

Edge Computing Observability

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.

Note: You will need an AWS account and the associated administrative login credentials used in our experiments.

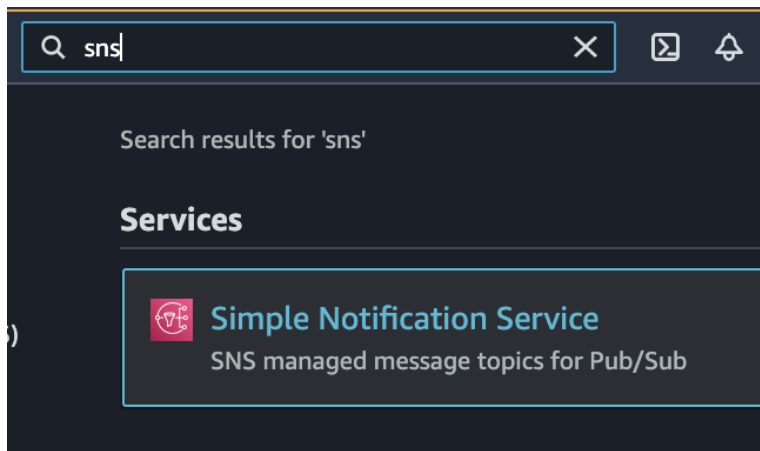
Sign in to AWS

Open the console link provided for your AWS account in `us-east-1.console.aws.amazon.com`

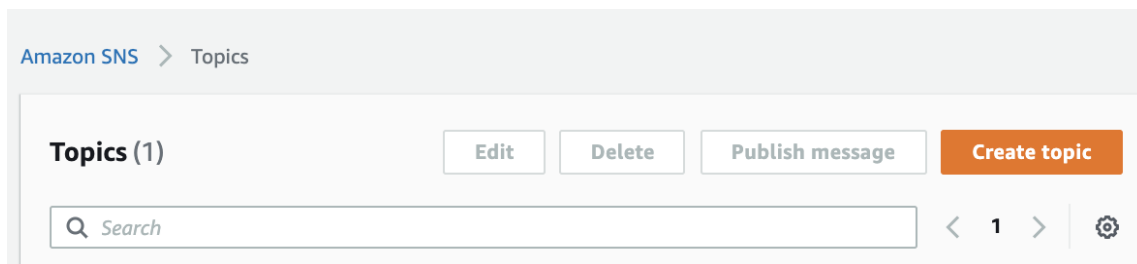
Create Simple Notification Service (SNS) Topic

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

1. Navigate to the SNS service.



2. On the left side of the screen, select Topics.
3. Click “Create topic”



4. Choose Standard for the Topic Type. In the Name field , type a name for your topic that includes your name and optionally a Display Name of Monitoring Topic for Experiment. Scroll to the bottom of the screen and click “Create topic”

Amazon SNS > Topics > 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

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](#)

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

5. Creating the topic will bring you to the topic's specific dashboard.

✓ Topic geoniece-topic created successfully.

You can create subscriptions and send messages to them from this topic.

[Publish message](#)


Amazon SNS > Topics > geoniece-topic

geoniece-topic

[Edit](#)
[Delete](#)
[Publish message](#)

Details

Name

geoniece-topic

ARN

arn:aws:sns:us-east-1:124926150123:geoniece-topic

Type

Standard

Display name

Monitoring Topic for Experiment

Topic owner

124926150123

Create Subscription

1. Click “Create subscription” on the right side of the screen.

geoniece-topic

EditDeletePublish message

Details

Name geoniece-topic	Display name Monitoring Topic for Experiment
ARN arn:aws:sns:us-east-1:124926150123:geoniece-topic	Topic owner 124926150123
Type Standard	

Subscriptions

Access policy

Delivery retry policy (HTTP/S)

Delivery status logging

Encryption

Tags

Subscriptions (0)

EditDeleteRequest confirmationConfirm subscription

Create subscription

2. 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.

