



Immersion Day

Introduction to Monitoring on AWS



Table of Contents

Overview	3
Create Simple Notification Service (SNS) Topic	4
Launch an Elastic Compute Cloud (EC2) Instance	6
Configure a CloudWatch Alarm.....	10
Appendix A – Monitor Your Estimated Charges Using CloudWatch	13

Overview

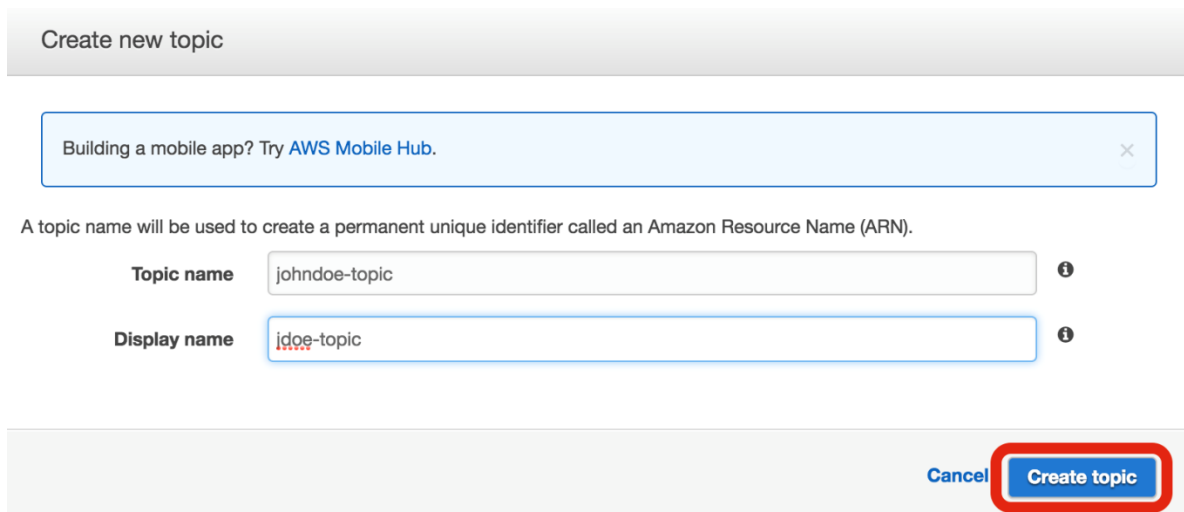
Amazon CloudWatch monitors your Amazon Web Services (AWS) resources and the applications you run on AWS in real-time. You can use CloudWatch to collect and track metrics, which are the variables you want to measure for your resources and applications. CloudWatch alarms send notifications or automatically make changes to the resources you are monitoring based on rules that you define. For example, you can monitor the CPU usage and disk reads and writes of your Amazon Elastic Compute Cloud (Amazon EC2) instances and then use this data to determine whether you should launch additional instances to handle increased load. You can also use this data to stop under-used instances to save money. In addition to monitoring the built-in metrics that come with AWS, you can monitor your own custom metrics. With CloudWatch, you gain system-wide visibility into resource utilization, application performance, and operational health.

In this lab, you will utilize CloudWatch to track EC2 CPU utilization and set up Alarm based on a configured threshold. The Alarm will trigger a Simple Notification Service (SNS) notification. As an optional exercise you will utilize CloudWatch to monitor Billing and send a notification if estimated charges are above a defined threshold.

Create Simple Notification Service (SNS) Topic

In this example we will launch a default Amazon Linux Instance with a simple “stress” tool installed and executed on initialization. The stress tool will generate a simulated workload on the CPU. Before launching the EC2 instance, you will first configure an SNS topic to utilize for the alert.

1. From the AWS console click **Services > SNS**.
2. Under **Common Actions** click **Create Topic**.
3. In the **Topic Name** field , type a name for your topic that includes your name and optionally a **Display Name** and click **Create Topic**.



The screenshot shows the 'Create new topic' form in the AWS SNS console. At the top is a header 'Create new topic'. Below it is a light blue banner with the text 'Building a mobile app? Try [AWS Mobile Hub](#).'. Underneath the banner, a note states: 'A topic name will be used to create a permanent unique identifier called an Amazon Resource Name (ARN)'. There are two input fields: 'Topic name' with the value 'johndoe-topic' and 'Display name' with the value 'jdoe-topic'. Both fields have an information icon to their right. At the bottom right of the form, there are two buttons: 'Cancel' and 'Create topic'. The 'Create topic' button is highlighted with a red rounded rectangle.

