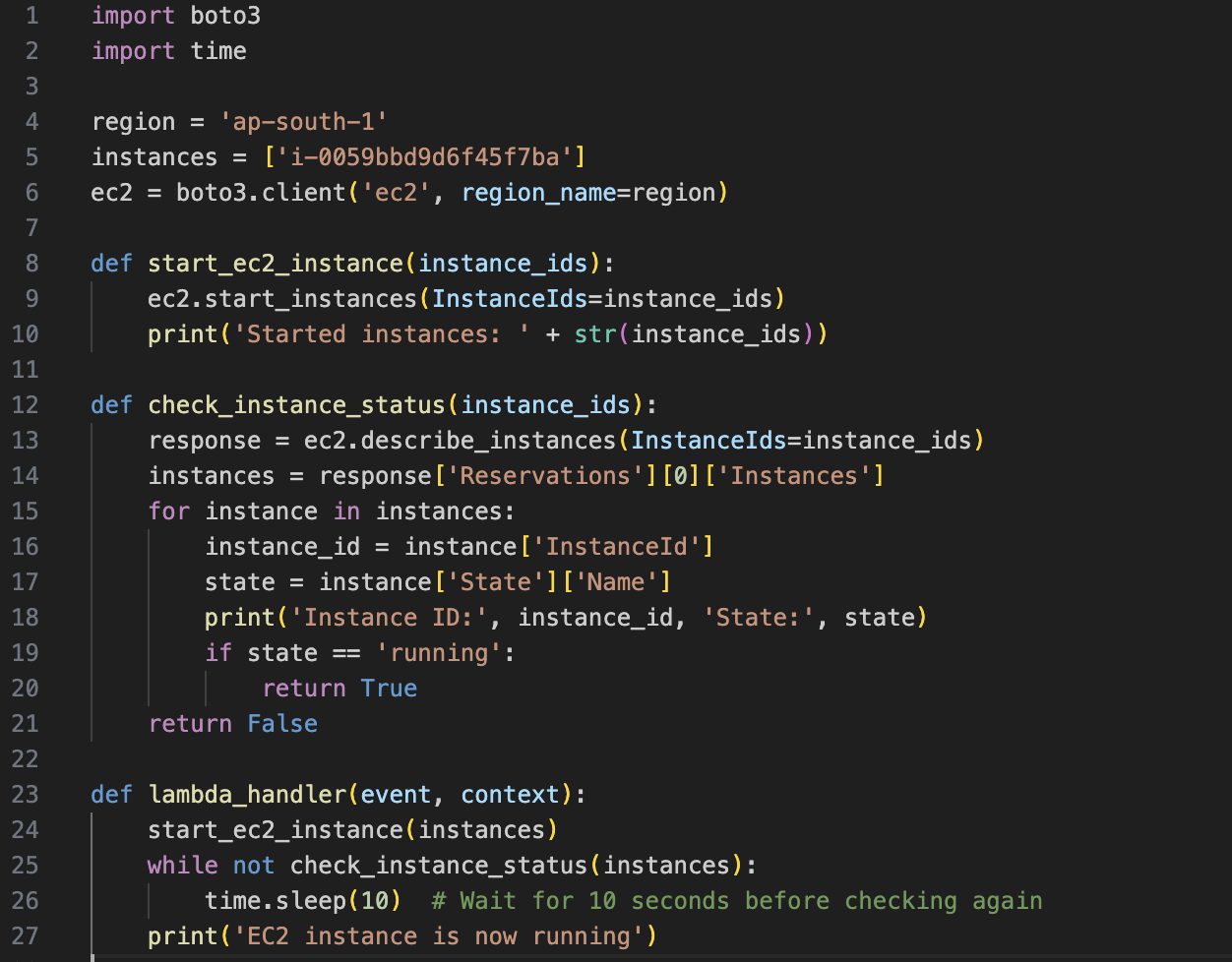
# 

**Now, for each of the Lambda Functions, here are the Codes:**

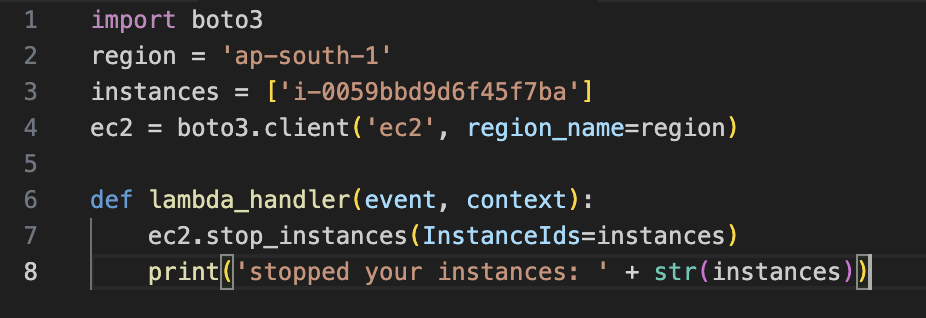
**1. InstanceState-sns-Lambda:**

****

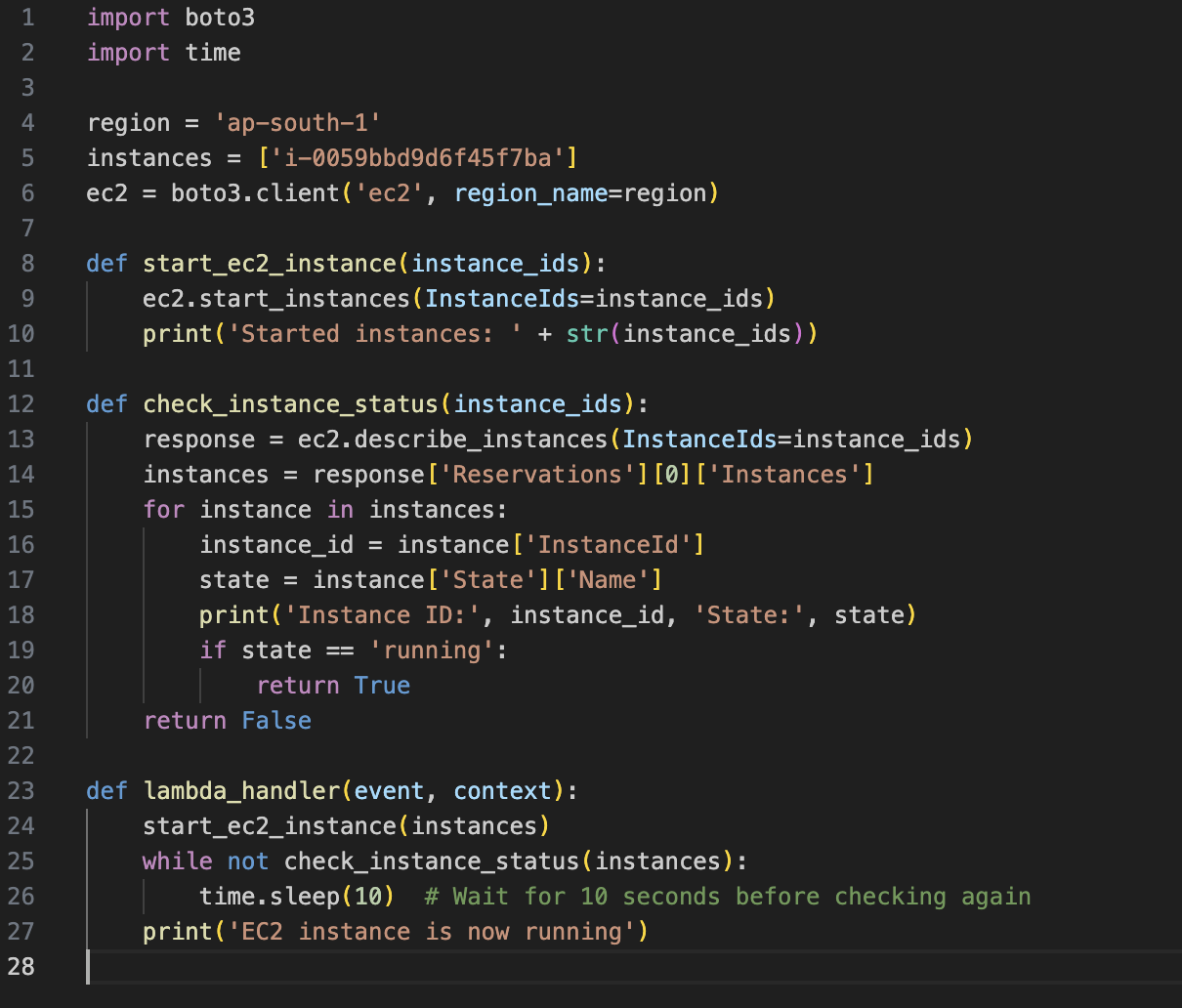
**2. startEc2:**

****

**3. StopEc2:**

****

**4. start-ec2-full:**



**5. DockerStatus-sns-function:**



**SNS (Simple Notification Service):**

# AWS Simple Notification Service (SNS) is a fully managed messaging service that enables applications, services, and users to send notifications securely, reliably, and at scale.

|  |  |  |  |
| --- | --- | --- | --- |
| **Function Name** | **Subscription** | **PROTOCOL** | **ARN** |
| [DockerStatus-sns-topic](https://ap-south-1.console.aws.amazon.com/sns/v3/home?region=ap-south-1#/topic/arn:aws:sns:ap-south-1:155727836473:DockerStatus-sns-topic) | systems@rubiscape.com | Email | arn:aws:sns:ap-south-1:155727836473:DockerStatus-sns-topic |