[Amazon SNS](#) > [Subscriptions](#) > Create subscription

Create subscription

Details

Topic ARN

Protocol


The type of endpoint to subscribe

Endpoint

An email address that can receive notifications from Amazon SNS.

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

- The subscription should show the created messaging.

 **Subscription to geoniece-topic created successfully.**
The ARN of the subscription is arn:aws:sns:us-east-1:124926150123:geoniece-topic:d567bba5-b27a-4abb-bfd3-24153324cb79.

[Amazon SNS](#) > [Topics](#) > [geoniece-topic](#) > Subscription: d567bba5-b27a-4abb-bfd3-24153324cb79

Subscription: d567bba5-b27a-4abb-bfd3-24153324cb79

[Edit](#)[Delete](#)

- Click on the topic name in the breadcrumb navigation.
- Scroll to the subscription section, and our new subscription will be displayed with the status Pending

Subscriptions (1)				
<div> <div>Edit</div> <div>Delete</div> <div>Request confirmation</div> <div>Confirm subscription</div> </div> <div>Create subscription</div>				
<div> <div>Q Search</div> <div>< 1 ></div> <div>⚙</div> </div>				
ID	Endpoint	Status	Protocol	
<div>○</div> <div>Pending confirmation</div>	george.niece@digitaltransformationstrategies.net	<div>⌚</div> <div>Pending confirmation</div>	EMAIL	

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.

AWS Notification - Subscription Confirmation External Inbox x

Monitoring Topic for Experiment <no-reply@sns.amazonaws.com>

to me ▼

You have chosen to subscribe to the topic:

arn:aws:sns:us-east-1:124926150123:geoniece-topic

To confirm this subscription, click or visit the link below (If this was in error no action is necessary):

[Confirm subscription](#)

Please do not reply directly to this email. If you wish to remove yourself from receiving all future SNS subscription confirmations, please contact your account manager.

7. Your subscription should now be Status “Confirmed” and not “PendingConfirmation” under the Subscriptions section in the SNS console.

Subscriptions

Access policy

Delivery retry policy (HTTP/S)

Delivery status logging

Encryption

Tags

Subscriptions (1)

Edit

Delete


Request confirmation



Confirm subscription

Create subscription

Q Search

< 1 >

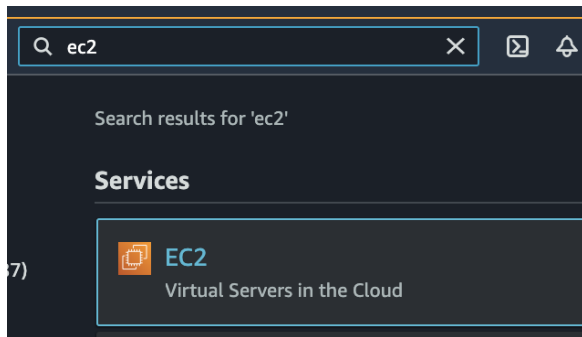


	ID ▾	Endpoint ▾	Status ▾	Protocol ▲
	d567bba5-b27a-4abb-bfd3-24153324cb79	george.niece@digitaltransformationstrategies.net	 Confirmed	EMAIL

Launch Elastic Compute Cloud (EC2) Instance/VM

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. Navigate to the EC2 Service through the service menu.



2. Click on Launch Instance

Resources

You are using the following Amazon EC2 resources in the US East (N. Virginia) Region:

Instances (running)	0	Dedicated Hosts	0
Elastic IPs	1	Instances	1
Key pairs	2	Load balancers	1
Placement groups	0	Security groups	7
Snapshots	0	Volumes	1


Launch instance

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

Launch instance ▼

Note: Your instances will launch in the US East (N. Virginia) Region

3. In the Choose AMI section, select the “Amazon Linux 2 AMI” and (x86) radio input and click Select



Amazon Linux 2 AMI (HVM), SSD Volume Type - ami-0dc2d3e4c0f9ebd18 (64-bit x86) / ami-008a8487adc2b32ec (64-bit Arm)

Free tier eligible


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.

