

INTRODUCTION TO MONITORING ON AWS

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.

- **Part 1:** [Create Simple Notification Service \(SNS\) Topic](#)
- **Part 2:** [Launch an Elastic Compute Cloud \(EC2\) Instance](#)
- **Part 3:** [Configure a CloudWatch Alarm](#)

Part 1: Create Simple Notification Service (SNS) Topic

First, we will set up a topic for notifying our email address that we will then be attaching to our alarm.

1. From the AWS console click Services > [SNS](#).
2. On the left side of the screen, select **Topics** or Click Next Step

Application Integration

Amazon Simple Notification Service

Pub/sub messaging for microservices and serverless applications.

Amazon SNS is a highly available, durable, secure, fully managed pub/sub messaging service that enables you to decouple microservices, distributed systems, and event-driven serverless applications. Amazon SNS provides topics for high-throughput, push-based, many-to-many messaging.

Create topic

Topic name
A topic is a message channel. When you publish a message to a topic, it fans out the message to all subscribed endpoints.

Next step

[Start with an overview](#)

3. The “**Create topic**” opens.
4. For type, select Standard and in the Name field , type a name for your topic that includes your name and optionally a Display Name. Scroll to the bottom of the screen and click “**Create topic**”.

Create topic

Details

Type [Info](#)

Topic type cannot be modified after topic is created

☐ FIFO (first-in, first-out)

- Strictly-preserved message ordering
- Exactly-once message delivery
- High throughput, up to 300 publishes/second
- Subscription protocols: SQS

☒ Standard

- Best-effort message ordering
- At-least once message delivery
- Highest throughput in publishes/second
- Subscription protocols: SQS, Lambda, HTTP, SMS, email, mobile application endpoints

Name

john DOE-topic

Maximum 256 characters. Can include alphanumeric characters, hyphens (-) and underscores (_).

Display name - optional

To use this topic with SMS subscriptions, enter a display name. Only the first 10 characters are displayed in an SMS message. [Info](#)

JohnDoe Topic

Maximum 100 characters, including hyphens (-) and underscores (_).

5. Creating the topic will bring you to the topic's specific dashboard. Click "Create subscription" on the right side of the screen.

Amazon SNS > Topics > john DOE-topic

john DOE-topic

Edit Delete Publish message

Details

Name john DOE-topic	Display name JohnDoe Topic
ARN arn:aws:sns:us-east-1:971183357721:john DOE-topic	Topic owner 971183357721

Subscriptions | Access policy | Delivery retry policy (HTTP/S) | Delivery status logging | Encryption | Tags

Subscriptions (0) Edit Delete Request confirmation Confirm subscription **Create subscription**

Q Search < 1 > ⚙

6. 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"**.

Create subscription

Details

Topic ARN

Protocol

The type of endpoint to subscribe

Email

Endpoint

An email address that can receive notifications from Amazon SNS.

After your subscription is created, you must confirm it. [Info](#)

Subscription filter policy - optional

This policy filters the messages that a subscriber receives. [Info](#)

Redrive policy (dead-letter queue) - optional

Send undeliverable messages to a dead-letter queue. [Info](#)

Cancel

Create subscription

7. 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.
8. Your subscription should now be active and not "PendingConfirmation" under the Subscriptions section in the SNS console.

Amazon SNS

Subscriptions

Dashboard

Topics

Subscriptions

Mobile

Push notifications

Text messaging (SMS)

Subscriptions (1)

Edit Delete Request confirmation Confirm subscription Create subscription

	ID	Endpoint	Status	Protocol	Topic
<input type="radio"/>	7f5a2804-37a3-472d-b03e-fdee2813502c		Confirmed	EMAIL	johndoe-topic