4. In the Topic configuration, click **Create Subscription**.

The screenshot shows the AWS SNS console interface. On the left is a navigation menu with 'Topics' selected. The main area is titled 'Topic details: johndoe-topic'. Below this, there are buttons for 'Publish to topic' and 'Other topic actions'. A metadata section shows 'Topic ARN', 'Topic owner', 'Region', and 'Display name'. The 'Subscriptions' section is below, featuring buttons for 'Create subscription' (highlighted with a red box), 'Request confirmations', 'Confirm subscription', and 'Other subscription actions'. A table with columns 'Subscription ID', 'Protocol', 'Endpoint', and 'Subscriber' is shown below the buttons.

5. In the **Protocol** drop down select **Email** and enter a working email address you are able to access. Utilize a non-business email if there may potentially be a spam filter that will block the SNS messages. Click **Create Subscription**.

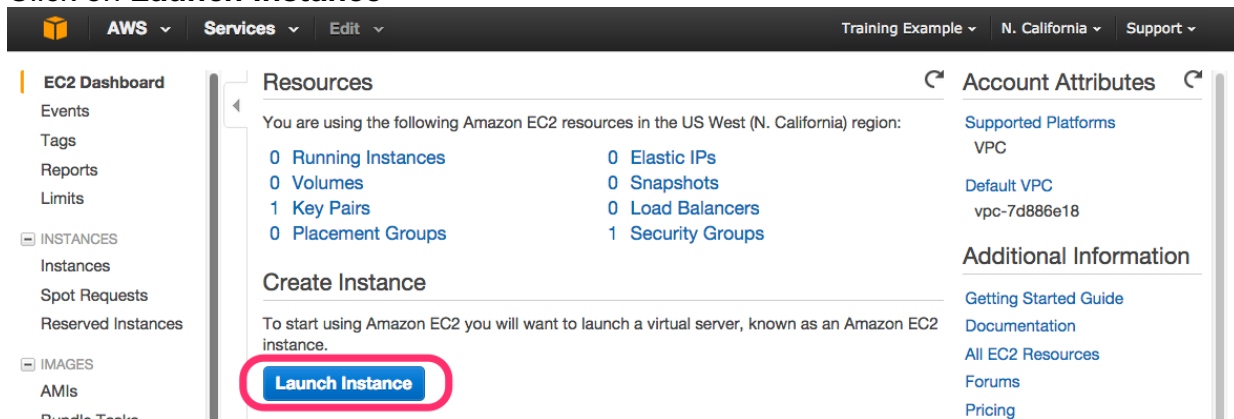
The screenshot shows the 'Create Subscription' form. It has three input fields: 'Topic ARN' with the value 'arn:aws:sns:us-east-1:621444544941:johndoe-topic', 'Protocol' with a dropdown menu showing 'Email', and 'Endpoint' with the value 'johndoe@domain.com'. At the bottom right, there are two buttons: 'Cancel' and 'Create subscription' (highlighted with a red box).

6. A verification email will be sent to your address with the subject "AWS Notification – Subscription Confirmation". Open the email and click the **Confirm Subscription** link.
7. Your subscription should now be active and **not** "PendingConfirmation" under the **Subscriptions** section in the SNS console.

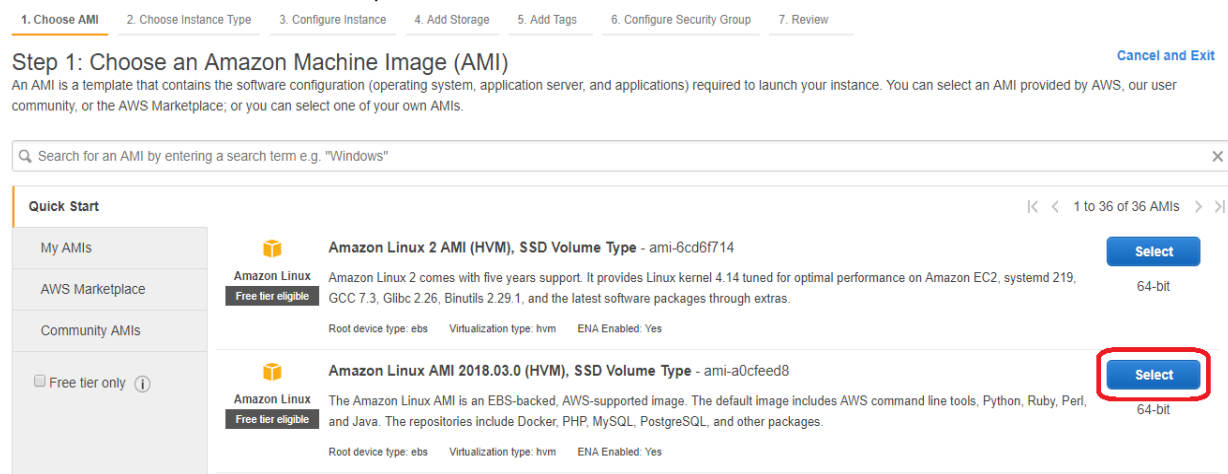
Launch an Elastic Compute Cloud (EC2) Instance

In this step you will launch an EC2 instance and configure the User Data to install and launch the stress tool. The stress tool will begin simulating CPU load 5 minutes after the instance launches to allow you time to configure the CloudWatch Alarm.