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

Select

☒ 64-bit (x86)
☐ 64-bit (Arm)

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



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 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 Free tier eligible	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. 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 -y install stress
stress --cpu 1
```

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

Step 3: Configure Instance Details

Additional charges will apply for dedicated tenancy.

Elastic Inference ⓘ ☐ Add an Elastic Inference accelerator
Additional charges apply.

Credit specification ⓘ ☐ Unlimited
Additional charges may apply.

File systems ⓘ [Add file system](#) [Create new file system](#)

▼ **Advanced Details**

Enclave ⓘ ☐ Enable

Metadata accessible ⓘ

Metadata version ⓘ

Metadata token response hop limit ⓘ

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

```
#!/bin/sh
yum -y update
amazon-linux-extras install epel -y
yum -y install stress
stress --cpu 1
```

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

6. Click Next: Add Storage

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 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. You can edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volume options in Amazon EC2.

Volume Type ⓘ	Device ⓘ	Snapshot ⓘ	Size (GiB) ⓘ	Volume Type ⓘ	IOPS ⓘ	Throughput (MB/s) ⓘ	Delete on Termination ⓘ
Root	/dev/xvda	snap-053c42bdb1128764a	<input type="text" value="8"/>	General Purpose GP ⓘ	100 / 3000	N/A	<input checked="" type="checkbox"/>
Add New Volume							

7. On the Add Storage we note options that are very important for data considerations. Note that Delete on Termination is specified. That means that this instance will have the disk deleted if it were terminated. In the case, where an instance backing store needed to be saved when the instance attached to it is deleted we'd uncheck this option. We'll leave it default for our experiment. The other option noted is the Encryption. We won't encrypt this disk since it will be ephemeral and have nothing of note on it for our experiment.