Part 2: 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

The screenshot shows the AWS Management Console interface. On the left is a navigation menu with the following items: **EC2 Dashboard** (marked as 'New'), Events (marked as 'New'), Tags, Limits, **Instances** (expanded), Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts (marked as 'New'), Scheduled Instances, Capacity Reservations, **Images** (expanded), AMIs, **Elastic Block Store** (expanded), Volumes, and Snapshots. The main content area is titled 'Resources' and displays a summary of EC2 resources in the US East (N. Virginia) Region: Running instances (0), Elastic IPs, Dedicated Hosts (0), Snapshots, Volumes (2), Load balancers, Key pairs (2), Security groups, and Placement groups (0). Below this is a blue box with an information icon and text: 'Easily size, configure, and deploy Microsoft SQL Server Always On availability groups on AWS. Launch Wizard for SQL Server. [Learn more](#)'. At the bottom of the main content area is a section titled 'Launch instance' with the text 'To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.' and a prominent orange 'Launch instance' button with a dropdown arrow. A blue arrow points to this button. Below the button is a note: 'Note: Your instances will launch in the US East (N. Virginia) Region'.

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

The screenshot shows the 'Step 1: Choose an Amazon Machine Image (AMI)' screen in the AWS Management Console. At the top, there is a progress bar with seven steps: 1. Choose AMI (active), 2. Choose Instance Type, 3. Configure Instance, 4. Add Storage, 5. Add Tags, 6. Configure Security Group, and 7. Review. Below the progress bar is a search bar with the placeholder text 'Search for an AMI by entering a search term e.g. "Windows"'. To the right of the search bar is a 'Cancel and Exit' link. Below the search bar is a 'Quick Start' section with a list of AMIs. The first AMI, 'Amazon Linux 2 AMI (HVM), SSD Volume Type - ami-04d29b6f966df1537 (64-bit x86) / ami-03156384f702d4eaf (64-bit Arm)', is highlighted with a blue border. It includes a 'Free tier eligible' badge and a description: 'Amazon Linux 2 comes with five years support. It provides Linux kernel 4.14 tuned for optimal performance on Amazon EC2, systemd 219, GCC 7.3, Glibc 2.26, Binutils 2.29.1, and the latest software packages through extras. This AMI is the successor of the Amazon Linux AMI that is approaching end of life on December 31, 2020 and has been removed from this wizard.' Below the description are the details: 'Root device type: ebs', 'Virtualization type: hvm', and 'ENA Enabled: Yes'. To the right of the AMI details is a 'Select' button. Below the 'Select' button are two radio buttons: '64-bit (x86)' (selected) and '64-bit (Arm)'.

4. Select the General purpose **t2.micro** instance type and click **"Next: Configure Instance Details"**.
5. Now we will add a script that will create a test stress script to simulate hits on your instance. Still on the Configure Instance Details page, expand the Advanced Details section at the bottom of the page, and type the following initialization script information into the User Data field (this will automatically install and start the stress tool):

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

6. Click **"Next: Add Storage"**.

Advanced Details

Enclave ☐ Enable

Metadata accessible ☐ Enabled

Metadata version V1 and V2 (token optional)

Metadata token response hop limit 1

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

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

Cancel Previous **Review and Launch** Next: Add Storage

7. Click **"Next: Add Tags"** to accept the default Storage Device Configuration.
8. Click Add Tag. Write "Name" in the Key placeholder. Then choose a reasonable name value 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.

For this lab, you can name yours in this format: **"[Your Name] Server"**. Then click **"Next: Configure Security Group"**.

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

Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver.

A copy of a tag can be applied to volumes, instances or both.

Tags will be applied to all instances and volumes. [Learn more](#) about tagging your Amazon EC2 resources.

Key (128 characters maximum)	Value (256 characters maximum)	Instances	Volumes
Name	JohnDoe Server	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Add another tag (Up to 50 tags maximum)

9. 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. Add Tags 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 ⓘ	Description ⓘ
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.