1. Click **EC2 Dashboard** towards the top of the left menu.
2. Click on **Launch Instance**



3. In the **Quick Start** section, select the “Amazon Linux AMI” and click **Select**



PLEASE NOTE: You must select “Amazon Linux AMI”, **NOT** “Amazon Linux 2 AMI”! This lab will not work properly if you select Amazon Linux 2.

4. Select the General purpose t2.micro instance type and click **Next: Configure Instance Details**

Introduction to Monitoring on AWS

Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. [Learn more](#) about instance types and how they can meet your computing needs.

Filter by: **All instance types** **Current generation** **Show/Hide Columns**

Currently selected: t2.micro (Variable ECUs, 1 vCPUs, 2.5 GHz, Intel Xeon Family, 1 GiB memory, EBS only)

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
<input checked="" type="checkbox"/>	General purpose	t2.micro <small>Free tier eligible</small>	1	1	EBS only	-	Low to Moderate
<input type="checkbox"/>	General purpose	t2.small	1	2	EBS only	-	Low to Moderate
<input type="checkbox"/>	General purpose	t2.medium	2	4	EBS only	-	Low to Moderate
<input type="checkbox"/>	General purpose	m3.medium	1	3.75	1 x 4 (SSD)	-	Moderate
<input type="checkbox"/>	General purpose	m3.large	2	7.5	1 x 32 (SSD)	-	Moderate
<input type="checkbox"/>	General purpose	m3.xlarge	4	15	2 x 40 (SSD)	Yes	High
<input type="checkbox"/>	General purpose	m3.2xlarge	8	30	2 x 80 (SSD)	Yes	High

[Cancel](#)
[Previous](#)
[Review and Launch](#)
[Next: Configure Instance Details](#)

5. On the **Configure Instance Details** page, expand the **Advanced Details** section at the bottom of the page, and type the following initialization script information (*you can use Shift-Enter to create the necessary line break, or alternatively you could type this into Notepad and copy & paste the results*) into the User Data field (this will automatically install and start the stress tool), confirm “Auto-assign Public IP” is **Enabled** and click **Next: Add Storage**:

```
#!/bin/sh
yum -y update
yum -y install stress
stress -c 1 --backoff 300000000 -t 30m
```

Immersion Day

Introduction to Monitoring on AWS

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Tag Instance 6. Configure Security Group 7. Review

Step 3: Configure Instance Details

Number of instances: 1 [Launch into Auto Scaling Group](#)

Purchasing option: ☐ Request Spot Instances

Network: vpc-6c481d09 (172.31.0.0/16) | default (default) [Create new VPC](#)

Subnet: subnet-3f2d7805 (172.31.0.0/20) | Default in us-east-2 4091 IP Addresses available [Create new subnet](#)

Auto-assign Public IP: ☐ Use subnet setting (Enable)

IAM role: None [Create new IAM role](#)

Shutdown behavior: Stop

Enable termination protection: ☐ Protect against accidental termination

Monitoring: ☐ Enable CloudWatch detailed monitoring [Additional charges apply.](#)

Tenancy: ☐ Shared - Run a shared hardware instance [Additional charges will apply for dedicated tenancy.](#)

Network interfaces

Device	Network Interface	Subnet	Primary IP	Secondary IP addresses
eth0	New network interface	subnet-3f2d7805	Auto-assign	Add IP

[Add Device](#)

Advanced Details

User data: ☐ As text ☐ As file ☐ Input is already base64 encoded

```
#!/bin/bash
yum -y update
yum -y install stress
stress -c 1 --backoff 300000000 -t 30m
```

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Add Storage](#)

6. Click **Next: Tag Instance** to accept the default Storage Device Configuration.

AWS Services Edit Training Example N. California Support

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Tag Instance 6. Configure Security Group 7. Review

Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. [Learn more](#) about storage options in Amazon EC2.

Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Delete on Termination	Encrypted
Root	/dev/xvda	snap-14cff4d5	8	General Purpose (SSD)	24 / 3000	<input checked="" type="checkbox"/>	Not Encrypted

[Add New Volume](#)

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. [Learn more](#) about free usage tier eligibility and usage restrictions.