Introduction to Observability on AWS

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 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.

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encryption
Root	/dev/xvda	snap-053c42bdb1128764a	8	General Purpose	100 / 3000	N/A	<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 restrictions.

KMS Key Aliases	KMS Key ID
Not Encrypted (default) aws/ebs	alias/aws/ebs

8. Click Next: Add Tags to accept the default Storage Device Configuration.

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	Value	Instances
(128 characters maximum)	(256 characters maximum)	

This resource currently has no tags

Choose the [Add tag](#) button or [click to add a Name tag](#).

Make sure your [IAM policy](#) includes permissions to create tags.

[Add Tag](#) (Up to 50 tags maximum)

9. Click Add Tag.

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

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 = Webserve. 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)
Name	geoniece Server

Add another tag (Up to 50 tags maximum)

10. Write “Name” in the Key input. Then choose a reasonable 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. Note that this action will tag instances, volumes, and network interfaces for this virtual machine.

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

11. Leave the security group as noted. We’ll launch without a keypair which will only allow this instance to be connected with EC2 Connect through the console and not directly from outside via SSH. 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, 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 also 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: launch-wizard-6

Description: launch-wizard-6 created 2021-07-18T09:02:51.620-05:00

Type ⓘ	Protocol ⓘ	Port Range ⓘ	Source ⓘ
SSH ▼	TCP	22	Custom ▼ 0.0.0.0/0

Add Rule



Warning

Rules with source of 0.0.0.0/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow

12. Review your Instance Launch Configuration, and then click Review Launch.