| [grafana-alerts](https://ap-south-1.console.aws.amazon.com/sns/v3/home?region=ap-south-1#/topic/arn:aws:sns:ap-south-1:155727836473:grafana-alerts) | systems@rubiscape.com | Email | arn:aws:sns:ap-south-1:155727836473:grafana-alerts |
| [InstanceStatus-sns-topic](https://ap-south-1.console.aws.amazon.com/sns/v3/home?region=ap-south-1#/topic/arn:aws:sns:ap-south-1:155727836473:InstanceStatus-sns-topic) | systems@rubiscape.com | Email | arn:aws:sns:ap-south-1:155727836473:InstanceStatus-sns-topic |
| [rubiscape-prod-sns-topic](https://ap-south-1.console.aws.amazon.com/sns/v3/home?region=ap-south-1#/topic/arn:aws:sns:ap-south-1:155727836473:rubiscape-prod-sns-topic) | systems@rubiscape.com | Email | arn:aws:sns:ap-south-1:155727836473:rubiscape-prod-sns-topic |

# 

# 

# 

# 

# 

# 

# 

# **SYDNEY REGION**

# **AWS Environment Structure:**

The new AWS environment setup is done using the AWS native resources only like VPC, subnets, EC2, ECS, Application Load Balancer.

|  |  |
| --- | --- |
| Environment | Description |
| PROD Environment | Production environment |