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Tag Instance](#)

7. Next, choose a “friendly name” for your instance. This name, more correctly known as a tag, will appear in the console once the instance launches. It makes it easy to keep track of running machines in a complex environment. Name yours according to this format: “[Your Name] Server. Then click **Next: Configure Security Group**

- Remove the Security Group rule with by clicking the “x” on the right so there are no rules. (You will not need to connect with this instance). Then click **Review and Launch**

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Tag Instance 6. Configure Security Group 7. Review

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group: ☒ Create a new security group
☐ Select an existing security group

Security group name:
Description:

Type	Protocol	Port Range	Source
This security group has no rules			

[Add Rule](#)

Warning
 You will not be able to connect to this instance as the AMI requires port(s) 22 to be open in order to have access. Your current security group doesn't have port(s) 22 open.

[Cancel](#) [Previous](#) [Review and Launch](#)

- Review your Instance Launch Configuration, and then click **Launch**.

AWS Services Edit Training Example N. California Support

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Tag Instance 6. Configure Security Group 7. Review

Step 7: Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

Improve your instances' security. Your security group, John-Doe-WebTier, is open to the world.
 Your instances may be accessible from any IP address. We recommend that you update your security group rules to allow access from known IP addresses only.
 You can also open additional ports in your security group to facilitate access to the application or service you're running, e.g., HTTP (80) for web servers. [Edit security groups](#)

▼ **AMI Details** [Edit AMI](#)

Amazon Linux AMI 2014.09.1 (HVM) - ami-4b6f650e
 The Amazon Linux AMI is an EBS backed image. It includes the 3.14 kernel, Ruby 2.1, PHP 5.5, PostgreSQL 9.3, Docker 1.2, the AWS command line tools, and repository access to many other packages.
 Root Device Type: ebs Virtualization type: hvm

▼ **Instance Type** [Edit instance type](#)

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
t2.micro	Variable	1	1	EBS only	-	Low to Moderate

▼ **Security Groups** [Edit security groups](#)

Security group name John-Doe-WebTier

[Cancel](#) [Previous](#) [Launch](#)

© 2008 - 2015, Amazon Web Services, Inc. or its affiliates. All rights reserved. [Privacy Policy](#) [Terms of Use](#) [Feedback](#)

- In the drop down choose “Proceed without a keypair” and click **Launch Instances**.

Select an existing key pair or create a new key pair ×

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about [removing existing key pairs from a public AMI](#).

Proceed without a key pair

☒ I acknowledge that I will not be able to connect to this instance unless I already know the password built into this AMI.

Cancel **Launch Instances**

11. Click the **View Instances** button in the lower right-hand portion of the screen to view the list of EC2 instances. Once your instance has launched, you will see your Server as well as the Availability Zone the instance is in.

Configure a CloudWatch Alarm

1. In the EC2 Console, click the checkbox next to your server name to view details about this EC2 instance. Click the **Monitoring** tab and then click **Enable Detailed Monitoring** to provide monitoring data at a 1 minute interval vs. the default of 5 minutes.

Enable Detailed Monitoring ×

Enable detailed monitoring for your instance to get these metrics at 1-minute frequency.
[Learn more](#)

Are you sure you want to enable detailed monitoring for the following instances?
(Additional charges apply.)

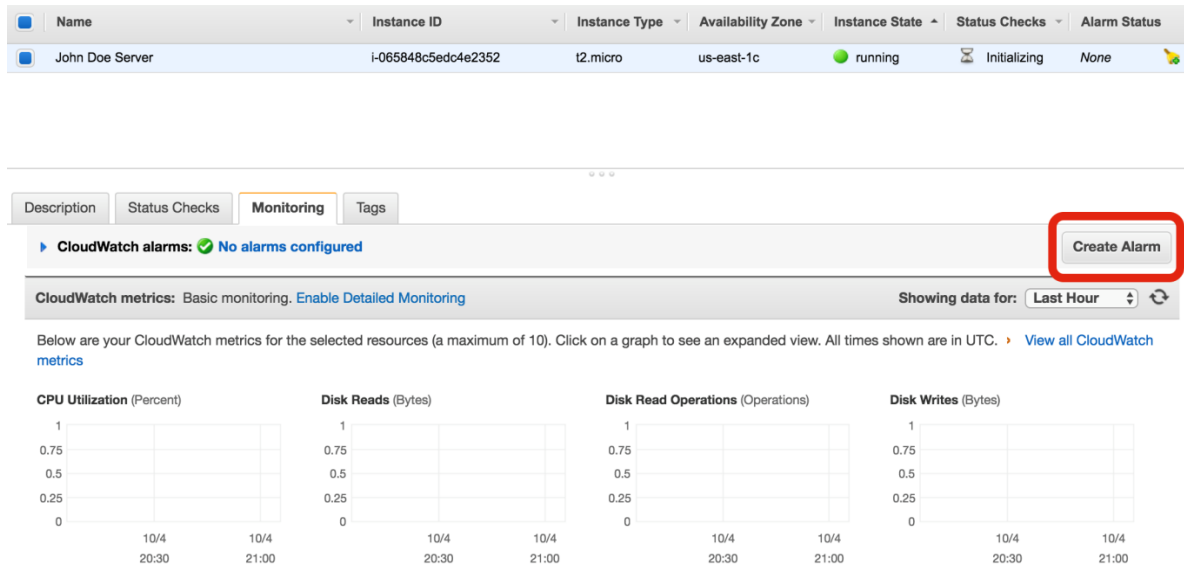
i-0dc7b3f8c2eec8bc7 (John Doe Server)

