***Create AWS CloudWatch Alarms for AWS EC2 by using Tags***

It can take a long time to create and configure a standard set of CloudWatch alarms for a large fleet of EC2 instances. This is especially important in large-scale migrations and multi-account situations, where you need to quickly set up a uniform set of alarms for your instances. The method presented here enables you to rapidly and reliably set up a standard set of CloudWatch alarms for new instances, as well as to remove the alarms when the instances are terminated.

The default configuration creates alarms for any Windows, Amazon Linux, Red Hat, Ubuntu, or SUSE Linux EC2 instance with the following metrics:

* CPU Utilization
* CPU Credit Balance (for T Class instances)
* Disk Space (Amazon CloudWatch agent predefined basic metric)
* Memory (Amazon CloudWatch agent predefined basic metric)

**Steps for Deployment of CloudWatchAutoAlarm:**

**Step 01(Optional):** Create an Amazon SNS topic that CloudWatch\_Auto\_Alarms will use for notifications (E-mail, Ticket Creation etc). You can use this sample CloudFormation template (**SNS-topic.yml** from repository).

**Step 02:** Create an S3 bucket that will be used to store and access the CloudWatch\_Auto\_Alarms lambda function deployment package.

**Step 03:** Create a zip file containing the CloudWatchAutoAlarms AWS Lambda function code (**actions.py and cw\_auto\_alarms.py** from repository).

**Step 04:** Copy the **amazon-cloudwatch-auto-alarms.zip** file to your S3 bucket

**Step 05:** Deploy the AWS lambda function using the **CloudWatchAutoAlarms.yaml** CloudFormation template and the deployment package you uploaded to your S3 bucket.

**Launch a new EC2 instance from the Amazon EC2 console**

**Step 01:** Sign in to your AWS account and open the Amazon EC2 console.

**Step 02:** Choose Launch Instance and Choose any AMI from above mentioned list (from Description).

**Step 03:** Choose the t2.micro instance type, and then choose Next: Configure Instance Details.

**Step 04:** Choose a VPC and subnet. Choose a subnet that has internet connectivity so that the CloudWatch agent can connect to the CloudWatch service endpoints.

**Step 05:** For IAM role, Create IAM role having **AmazonSSMManagedInstanceCore**. This allows you to connect to the instance with AWS Systems Manager Session Manager.

**Step 06:** (Only for some Linux and Ubuntu instance) Install SSM agent.

**Step 07:** This installs the required Amazon CloudWatch agent for EC2.

**Step 08:** Choose Next: Add Storage. Keep the defaults, and then choose Next: Add Tags.

**Step 09:** Choose Add Tag and enter **Create\_Auto\_Alarms** for the tag key. Keep the value empty for the Create\_Auto\_Alarms tag key. By adding the tag key, the CloudWatchAutoAlarms Lambda function automatically creates a default alarm set for the EC2 instance.

**Step 10:** Choose Review and Launch, and then choose Launch.

**Step 11:** On Select an existing key pair or create a new key pair, choose Proceed without a key pair.

**Step 12:** Choose Launch Instances.

**Step 13:** Open the Amazon CloudWatch console and confirm on the Alarms page that the alarms are created:

The Alarms page displays alarms created by the CloudWatchAutoAlarms Lambda function.

**The alarms are named using the following format:**

**AutoAlarm-<InstanceId>-<Namespace>-<MetricName>-<Dimensions…>-<ComparisonOperator>-<Threshold>-<Period>**