## 

## 

## **Networking Architecture:**

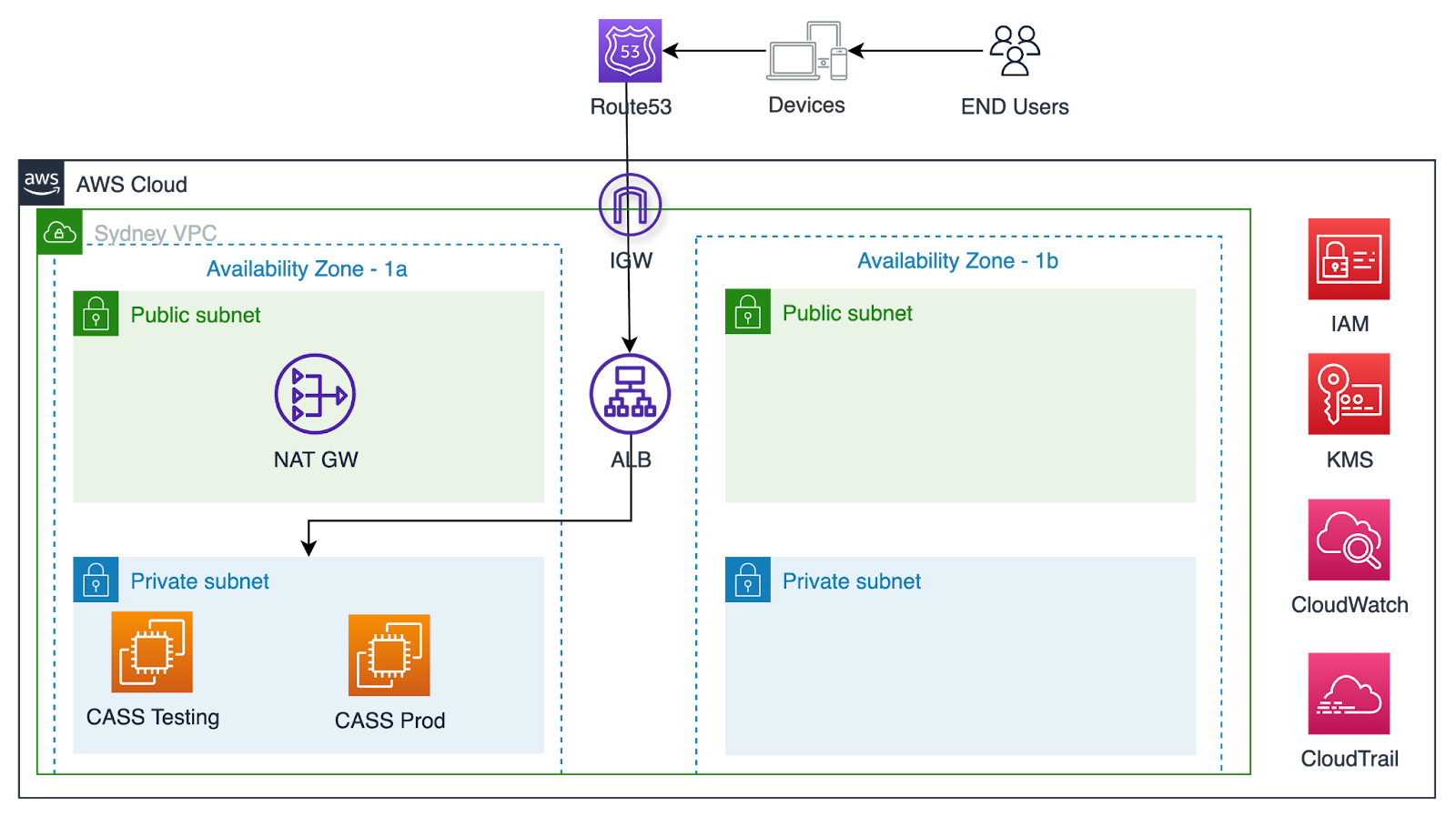
In AWS Virtual Private Cloud (VPC) provides secure Networking for the resources in AWS. Searce team will create the networking based on the below architecture. It will be configured with its own network access control list (NACL), and routing table. The following sections cover a detailed explanation of all components.

Please find the application details about Streamlyn Business Line below.

|  |  |  |
| --- | --- | --- |
| Region | Environment | Application Name |
| **Sydney** | PROD | CASS Prod |
| Pritunl | cassengine-pritunl-vpn |
| Testing | CASSTesting |

The following diagram displays Rubiscape’s Production Environments

**Architectures:**

****

## 

## **Routing in AWS:**

### **Route Tables:**

A route table contains a set of rules called routes that are used to determine where network traffic is directed. The following tables describe the route table rules and subnet associations.

### **Route Table and Subnet Associations:**

A route table contains a set of rules called routes that are used to determine where network traffic is directed.

### 

### **Production VPC Route Tables:**

* **Public RTB:** This RTB is attached to the public subnets that can communicate with the following destination CIDRs.
* **Private RTB:** This RTB is attached to the private subnets that can communicate with the following destination CIDRs.

**Public Route Table ID:** **rtb-0f277f28653d7d3e9**

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Destination** | **Target** | **Subnet Associations** |
| cassengine-prod-public-rt | 0.0.0.0/0 192.168.20.0/24 | [igw-0098f9e56ce79eaed](https://ap-southeast-2.console.aws.amazon.com/vpcconsole/home?region=ap-southeast-2#igws:internetGatewayId=igw-0098f9e56ce79eaed) local | cassengine-prod-public-az2-subnet  cassengine-prod-public-az1-subnet |

**Private Route Table ID:** **rtb-0ce7d5ac19d60d08f**

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Destination** | **Target** | **Subnet Associations** |
| cassengine-prod-app-rt | 0.0.0.0/0 192.168.20.0/24 | [nat-0d6fe57499b7c56bb](https://ap-southeast-2.console.aws.amazon.com/vpcconsole/home?region=ap-southeast-2#NatGateways:natGatewayId=nat-0d6fe57499b7c56bb)  Local | Cassengine-prod-app-az2-subnet  cassengine-prod-app-az1-subnet |

## 

## **VPC:**

Amazon **VPC (Virtual Private Cloud)** is a networking service that allows you to create a **secure, isolated** virtual network within AWS. It enables you to define your own **IP address ranges, subnets, routing, and security settings**, providing full control over your cloud network. The Production VPC is configured with four-tier architecture.

|  |  |
| --- | --- |
| **Tier** | **Purpose** |
| Public Subnet | This tier is a public subnet that hosts externally facing services that require unique IPs and that are directly accessed. It also hosts the NAT gateway which will be leveraged by all the workload instances to access the internet. |
| Private Subnet | This tier is a private subnet. |

The following tables describe the Security VPC name and VPC ID’s.