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](#)

13. 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.](#)


☒ I acknowledge that without a key pair, I can connect to this instance only by using EC2 Instance Connect or if I know the password built into the AMI. Note that EC2 Instance Connect is only supported on Amazon Linux 2 and Ubuntu. [Learn more.](#)


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

14. 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.


Instances (1) [Info](#)  [Connect](#) [Instance state ▼](#) [Actions ▼](#) [Launch instances](#)

< 1 >


search: i-0a8e45e824d7e59d6  [Clear filters](#)


<input type="checkbox"/>	Name	Instance ID	Instance state ▼	Instance type
<input type="checkbox"/>	geoniece Server	i-0a8e45e824d7e59d6	 Pending	t2.micro

15. If the instance is Pending, wait a minute or two and click the refresh until you see the instance state as Running


Instances (1) [Info](#)  [Connect](#) [Instance state ▼](#) [Actions ▼](#) [Launch instances](#)

< 1 >


search: i-0a8e45e824d7e59d6  [Clear filters](#)


<input type="checkbox"/>	Name	Instance ID	Instance state ▼	Instance type
<input type="checkbox"/>	geoniece Server	i-0a8e45e824d7e59d6	 Running	t2.micro

16. Copy the Instance ID and save that in a text file or other location, as we'll need that later in the experiment to configure our CloudWatch Alarm.

Instances (1/1) [Info](#)  [Connect](#) [Instance state ▼](#) [Actions ▼](#) [Launch instances](#)

< 1 >

search: i-0a8e45e824d7e59d6  [Clear filters](#)

<input checked="" type="checkbox"/>	Name	Instance ID	Instance state ▼	Instance type
<input checked="" type="checkbox"/>	geoniece Server	i-0a8e45e824d7e59d6	 Running	t2.micro

Configure a CloudWatch Alarm

1. In the EC2 Console, click the checkbox next to your server name to view details about this EC2 instance.

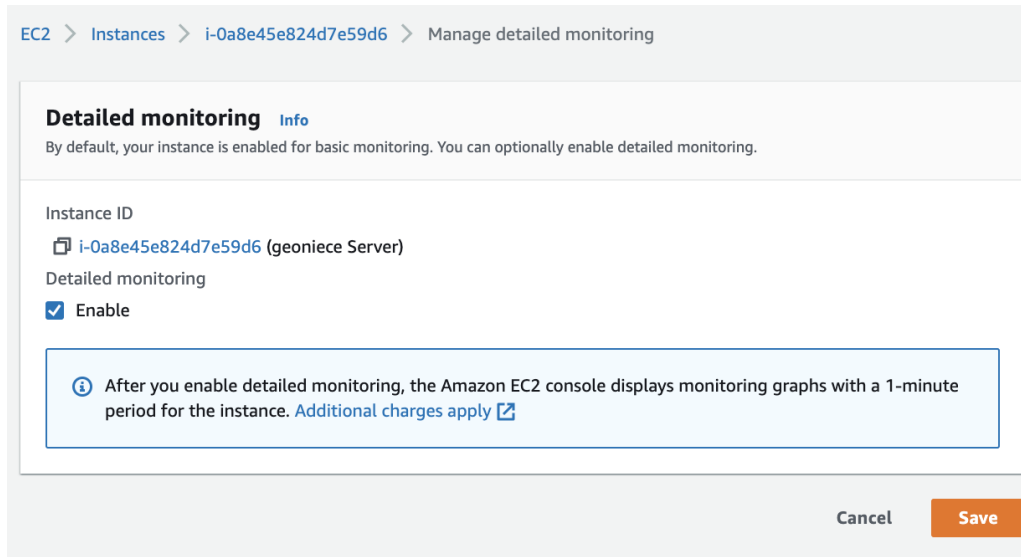