Cancel **Yes, Enable**

2. Click the **Description** tab and copy your “Instance ID” to the clipboard or other location such as notepad.
3. Click the **Monitoring** tab and click **Create Alarm**.

Immersion Day

Introduction to Monitoring on AWS



- To the right of the “Send a notification to:” drop down, select the SNS Topic you created in the previous step. In the “Whenever:” field, set the **Average** of **CPU Utilization** to “>=” 60%. In the “For at least:” field, set the “Consecutive periods to **1 Minute**.” Add your name to the “Name of alarm:” field and click **Create Alarm**. Note: If 1 minute period is not an option, click the **Description** tab and then click back to the **Monitoring** tab and proceed to set up the Alarm.

The screenshot shows the 'Create Alarm' dialog box in the AWS Management Console. The 'Send a notification to:' field is set to 'johndoe_topic (johndoe@domain.com)'. The 'Take the action:' field has options: Recover this instance, Stop this instance, Terminate this instance, and Reboot this instance. The 'Whenever:' field is set to 'Average of CPU Utilization'. The 'Is:' field is set to '>= 60 Percent'. The 'For at least:' field is set to '1 consecutive period(s) of 1 Minute'. The 'Name of alarm:' field is set to 'johndoe-awsec2-i-0dc7b3f8c2eec8bc7-CPU-Utiliz'. The 'Create Alarm' button is highlighted.

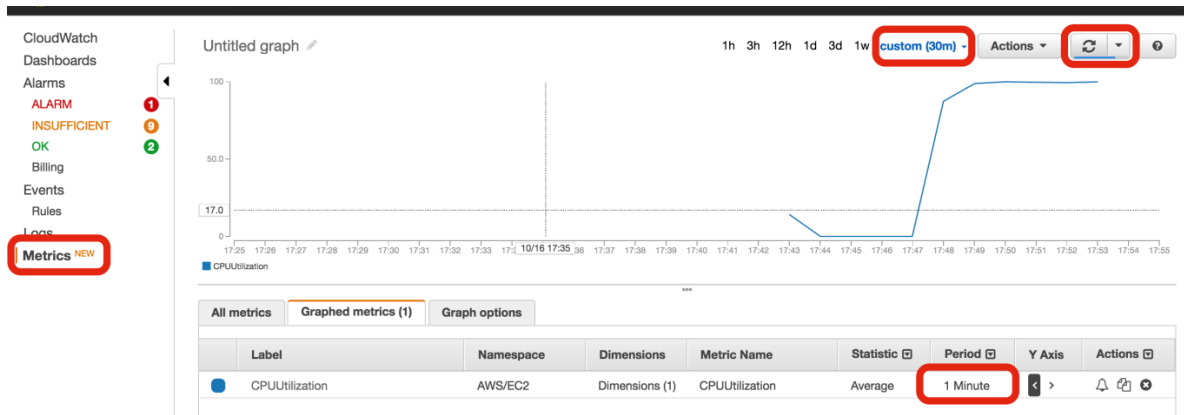
- In the top left area of the AWS Console select **Services > CloudWatch**.
- Click Alarms in the left pane of the Console and check the State of your Alarm.

Immersion Day

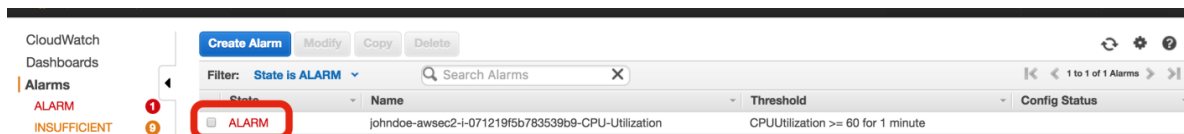
Introduction to Monitoring on AWS



7. In the CloudWatch Console select **Metrics** in the left pane. Select the **All Metrics** tab and paste your Instance ID into the filter. Add an additional filter “cpu”. Select **CPUUtilization** metric. Select the **Graphed metrics** tab and change the **Period** to 1 Minute. Change the graph interval to a custom value of 30m and select Auto refresh of 1min.