### **VPC details:**

|  |  |
| --- | --- |
| **NAME** | **VPC ID** |
| **cassengine-prod-vpc** | [vpc-0a75ef611edef3938](https://ap-southeast-2.console.aws.amazon.com/vpcconsole/home?region=ap-southeast-2#VpcDetails:VpcId=vpc-0a75ef611edef3938) |

### **Subnet IP Ranges**

Production VPC is provisioned with **10.0.0.0/16** CIDRs and it contains six private and two public subnets. These subnets have been created in **ap-south-1 (Mumbai)** region.

| **Subnets** | **CIDR** |
| --- | --- |
| cassengine-prod-public-az1-subnet | 192.168.20.0/26 |
| cassengine-prod-app-az1-subnet | 192.168.20.128/26 |
| cassengine-prod-public-az2-subnet | 192.168.20.64/26 |
| cassengine-prod-app-az2-subnet | 192.168.20.192/26 |

2

## **Security Control:**

AWS Services like Security Groups and Network Access control can be leveraged to provide firewall capabilities and security control.

### **NACLs:**

NACLs provide stateless firewall capabilities that can only be applied at the subnet level. NACLs are best used for blacklisting ports, services, or hosts for entire subnets. Given their stateless nature, any bi-directional communications would require ingress and Egress NACL (Outbound) rules to be configured. NACLs will be used sparingly as heavy implementation of NACLs can result in unexpected network communication blocks and difficulty to troubleshoot. NACLs will be used as guardrails to blacklist all ingress or egress traffic to subnets that should never occur.

Below is the list of Ingress and Egress rules that will be applied for the NACLs in **Prod and DEV VPCs**.

The following table provides the NACL details in different VPCs.

**NACL:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Network ACL ID** | **Associated with** | **Default** |
| - | [acl-0c89a7ef999438d70](https://ap-southeast-2.console.aws.amazon.com/vpcconsole/home?region=ap-southeast-2#NetworkAclDetails:networkAclId=acl-0c89a7ef999438d70) | All the Subnets in the VPC | YES |

The **NACLs** have the following Ingress and Egress rules.

**Ingress NACL (Inbound)**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Rule** | **Type** | **Protocol** | **Port Range** | **Destination** | **Allow/Deny** |
| 100 | ALL Traffic | ALL | ALL | 0.0.0.0/0 | ALLOW |
| \* | ALL Traffic | ALL | ALL | 0.0.0.0/0 | DENY |

**Note:** In the AWS Console you can see the **Destination** as the **Source.**

Egress NACL (Outbound)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Rule** | **Type** | **Protocol** | **Port Range** | **Destination** | **Allow/Deny** |
| 100 | ALL Traffic | ALL | ALL | 0.0.0.0/0 | ALLOW |
| \* | ALL Traffic | ALL | ALL | 0.0.0.0/0 | DENY |

**Note:** In the AWS Console you can see the **Destination** as the **Source.**

### **Security Groups:**

Security Groups provide stateful firewall capabilities that can be applied directly to AWS resources. Security Groups will be used within the environment to prevent communication between hosts and tiers that do not require direct access.

The security groups can be used to restrict access between Business Unit applications and services as well as between tiers, such as web and app tiers. A standardized Security Group approach is recommended. AWS resources should have a baseline of up to three security groups applied depending on role. The following diagram shows the different security groups that may be applied.



***Figure 2: Security Group Layered Approach***

**Security Group Design:**

In addition to standard port requirements that are configured as part of the base infrastructure, the following application specific ports will be added to the required Security Groups in the Management, Security and Workload VPCs.

#### **Prod VPC Security Groups**

This section describes the Prod VPC security groups and its inbound and outbound rules.

##### **1. Cassengine Prod ALB security group:**

The following table provides the Security group Name and Security-ID details.

| **Name** | **Group ID** | **VPCID** |
| --- | --- | --- |
| cassengine-prod-alb-sg | [sg-01797fe57c3bb5d77](https://ap-southeast-2.console.aws.amazon.com/ec2/home?region=ap-southeast-2#SecurityGroup:groupId=sg-01797fe57c3bb5d77) | [vpc-0a75ef611edef3938](https://ap-southeast-2.console.aws.amazon.com/vpcconsole/home?region=ap-southeast-2#vpcs:VpcId=vpc-0a75ef611edef3938) |

The cassengine-prod-alb-sghas the following inbound and outbound rules.

###### **Inbound**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Type** | **Protocol** | **Port Range** | **Source** | **Description** |
| HTTPS | TCP | 443 | 0.0.0.0/0 | - |
| HTTP | TCP | 80 | 0.0.0.0/0 | - |

#### 

###### **Outbound**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Type** | **Protocol** | **Port Range** | **Source** | **Description** |
| All traffic | ALL | ALL | 0.0.0.0/0 | - |

**2**.**Cassengine Prod EC2 security group:**

The following table provides the Security group Name and Security-ID details.

| **Name** | **Group ID** | **VPCID** |
| --- | --- | --- |
| cassengine-prod-ec2-sg | [sg-0a6046a21212a526d](https://ap-southeast-2.console.aws.amazon.com/vpcconsole/home?region=ap-southeast-2#SecurityGroup:groupId=sg-0a6046a21212a526d) | [vpc-0a75ef611edef3938](https://ap-southeast-2.console.aws.amazon.com/vpcconsole/home?region=ap-southeast-2#vpcs:VpcId=vpc-0a75ef611edef3938) |