10. Review your Instance Launch Configuration, and then click Launch.
11. 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
⌵

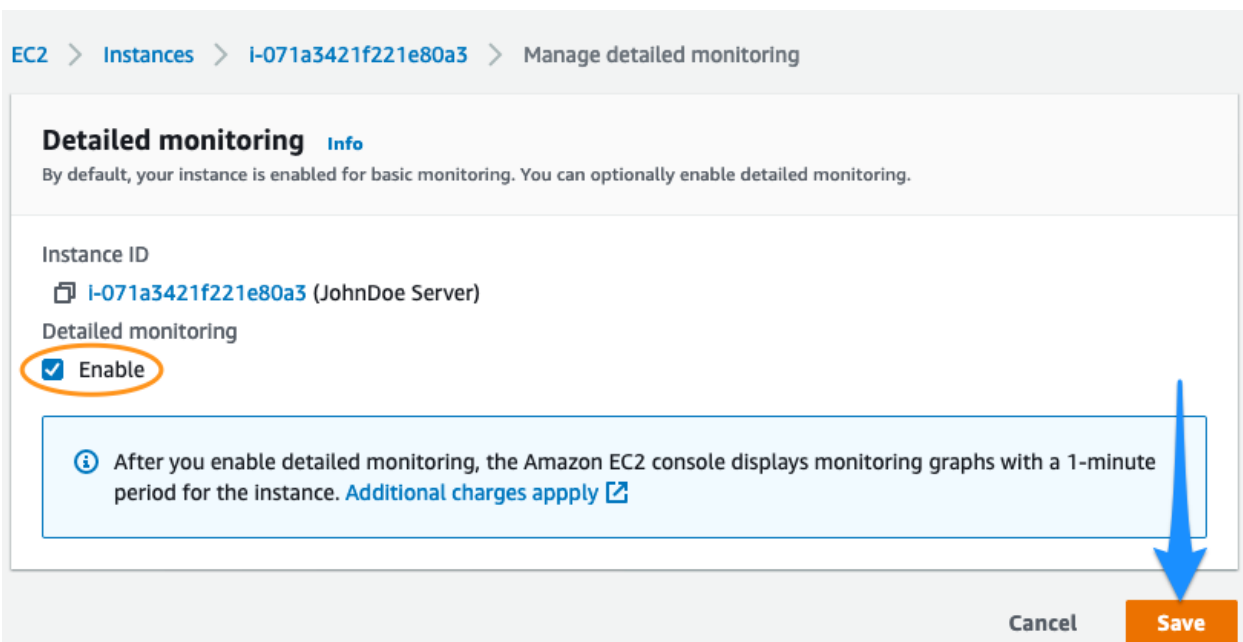
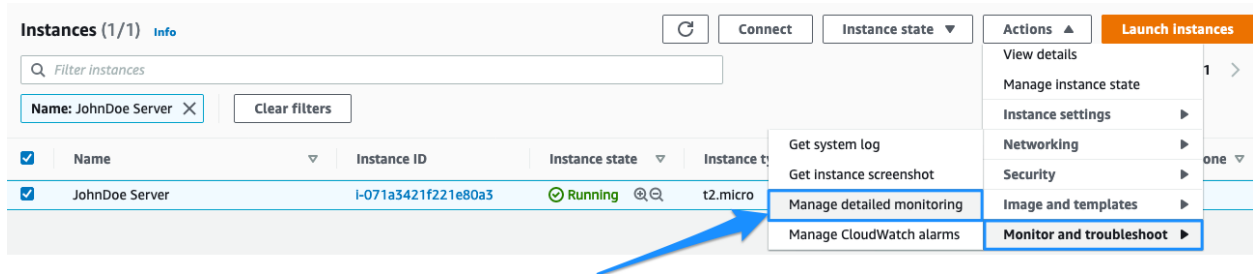
☒ I acknowledge that I will not be able to connect to this instance unless I already know the password built into this AMI.

[Cancel](#)
[Launch Instances](#)

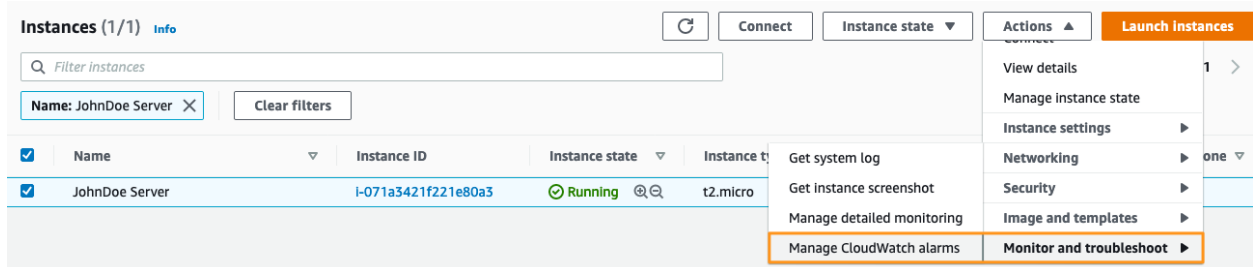
12. Click View Instances button in the lower right-hand portion of the screen to view the list of EC2 instances. Once your instance has launched, you will see your server as well as the Availability Zone the instance is in.