8. After 5 minutes, the stress tool will begin to simulate CPU workload and trigger the Alarm once the threshold is reached. You can view the Alarm state in the CloudWatch console under **Alarms**. If you setup an email notification you will receive an email alert when the Alarm is triggered.



Great Job! You have successfully configured a CloudWatch Alarm!!

Appendix A – Monitor Your Estimated Charges Using CloudWatch

In this scenario, you create an Amazon CloudWatch alarm that will monitor your estimated Amazon Web Services (AWS) charges. When you enable the monitoring of estimated charges for your AWS account, the estimated charges are calculated and sent several times daily to CloudWatch as metric data that is stored for 14 days. Billing metric data is stored in the US East (N. Virginia) Region and represents worldwide charges. This data includes the estimated charges for every service in AWS that you use, as well as the estimated overall total of your AWS charges. You can choose to receive alerts by email when charges have exceeded a certain threshold. These alerts are triggered by CloudWatch and messages are sent using Amazon Simple Notification Service (Amazon SNS).

Step 1: Enable Monitoring of Your Estimated Charges

Before you can create an alarm on your estimated charges, you must enable monitoring of your estimated AWS charges, which creates metric data that you can use to create a billing alarm. It takes about 15 minutes before you can view billing data and create alarms. After you enable billing metrics you cannot disable the collection of data, but you can delete any alarms you have created. You must be signed in as the account owner (the "root user") to enable billing alerts for your AWS account.

To enable monitoring of your estimated charges

1. Open the Billing and Cost Management console at <https://console.aws.amazon.com/billing/home?#>.
2. In the spaces provided, enter your user name and password, and then click **Sign in using our secure server**.

3. In the navigation pane, click **Preferences**, and then select the **Receive Billing Alerts** check box.

Dashboard
Bills
Cost Explorer
Budgets
Payment Methods
Payment History
Consolidated Billing
Reports
Preferences
Credits
Tax Settings
DevPay

Preferences ?

☐ **Receive PDF Invoice By Email**
Turn on this feature to receive a PDF version of your invoice by email. Invoices are generally available within the first three days of the month.

☒ **Receive Billing Alerts**
Turn on this feature to monitor your AWS usage charges and recurring fees automatically, making it easier to track and manage your spending on AWS. You can set up billing alerts to receive email notifications when your charges reach a specified threshold. Once enabled, this preference cannot be disabled. [Manage Billing Alerts](#)

☐ **Receive Billing Reports**
Turn on this feature to receive ongoing reports of your AWS charges once or more daily. AWS delivers these reports to the Amazon S3 bucket that you specify where indicated below. For consolidated billing customers, AWS generates reports only for paying accounts. Linked accounts cannot sign up for billing reports.

Save to S3 Bucket:

Step 2: Create a Billing Alarm

After you've enabled monitoring of your estimated AWS charges, you can create a billing alarm in the Amazon CloudWatch console. In this scenario, you'll create an alarm that will send an email message when your estimated charges for AWS exceed \$200. When you enable the monitoring of your estimated charges for the first time, it takes about 15 minutes before you can view billing data and set billing alarms.

To create a billing alarm

1. Open the CloudWatch console at <https://console.aws.amazon.com/cloudwatch/>.
2. If necessary, change the region to US East (N. Virginia). Billing metric data is stored in the US East (N. Virginia) Region and represent worldwide charges. For more information, see [Regions and Endpoints](#).
3. In the navigation pane, click **Alarms**, and then in the **Alarms** pane, click **Create Alarm**.
4. In the **CloudWatch Metrics by Category** pane, under **Billing Metrics**, click **Total Estimated Charge**.

Create Alarm

1. Select Metric2. Define Alarm

Browse Metrics

Search Metrics

CloudWatch Metrics by Category

Your CloudWatch metric summary has loaded. Total metrics: 1,233

Billing Metrics : 49
Total Estimated Charge : 1
By Service : 48
By Linked Account : 3
By Linked Account and Service : 27

DynamoDB Metrics : 4
Table Metrics : 4

EBS Metrics : 72
Per-Volume Metrics : 72

EC2 Metrics : 338**ELB Metrics : 138****ES Metrics : 10**

Update Graph

Time Range

Relative

Absolute

UTC (GMT)