###### **Inbound:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Type** | **Protocol** | **Port Range** | **Source** | **Description** |
| Custom TCP | TCP | 8090 | [sg-01797fe57c3bb5d77 / cassengine-sydney-cf-ALBSecurityGroup-Wy3KMFdhFYkX](https://ap-southeast-2.console.aws.amazon.com/vpcconsole/home?region=ap-southeast-2#SecurityGroup:groupId=sg-01797fe57c3bb5d77) | - |
| Custom TCP | TCP | 8080 | 192.168.20.117/32 | Frontend Pritunl VPN |
| Custom TCP | TCP | 8085 | 192.168.20.117/32 | Backend Pritunl VPN |
| Custom TCP | TCP | 8080 | [sg-01797fe57c3bb5d77 / cassengine-sydney-cf-ALBSecurityGroup-Wy3KMFdhFYkX](https://ap-southeast-2.console.aws.amazon.com/vpcconsole/home?region=ap-southeast-2#SecurityGroup:groupId=sg-01797fe57c3bb5d77) | - |
| Custom TCP | TCP | 8082 | [sg-01797fe57c3bb5d77 / cassengine-sydney-cf-ALBSecurityGroup-Wy3KMFdhFYkX](https://ap-southeast-2.console.aws.amazon.com/vpcconsole/home?region=ap-southeast-2#SecurityGroup:groupId=sg-01797fe57c3bb5d77) | - |
| Custom TCP | TCP | 8085 | [sg-01797fe57c3bb5d77 / cassengine-sydney-cf-ALBSecurityGroup-Wy3KMFdhFYkX](https://ap-southeast-2.console.aws.amazon.com/vpcconsole/home?region=ap-southeast-2#SecurityGroup:groupId=sg-01797fe57c3bb5d77) | - |
| Custom TCP | TCP | 8082 | 192.168.20.117/32 | Pritunl survey traffic |
| Custom TCP | TCP | 8090 | 192.168.20.117/32 | Visualization Pritunl VPN |
| SSH | TCP | 22 | 192.168.20.117/32 | SSH Pritunl VPN |

#### 

###### **Outbound**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Type** | **Protocol** | **Port Range** | **Source** | **Description** |
| All traffic | ALL | ALL | 0.0.0.0/0 | - |

**3**.**Cassengine Pritunl VPN security group:**

The following table provides the Security group Name and Security-ID details.

| **Name** | **Group ID** | **VPCID** |
| --- | --- | --- |
| cassengine-pritunl-vpn-sg | [sg-0bbddd7e1f83c96fc](https://ap-southeast-2.console.aws.amazon.com/vpcconsole/home?region=ap-southeast-2#SecurityGroup:groupId=sg-0bbddd7e1f83c96fc) | [vpc-0a75ef611edef3938](https://ap-southeast-2.console.aws.amazon.com/vpcconsole/home?region=ap-southeast-2#vpcs:VpcId=vpc-0a75ef611edef3938) |

###### 

###### **Inbound:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Type** | **Protocol** | **Port Range** | **Source** | **Description** |
| HTTPS | TCP | 443 | 0.0.0.0/0 | Pritunl VPN |
| HTTP | TCP | 80 | 0.0.0.0/0 | Pritunl VPN |
| SSH | TCP | 22 | 36.255.185.119/32 | sanket\_HomeIP |
| SSH | TCP | 22 | 202.71.158.34/32 | Rubiscape\_office\_PublicIP |
| Custom UDP | UDP | 1194 | 0.0.0.0/0 | Pritunl VPN |

#### 

###### **Outbound**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Type** | **Protocol** | **Port Range** | **Source** | **Description** |
| All traffic | ALL | ALL | 0.0.0.0/0 | - |

**4**.**Cassengine Prod LB security group:**

The following table provides the Security group Name and Security-ID details.

| **Name** | **Group ID** | **VPCID** |
| --- | --- | --- |
| cassengine-prod-lb | [sg-01797fe57c3bb5d77](https://ap-southeast-2.console.aws.amazon.com/ec2/home?region=ap-southeast-2#SecurityGroup:groupId=sg-01797fe57c3bb5d77) | [vpc-0a75ef611edef3938](https://ap-southeast-2.console.aws.amazon.com/vpcconsole/home?region=ap-southeast-2#vpcs:VpcId=vpc-0a75ef611edef3938) |

###### **Inbound:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Type** | **Protocol** | **Port Range** | **Source** | **Description** |
| HTTPS | TCP | 443 | 0.0.0.0/0 | - |
| HTTP | TCP | 80 | 0.0.0.0/0 | - |

#### 

###### **Outbound**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Type** | **Protocol** | **Port Range** | **Source** | **Description** |
| All traffic | ALL | ALL | 0.0.0.0/0 | - |

## 

## **EC2 Instances:**

Amazon **EC2 (Elastic Compute Cloud)** is a cloud-based virtual server service that provides scalable compute capacity. It allows users to launch, configure, and manage virtual machines (instances) on demand, without needing physical hardware.

| **Name** | **Private IP address** | **Instance ID** | **Subnet ID** | **Security Group** |
| --- | --- | --- | --- | --- |
| CASSTesting | 192.168.20.150 | [i-0497a092b652f9cbb](https://ap-southeast-2.console.aws.amazon.com/ec2/home?region=ap-southeast-2#InstanceDetails:instanceId=i-0497a092b652f9cbb) | [subnet-00e928e92c9a860bc](https://ap-southeast-2.console.aws.amazon.com/vpc/home?region=ap-southeast-2#subnets:subnetId=subnet-00e928e92c9a860bc) | [sg-0a6046a21212a526d](https://ap-southeast-2.console.aws.amazon.com/ec2/home?region=ap-southeast-2#SecurityGroup:securityGroupId=sg-0a6046a21212a526d) |
| cassengine-pritunl-vpn | 192.168.20.117 | [i-0f0a849398a30c27f](https://ap-southeast-2.console.aws.amazon.com/ec2/home?region=ap-southeast-2#InstanceDetails:instanceId=i-0f0a849398a30c27f) | [subnet-00fecb3517f45e44f](https://ap-southeast-2.console.aws.amazon.com/vpc/home?region=ap-southeast-2#subnets:subnetId=subnet-00fecb3517f45e44f) | [sg-0bbddd7e1f83c96fc](https://ap-southeast-2.console.aws.amazon.com/ec2/home?region=ap-southeast-2#SecurityGroup:securityGroupId=sg-0bbddd7e1f83c96fc) |
| CASS Prod | 192.168.20.196 | [i-05634f2ed12b2af86](https://ap-southeast-2.console.aws.amazon.com/ec2/home?region=ap-southeast-2#InstanceDetails:instanceId=i-05634f2ed12b2af86) | [subnet-072fd9de5f6264329](https://ap-southeast-2.console.aws.amazon.com/vpc/home?region=ap-southeast-2#subnets:subnetId=subnet-072fd9de5f6264329) | [sg-0a6046a21212a526d](https://ap-southeast-2.console.aws.amazon.com/ec2/home?region=ap-southeast-2#SecurityGroup:securityGroupId=sg-0a6046a21212a526d) |