Part 3: 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 Actions » Monitor and troubleshoot » Manage detailed monitoring and then click **“Enable”** under Detailed monitoring to provide monitoring data at a 1 minute interval vs. the default of 5 minutes. Click Save



2. Click the Description tab and copy your “Instance ID” to the clipboard or other location such as a notepad.
3. Click on Actions » Monitor and troubleshoot » Manage CloudWatch alarms.



4. Select **"Create an alarm"**. Under Alarm notification, select the SNS topic created in Part 1.

EC2 > Instances > i-071a3421f221e80a3 > Manage CloudWatch alarms

Manage CloudWatch alarms [Info](#)

Create or edit a CloudWatch alarm that monitors CloudWatch metrics for the instance.

Add or edit alarm [Info](#)

You can create a new alarm or edit an existing alarm.

☒ **Create an alarm**
Create an alarm for i-071a3421f221e80a3

☐ **Edit an alarm**
Edit an existing alarm for i-071a3421f221e80a3

Search for alarm

Find an alarm to modify

Alarm notification [Info](#)

Configure the alarm to send notifications to an Amazon SNS topic when it is triggered. ☒

5. In the **"Alarm thresholds"** section, set the values as shown below and then click **"Create"**.

Alarm thresholds

Specify the metric thresholds for the alarm.

Group samples by

Average

Type of data to sample

CPU utilization

Alarm when

>=

Percent

60

Consecutive period

1

Period

5 Minutes

Alarm name

awsec2-i-071a3421f221e80a3-GreaterThanOrEqualToThreshold-CPUUtilization

Sample metric data [Info](#)

Sample metric data for i-071a3421f221e80a3

Add to dashboard

1h

3h

12h

1d

3d

1w



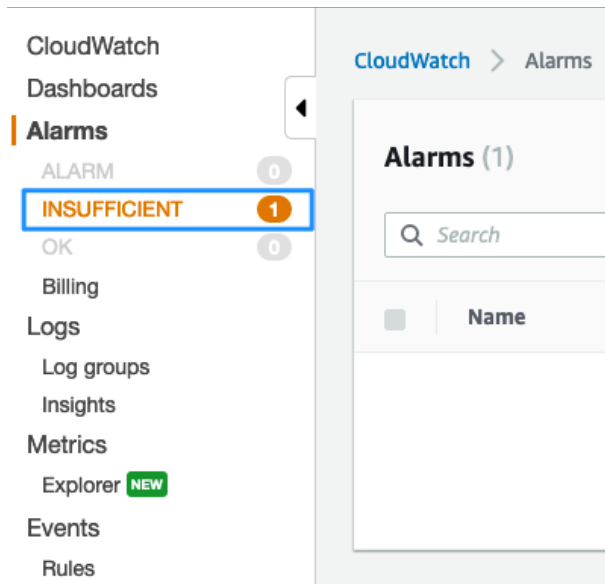
CPU utilization (Average)