From: 12

hours ago

To: 0

minutes ago

Zoom: 1h | 3h | 6h | 12h | 1d | 3d | 1w | 2w

Left Y-axis

Right Y-axis

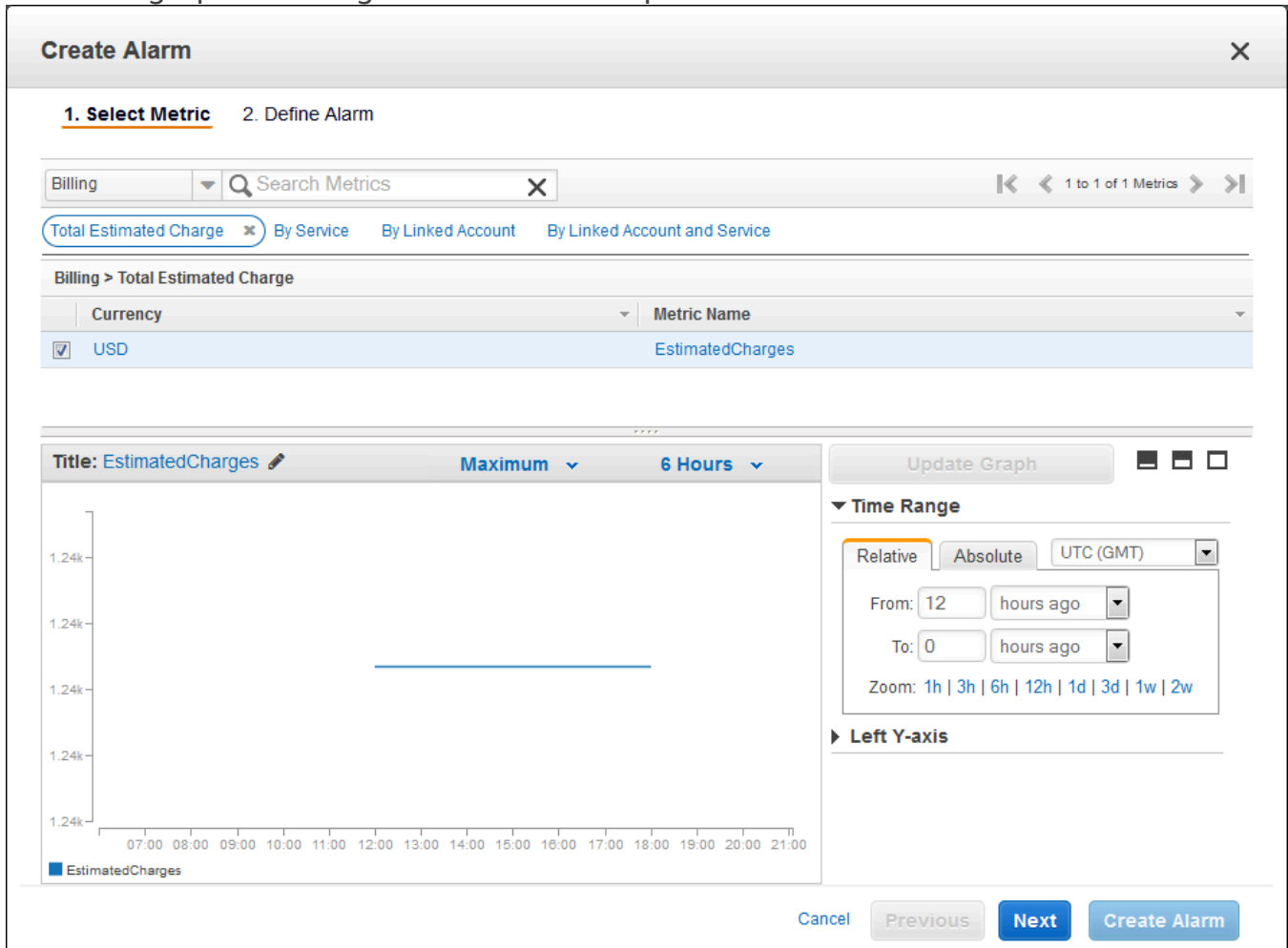
Cancel

Previous

Next

Create Alarm

- Under **Billing > Total Estimated Charge**, select the **EstimatedCharges** metric to view a graph of billing data in the lower pane.



- Click **Next**, and then in the **Alarm Threshold** pane, in the **Name** box, type a unique, friendly name for the alarm (for example, My Estimated Charges).

Create Alarm

1. Select Metric

2. Define Alarm

Alarm Threshold

Provide the details and threshold for your alarm. Use the graph on the right to help set the appropriate threshold.

Name:

Description:

Whenever charges for:

is:

Alarm Preview

This alarm will trigger when the blue line goes up to or above the red line

Namespace:

Currency:

Metric Name:

Actions

Define what actions are taken when your alarm changes state.

