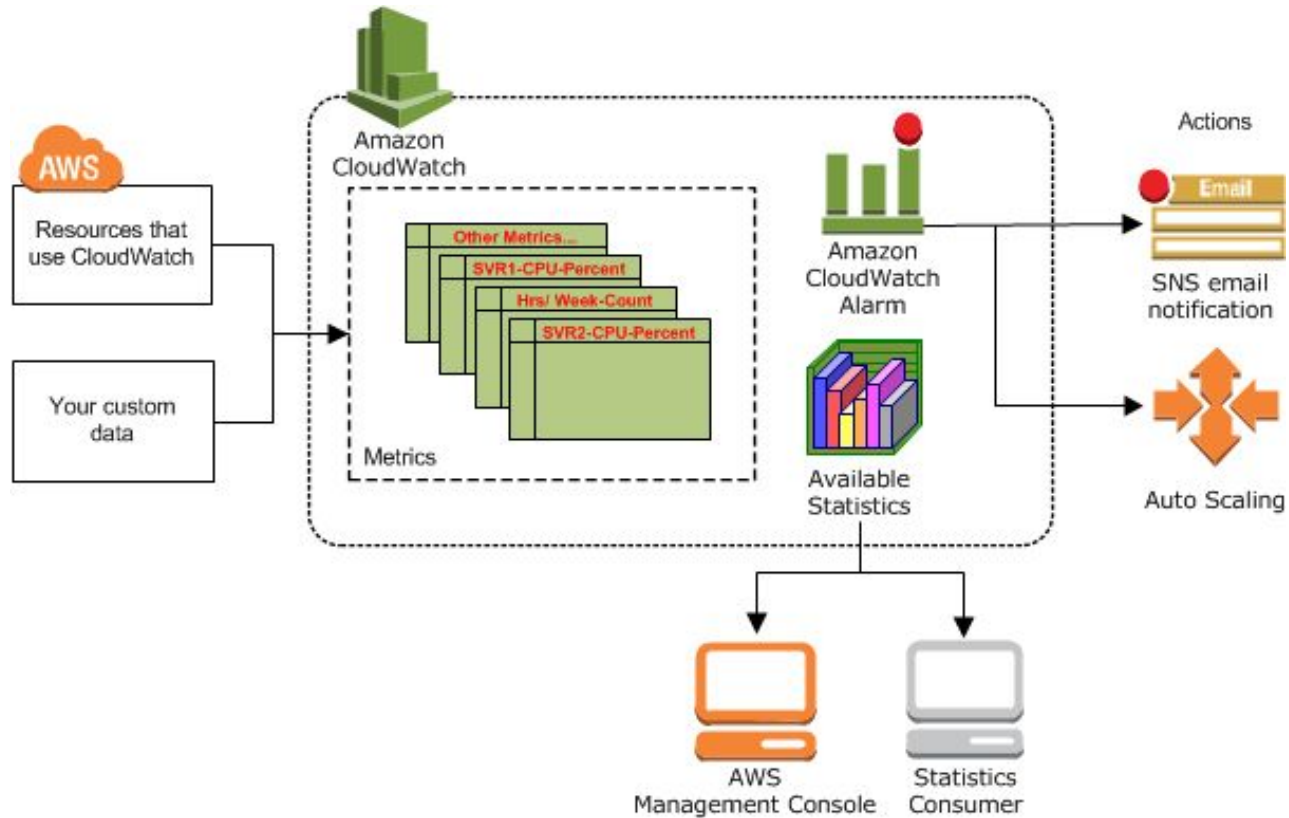
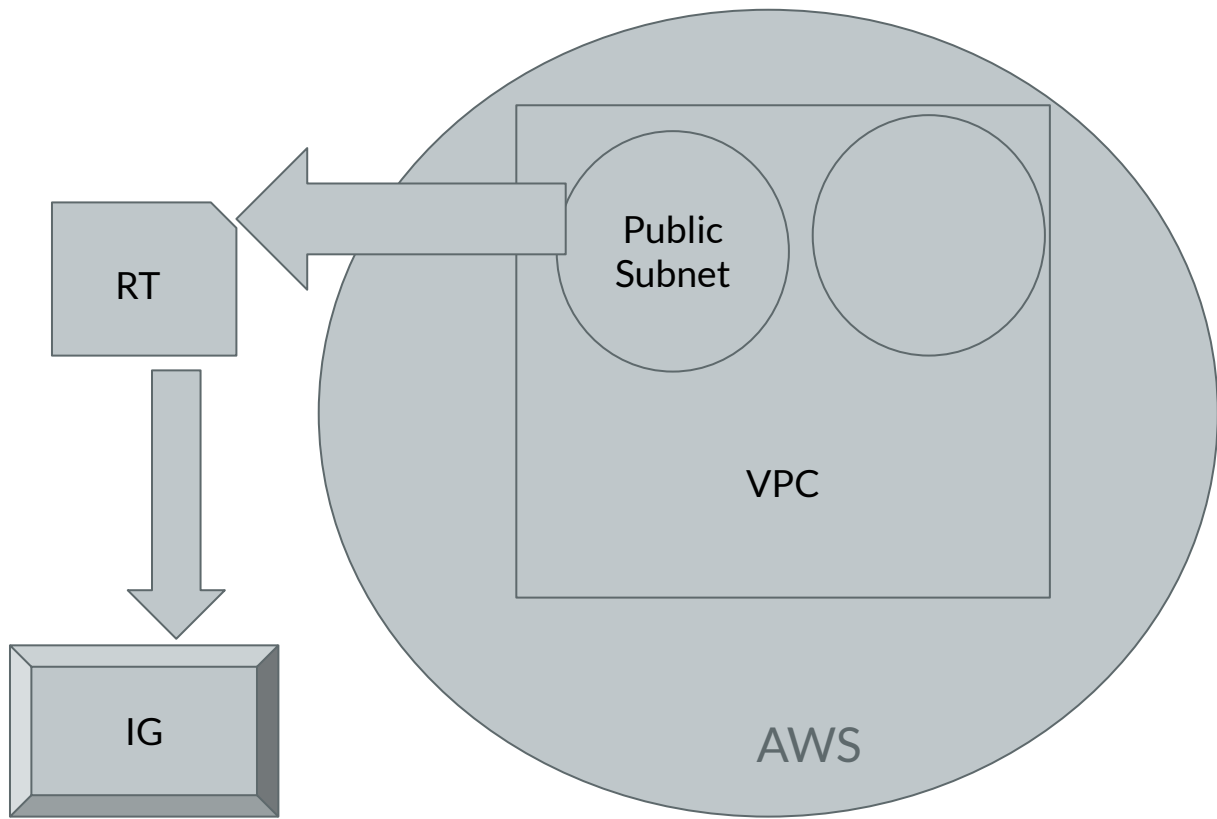