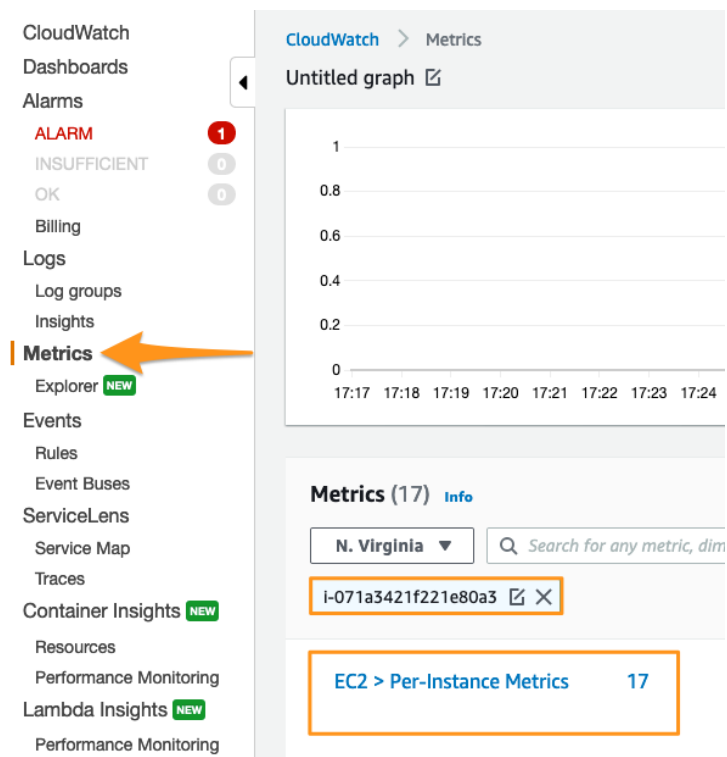
Cancel

Create

6. In the top left area of the AWS Console select Services > [CloudWatch](#).
7. Click Alarms in the left pane of the Console and check the State of your alarm. It most likely says INSUFFICIENT_DATA because you just created it.



8. In the CloudWatch Console select Metrics in the left pane. Select the All Metrics tab and paste your Instance ID into the filter.



9. Click on Per-Instance Metrics and then add an additional filter "CPU".

Metrics (5) [Info](#)

N. Virginia All > EC2 > Per-Instance Metrics

☒ I-071a3421f221e80a3 ☒ cpu ☐

<input type="checkbox"/>	Instance Name (5)	InstanceId	Metric Name
<input checked="" type="checkbox"/>	JohnDoe Server	I-071a3421f221e80a3 ▾	CPUUtilization ▾
<input type="checkbox"/>	JohnDoe Server	I-071a3421f221e80a3 ▾	CPUCreditUsage ▾
<input type="checkbox"/>	JohnDoe Server	I-071a3421f221e80a3 ▾	CPUCreditBalance ▾
<input type="checkbox"/>	JohnDoe Server	I-071a3421f221e80a3 ▾	CPUSurplusCreditBalance ▾
<input type="checkbox"/>	JohnDoe Server	I-071a3421f221e80a3 ▾	CPUSurplusCreditsCharged ▾

10. Select “CPUUtilization” metric. Click on “Graphed metrics” button and change the Period to 1 Minute. Change the graph interval to a custom value of 30m and select Auto refresh of 1min.

CloudWatch > Metrics

Untitled graph ☒ 1h 3h 12h 1d 3d 1w Custom (30m) Line Actions

Percent

100

50

0

17:14 17:15 17:16 17:17 17:18 17:19 17:20

■ CPUUtilization

Graphed metrics (1) Graph options

Add math expression ▾ Add dynamo

Clear Cancel Apply

Period: 1 Minute

Clear graph

<input checked="" type="checkbox"/>	Label	Details	Statistic	Period	Y Axis	Actions
<input checked="" type="checkbox"/>	CPUUtilization	EC2 • CPUUtilization • InstanceId: I-07...	Average ▾	1 Minute ▾		<input type="button" value="Add Metrics"/>

11. 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.

CloudWatch

Dashboards

Alarms

ALARM

INSUFFICIENT

OK

Billing

Logs

Log groups

Insights

CloudWatch > Alarms

Alarms (1) ☐ Hide Auto Scaling alarms

<input type="checkbox"/>	Name	State
<input type="checkbox"/>	awsec2-i-05930744e15e6f7f1-CPU-Utilization	⚠ In alarm

Congratulations!! You have successfully configured a CloudWatch Alarm!

Clean Up: Be sure to delete the following resources after you are finished:

- Select Delete on your alarm after you are finished.
- Stop and terminate your EC2 instance.
- Delete your SNS topic.