Notification

Delete

Whenever this alarm:

Send notification to: [New list](#) [Enter list](#) ⓘ

+ Notification

+ AutoScaling Action

+ EC2 Action

Cancel

Previous

Next

Create Alarm

7. In the **Description** box, enter a description for the alarm (for example, Estimated Monthly Charges).
8. Under **Whenever charges for**, in the **is** drop-down list, select **>=** (greater than or equal to), and then in the **USD** box, set the monetary amount (for example, 200) that must be exceeded to trigger the alarm and send an email.
Note: Under **Alarm Preview**, in the **Estimated Monthly Charges** thumbnail graph, you can see an estimate of your charges that you can use to set an appropriate threshold for the alarm.
9. Under **Actions**, click **Notification**, and then in the **Whenever this alarm** drop-down menu, click **State is ALARM**.
10. In the **Send notification to** box, select an existing Amazon SNS topic.

To create a new Amazon SNS topic, click **Create topic**, and then in the **Send notification to** box, enter a name for the new Amazon SNS topic (for example., CFO),

and in the **Email list** box, enter the email address (for example, john.stiles@example.com) where email notifications should be sent.

Note: If you create a new Amazon SNS topic, the email account associated with the topic will receive a subscription confirmation email. You must confirm the subscription in order to receive future email notifications when the alarm is triggered.

The screenshot shows the 'Create Alarm' console in the AWS CloudWatch service. The interface is divided into two main sections: 'Alarm Threshold' and 'Alarm Preview'.

Alarm Threshold:

- Name:** My Estimated Charges
- Description:** Estimated Monthly Charges
- Whenever charges for:** EstimatedCharges
- is:** \geq USD \$ 200

Actions:

- Notification:** A notification is configured to trigger when the alarm state is 'ALARM'. The notification is sent to the email address john.stiles@example.com.
- Buttons:** + Notification, + AutoScaling Action, + EC2 Action

Alarm Preview:

- Graph:** A line graph titled 'EstimatedCharges >= 200' showing a blue line representing the metric value over time. The y-axis ranges from 0 to 1,500. The x-axis shows dates from 2/06 00:00 to 2/10 00:00. A red horizontal line indicates the threshold at 200. The blue line starts below the threshold and rises above it around 2/08 00:00.
- Text:** This alarm will trigger when the blue line goes up to or above the red line.
- Metadata:** Namespace: AWS/Billing, Currency: USD, Metric Name: EstimatedCharges

Bottom Navigation: Cancel, Previous, Next, Create Alarm

11. Click **Create Alarm**.

Important: If you added an email address to the list of recipients or created a new topic, Amazon SNS sends a subscription confirmation email to each new address shortly after you create an alarm. Remember to click the link contained in that message, which confirms your subscription. Alert notifications are only sent to confirmed addresses.

12. To view your billing alarm in the CloudWatch console, in the navigation pane, under **Alarms**, click **Billing**.

Step 3: Check Alarm Status

Now, check the status of the billing alarm that you just created.

To check alarm status using the CloudWatch console

1. Sign in to the AWS Management Console and open the CloudWatch console at <https://console.aws.amazon.com/cloudwatch/>.
2. If necessary, change the region to US East (N. Virginia). Billing metric data is stored in the US East (N. Virginia) Region and represent worldwide charges. For more information, see [Regions and Endpoints](#).
3. In the navigation pane, under **Alarms**, click **Billing**.

Step 4: Edit a Billing Alarm

Let's say that you want to increase the amount money you spend with AWS each month to \$400. You can edit your existing billing alarm and increase the dollar amount that must be exceeded before the alarm is triggered.

To edit a billing alarm using the CloudWatch console

1. Sign in to the AWS Management Console and open the CloudWatch console at <https://console.aws.amazon.com/cloudwatch/>.
2. If necessary, change the region to US East (N. Virginia). Billing metric data is stored in the US East (N. Virginia) Region and represent worldwide charges. For more information, see [Regions and Endpoints](#).
3. In the navigation pane, under **Alarms**, click **Billing**.
4. In the list of alarms, select the check box next to the alarm you want to change, and then click **Modify**.
5. Under **Alarm Threshold**, in the **USD** box, set the monetary amount (for example, 400) that must be exceeded to trigger the alarm and send an email, and then click **Save Changes**.

Step 5: Delete a Billing Alarm

Now that you have enabled billing, and you have created and edited your first billing alarm, you can delete the billing alarm if you no longer need it.

To delete a billing alarm using the CloudWatch console

1. Sign in to the AWS Management Console and open the CloudWatch console at <https://console.aws.amazon.com/cloudwatch/>.

2. If necessary, change the region to US East (N. Virginia). Billing metric data is stored in the US East (N. Virginia) Region and represent worldwide charges. For more information, see [Regions and Endpoints](#).
3. In the navigation pane, under **Alarms**, click **Billing**.
4. In the list of alarms, select the check box next to the alarm you want to delete, and then click **Delete**.
5. In the **Delete Alarms** dialog box, click **Yes, Delete**.