The screenshot shows the AWS EC2 console 'Instances' page. At the top, there are buttons for 'Connect', 'Instance state', 'Actions', and 'Launch instances'. A search bar contains 'Filter instances'. Below it, a filter box shows 'search: i-0a8e45e824d7e59d6' and a 'Clear filters' button. The instance list table has columns: Name, Instance ID, Instance state, and Instance type. One instance is listed: 'geoniece Server' with ID 'i-0a8e45e824d7e59d6', state 'Running' (indicated by a green checkmark), and type 't2.micro'.

<input checked="" type="checkbox"/>	Name	Instance ID	Instance state	Instance type
<input checked="" type="checkbox"/>	geoniece Server	i-0a8e45e824d7e59d6	Running	t2.micro

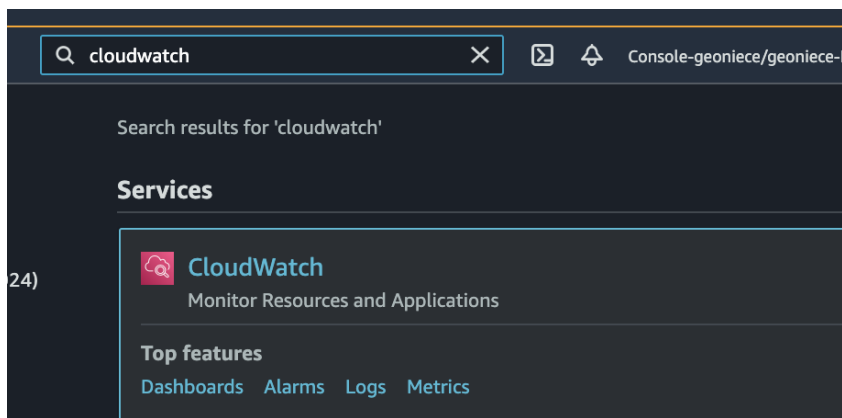
2. Click the Monitoring tab and then click Manage detailed monitoring.

The screenshot shows the 'Monitoring' tab for the selected EC2 instance. The instance name is 'i-0a8e45e824d7e59d6 (geoniece Server)'. Below the instance name, there are tabs for 'Details', 'Security', 'Networking', 'Storage', 'Status checks', 'Monitoring' (which is active), and 'Tags'. In the 'Monitoring' tab, there is a 'Manage detailed monitoring' button. At the bottom, there is an 'Add to dashboard' button and a time range selector with options: '1h', '3h', '12h', '1d', '3d', '1w', and 'custom'. There are also refresh and dropdown icons.

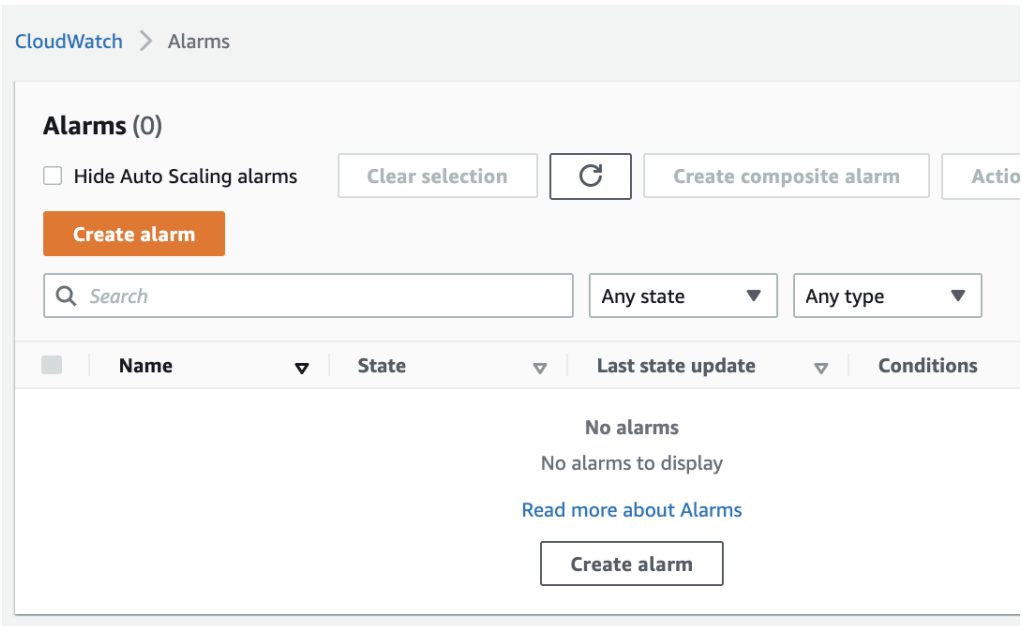
3. Enable Detailed Monitoring by checking Enable checkbox and choosing Save. This will update the CloudWatch configuration to provide monitoring data at a 1 minute interval vs. the default of 5 minutes.



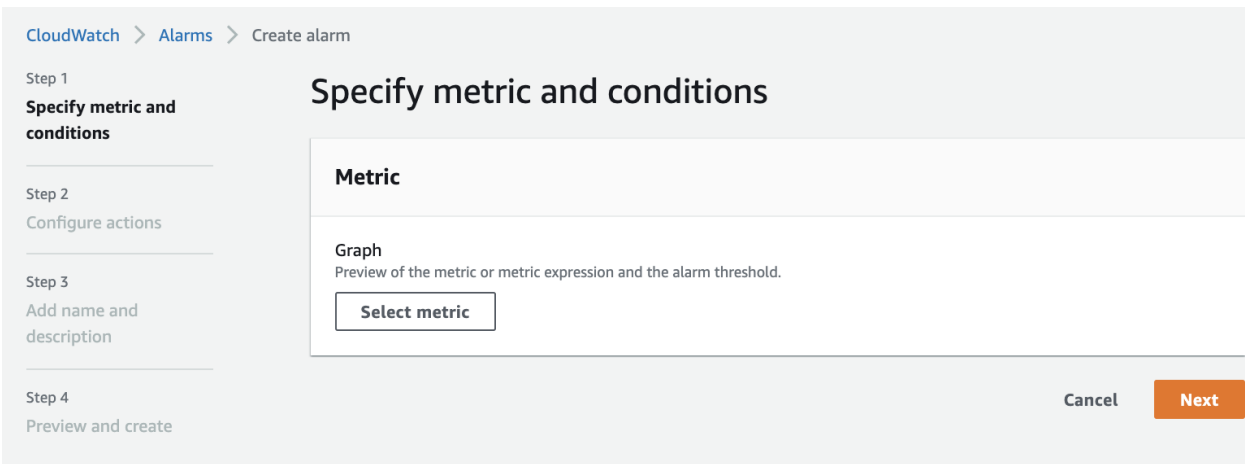
4. Navigate to the Cloud Alarms console



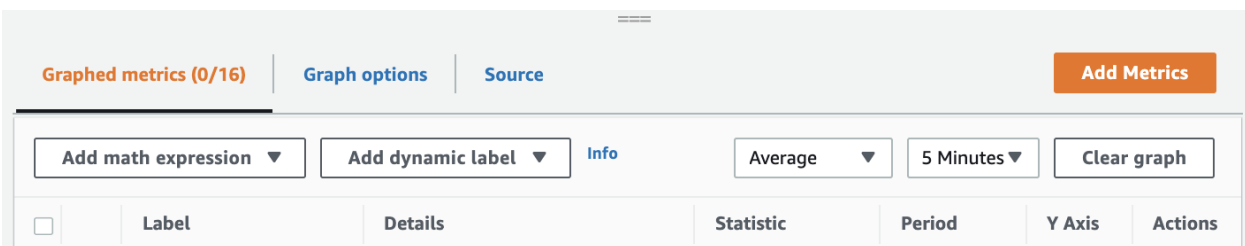
5. Click Create Alarm. If you don't see Create Alarm you need to choose Alarms in the left navigation pane for CloudWatch.



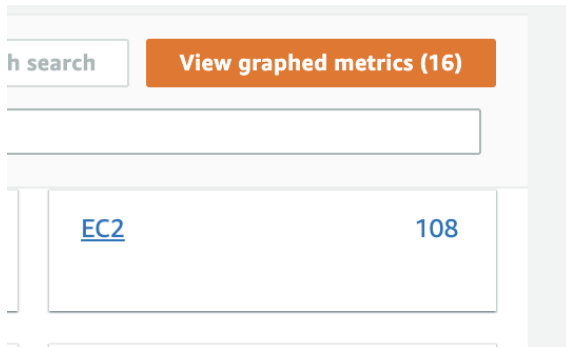
6. Choose Select metric.



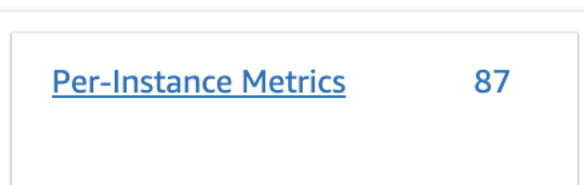
7. Choose Add metrics



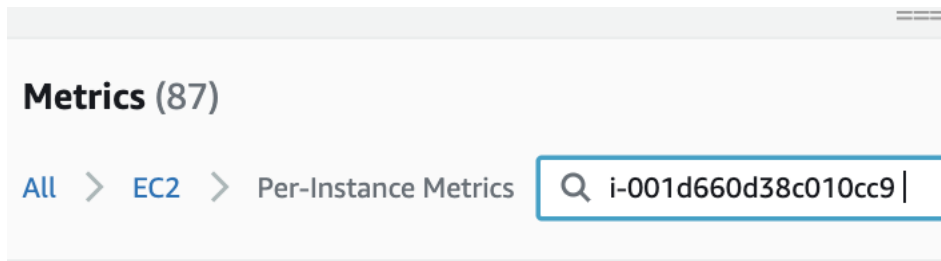
8. Choose EC2 for the metric type



9. Choose Per-instance Metrics



10. Paste the instance ID name we saved earlier.



11. Select the checkbox for CPU Utilization as our metric to monitor for this alarm. Choose Select metric.

Metrics (17) Graph se

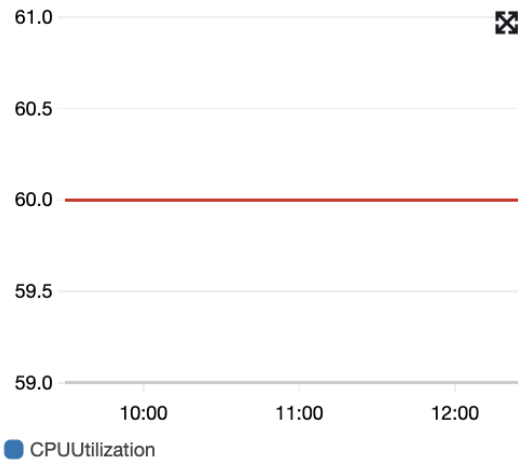