# AWS CloudWatch

Resource Monitoring

# AWS CloudWatch





# What CloudWatch can Do ?

- **Amazon CloudWatch is basically a metrics repository. An AWS service—such as Amazon EC2—puts metrics into the repository, and you retrieve statistics based on those metrics. If you put your own custom metrics into the repository, you can retrieve statistics on these metrics as well.**
- **You can use metrics to calculate statistics and then present the data graphically in the CloudWatch console.**
- **You can configure alarm actions to stop, start, or terminate an Amazon EC2 instance when certain criteria are met. In addition, you can create alarms that initiate Amazon EC2 Auto Scaling and Amazon Simple Notification Service (Amazon SNS) actions on your behalf.**
- **Metrics are stored separately in Regions, but you can use CloudWatch cross-Region functionality to aggregate statistics from different Regions.**

# Example

**put-metric-alarm** - Creates or updates an alarm and associates it with the specified metric, metric math expression, anomaly detection model, or Metrics Insights query.

The following example uses the **put-metric-alarm** command to send an Amazon Simple Notification Service email message when CPU utilization exceeds 70 percent:

```
aws cloudwatch put-metric-alarm
--alarm-name cpu-mon \
--alarm-description "Alarm when CPU exceeds 70 percent" \
--metric-name CPUUtilization \
--namespace AWS/EC2 \
--statistic Average \
--period 300 \
--threshold 70 \
--comparison-operator GreaterThanThreshold \
--dimensions "Name=InstanceId,Value=i-12345678" \
--evaluation-periods 2 \
--alarm-actions arn:aws:sns:us-east-1:111122223333:MyTopic \
--unit Percent
```

# Steps to Create a Dashboard from CLI

[https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/create\\_dashboard.html](https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/create_dashboard.html)

# Notes

If you are an IAM user, you must have Amazon EC2 permissions for some alarm operations:

- The **iam:CreateServiceLinkedRole** permission for all alarms with EC2 actions
- The **iam:CreateServiceLinkedRole** permissions to create an alarm with Systems Manager OpsItem or response plan actions.

Go to IAM and for the particular use provide these permissions.

# Assignment

- **Write a bash script to create a VPC and two subnets namely public subnet and private subnet. The public subnet should be accessible to the internet while the private subnet should only be accessible by resources within the subnet. Launch an instance in the public subnet and another in private subnet.**
  - **Using AWS CloudWatch Console add following metrics to each of the instances and create a dashboard of it.**
    - **X**
    - **Y**
    - **Z**
  - **Using AWS CloudWatch CLI commands add following metrics to each of the instances and create a dashboard of it.**
    - **X**
    - **Y**



# Assignment

- **Write a bash script to create an Ec2 instance. Add a metric and create an alarm for the ec2 instance. Connect the ec2 instance to provide a notification using AWS Simple notification service (SNS).**
-