## 

## **S3 Bucket:**

Amazon S3 (Simple Storage Service) is an object storage service provided by AWS that allows users to store and retrieve any amount of data at any time. It is designed for scalability, security, durability, and performance, making it ideal for storing backup files, logs, media files, and data lakes.

### **Types of S3 Buckets (Storage Classes):**

1. S3 Standard
2. S3 Intelligent-Tiering
3. S3 Standard-IA (Infrequent Access)
4. S3 One Zone-IA
5. S3 Glacier
6. S3 Glacier Deep Archive

|  |  |
| --- | --- |
| **Bucket Name** | **Bucket Arn** |
| [cf-templates-19mc2jynp9tpm-ap-southeast-2](https://ap-southeast-2.console.aws.amazon.com/s3/buckets/cf-templates-19mc2jynp9tpm-ap-southeast-2?region=ap-southeast-2) | arn:aws:s3:::cf-templates-19mc2jynp9tpm-ap-southeast-2 |

## **Elastic IP:**

An **Elastic IP (EIP)** is a static, public IPv4 address provided by AWS for use in Amazon EC2 instances. Unlike regular public IPs assigned to EC2 instances, Elastic IPs remain constant even if an instance is stopped or restarted.

|  |  |
| --- | --- |
| **EIP Name** | **Public IP** |
| cassengine-prod-nat1-eip | [13.239.167.81](https://ap-southeast-2.console.aws.amazon.com/ec2/home?region=ap-southeast-2#ElasticIpDetails:AllocationId=eipalloc-07966cfe74f3f1829) |

## **IAM Roles:**

**IAM (Identity and Access Management) Roles** are a way to grant **temporary** permissions to AWS resources without needing to share long-term credentials (such as access keys). Unlike IAM users, IAM roles are **not associated with a specific user** but can be assumed by AWS services, applications, or other AWS accounts.

Below table suggests IAM role created for account to be used by all the instances.

|  |  |  |
| --- | --- | --- |
| **IAM Role** | **Policy Attached** | **Description** |
| Rubiscape-Prod-Cloudwatch-MonitoringInstanceProfile | [CloudWatchLogsFullAccess](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-southeast-2#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2FCloudWatchLogsFullAccess)  [CloudWatchFullAccessV2](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-southeast-2#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2FCloudWatchFullAccessV2)  [CloudWatchFullAccess](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-southeast-2#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2FCloudWatchFullAccess)  [CloudWatchAgentServerPolicy](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-southeast-2#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2FCloudWatchAgentServerPolicy)  [AWSLambdaBasicExecutionRole-8af21ccf-48d4-46d5-b3b9-7598a09b16ac](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-southeast-2#/policies/details/arn%3Aaws%3Aiam%3A%3A155727836473%3Apolicy%2Fservice-role%2FAWSLambdaBasicExecutionRole-8af21ccf-48d4-46d5-b3b9-7598a09b16ac)  [AWSLambda\_FullAccess](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-southeast-2#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2FAWSLambda_FullAccess)  [AWSLambdaBasicExecutionRole-65d8438f-edd3-4832-a36c-3b75e0fcb8b8](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-southeast-2#/policies/details/arn%3Aaws%3Aiam%3A%3A155727836473%3Apolicy%2Fservice-role%2FAWSLambdaBasicExecutionRole-65d8438f-edd3-4832-a36c-3b75e0fcb8b8)  [AmazonSSMFullAccess](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-southeast-2#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2FAmazonSSMFullAccess)[AmazonSNSFullAccess](https://us-east-1.console.aws.amazon.com/iam/home?region=ap-southeast-2#/policies/details/arn%3Aaws%3Aiam%3A%3Aaws%3Apolicy%2FAmazonSNSFullAccess) | For CloudWatch Agent, Lamda and SSM. |

## 

## 

## **KMS:**

AWS **Key Management Service (KMS)** is a managed service that allows you to create, manage, and control encryption keys used to secure your data across AWS services and applications. It simplifies key management while ensuring strong security and compliance.

|  |  |  |
| --- | --- | --- |
| **Key Name** | **Description** | **ARN** |
| aws/sns | Default key that protects my SNS data when no other key is defined | arn:aws:kms:ap-southeast-2:155727836473:key/3392d5e5-95e5-484f-894c-2e95fba81538 |
| aws/acm | Default key that protects my ACM private keys when no other key is defined | arn:aws:kms:ap-southeast-2:155727836473:key/9fa71cf1-82b6-47a7-8a5b-9025431e4d9c |
| aws/backup | Default key that protects my Backup data when no other key is defined | arn:aws:kms:ap-southeast-2:155727836473:key/f793238f-3d01-4763-8ccc-e8946781f1e7 |
| [cassengine-prod-ebs](https://ap-southeast-2.console.aws.amazon.com/kms/home?region=ap-southeast-2#/kms/keys/790732fa-54da-45f9-98af-19efbd7f24a0) | cassengine-prod-ebs-encryption-key | arn:aws:kms:ap-southeast-2:155727836473:key/790732fa-54da-45f9-98af-19efbd7f24a0 |

**Load Balancers:**

Elastic Load Balancing scales your load balancer capacity automatically in response to changes in incoming traffic.

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **DNS Name** | **Load Balancer ARN** | **Availability Zones** |
| [cassengine-prod-lb](https://ap-southeast-2.console.aws.amazon.com/ec2/home?region=ap-southeast-2#LoadBalancer:loadBalancerArn=arn:aws:elasticloadbalancing:ap-southeast-2:155727836473:loadbalancer/app/cassengine-prod-lb/7dfe22261f4c2135;tab=listeners) | cassengine-prod-lb-549308365.ap-southeast-2.elb.amazonaws.com | arn:aws:elasticloadbalancing:ap-southeast-2:155727836473:loadbalancer/app/cassengine-prod-lb/7dfe22261f4c2135 | [subnet-00fecb3517f45e44f](https://ap-southeast-2.console.aws.amazon.com/vpc/home?region=ap-southeast-2#SubnetDetails:subnetId=subnet-00fecb3517f45e44f)  [subnet-0873810b10c20ea7e](https://ap-southeast-2.console.aws.amazon.com/vpc/home?region=ap-southeast-2#SubnetDetails:subnetId=subnet-0873810b10c20ea7e) |

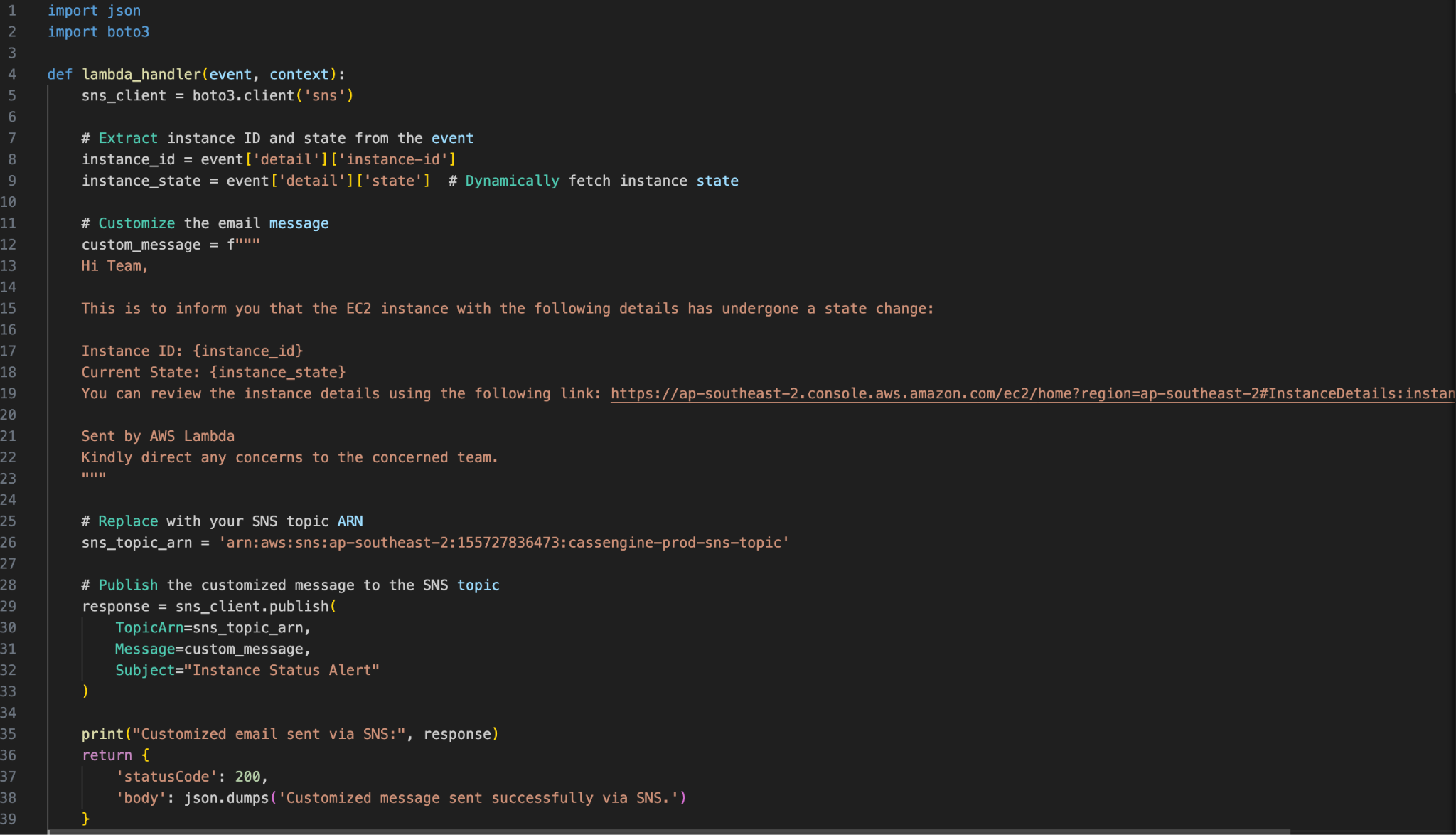
# **LAMBDA:**

AWS Lambda is a serverless compute service that automatically runs your code in response to events and scales as needed. You only pay for the execution time, making it cost-effective for event-driven applications.

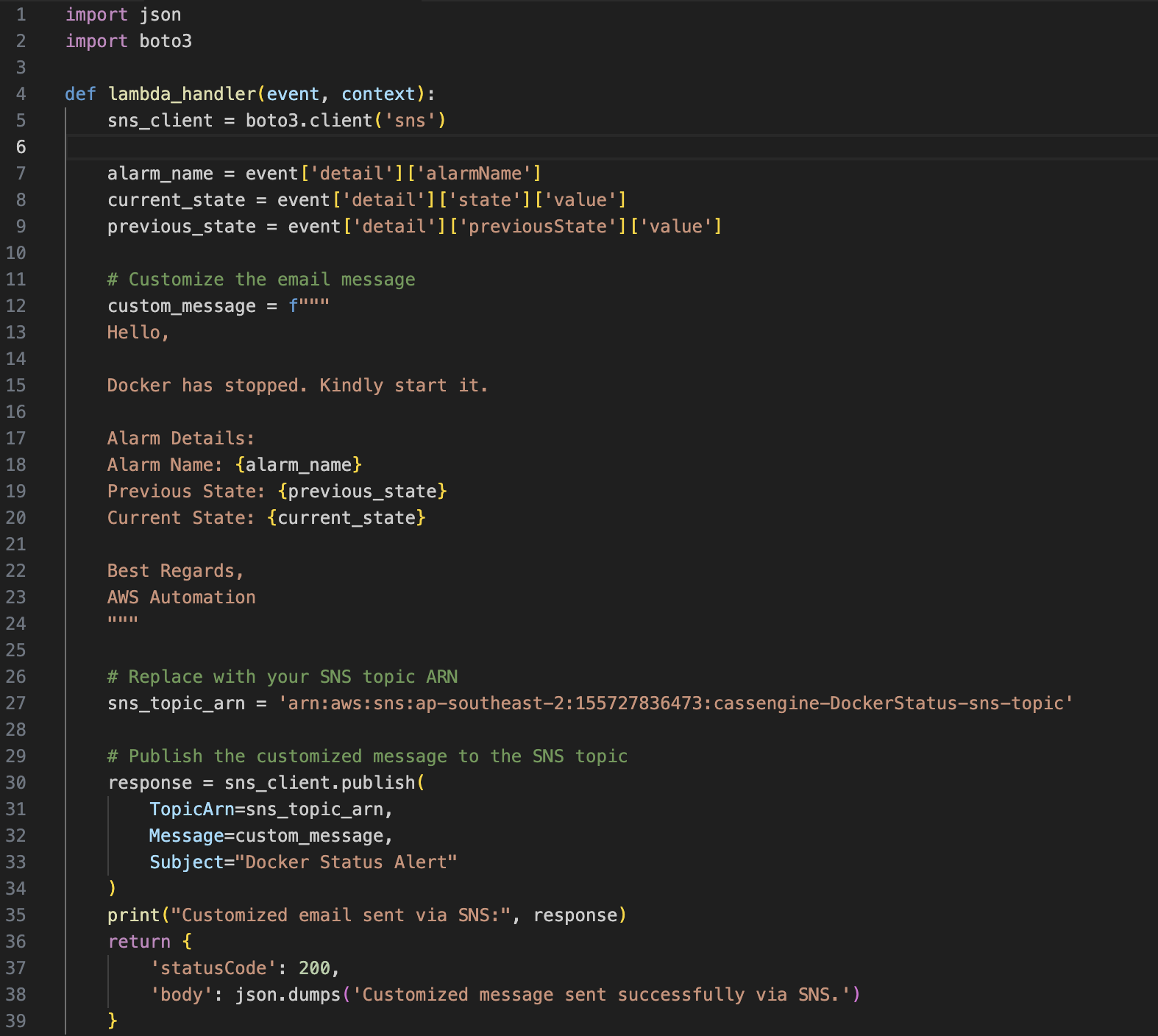
|  |  |  |  |
| --- | --- | --- | --- |
| **Function Name** | **Role Attached** | **Trigger** | **Destination** |
| [InstanceState-sns-Lambda](https://ap-south-1.console.aws.amazon.com/lambda/home?region=ap-south-1#/functions/InstanceState-sns-Lambda) | [InstanceState-sns-Lambda-role-04n6i7bg](https://ap-south-1.console.aws.amazon.com/go/view?arn=arn%3Aaws%3Aiam%3A%3A155727836473%3Arole%2Fservice-role%2FInstanceState-sns-Lambda-role-04n6i7bg&source=lambda) | EventBridge (Cloudwatch Events) | - |
| [DockerStatus-sns-function](https://ap-south-1.console.aws.amazon.com/lambda/home?region=ap-south-1#/functions/DockerStatus-sns-function) | [DockerStatus-sns-Lambda-role-kn8ucpzn](https://ap-south-1.console.aws.amazon.com/go/view?arn=arn%3Aaws%3Aiam%3A%3A155727836473%3Arole%2Fservice-role%2FDockerStatus-sns-Lambda-role-kn8ucpzn&source=lambda) | EventBridge (Cloudwatch Events) | - |

**Now, for each of the Lambda Functions, here are the Codes:**

**1. InstanceState-sns-Lambda:**

****

**2. dockerStatus-sns-function:**

****

**SNS (Simple Notification Service):**

# AWS Simple Notification Service (SNS) is a fully managed messaging service that enables applications, services, and users to send notifications securely, reliably, and at scale.

|  |  |  |  |
| --- | --- | --- | --- |
| **Function Name** | **Subscription** | **PROTOCOL** | **ARN** |
| [cassengine-DockerStatus-sns-topic](https://ap-southeast-2.console.aws.amazon.com/sns/v3/home?region=ap-southeast-2#/topic/arn:aws:sns:ap-southeast-2:155727836473:cassengine-DockerStatus-sns-topic) | systems@rubiscape.com | Email | arn:aws:sns:ap-southeast-2:155727836473:cassengine-DockerStatus-sns-topic |
| [cassengine-prod-sns-topic](https://ap-southeast-2.console.aws.amazon.com/sns/v3/home?region=ap-southeast-2#/topic/arn:aws:sns:ap-southeast-2:155727836473:cassengine-prod-sns-topic) | systems@rubiscape.com | Email | arn:aws:sns:ap-southeast-2:155727836473:cassengine-prod-sns-topic |

# 

# 

# 

# 