All > EC2 > Per-Instance Metrics

<input type="checkbox"/>	Instance Name (17)	InstanceId	Metric
<input checked="" type="checkbox"/>	geoniece Server	i-001d660d38c010cc9 ▼	CPUUtili
<input type="checkbox"/>	geoniece Server	i-001d660d38c010cc9 ▼	Networ
<input type="checkbox"/>	geoniece Server	i-001d660d38c010cc9 ▼	Networ

12. Change the Statistic to Average. For Period select 1 minute.

Metric Edit

Graph
This alarm will trigger when the blue line goes above the red line for 1 datapoints within 1 minute.



Namespace
AWS/EC2

Metric name

InstanceId

Instance name
geoniece Server

Statistic

Period

13. Scroll to the Conditions section. Choose Static for the Threshold type, Greater/Equal for the alarm condition for our CPUUtilization metric, and make the threshold value 60.

Conditions

Threshold type

☒ **Static**
Use a value as a threshold

☐ **Anomaly detection**
Use a band as a threshold

Whenever CPUUtilization is...
Define the alarm condition.

☐ **Greater**
> threshold

☒ **Greater/Equal**
≥ threshold

☐ **Lower/Equal**
≤ threshold

☐ **Lower**
< threshold

than...
Define the threshold value.

Must be a number

► **Additional configuration**

Cancel Next

14. Now our Metric configuration will reflect the 60% CPU configuration on our metric graph.
15. On the Configure actions screen we update the Notification to use our SNS Topic that we created in an earlier section of this experiment. For notification chose “In alarm”. Choose the “Select and existing SNS Topic”. To the right of the “Send a notification to:” drop down, select the SNS Topic you created in the earlier section. Choose Next.

16. Add your Alarm name, for our experiment we should name it in the format `name-cpu-alarm` and enter an Alarm description. Choose Next

Notification

Alarm state trigger
Define the alarm state that will trigger this action.

☒ **In alarm**
The metric or expression is outside of the defined threshold.

☐ **OK**
The metric or expression is within the defined threshold.

☐ **Insufficient data**
The alarm has just started or not enough data is available

Select an SNS topic
Define the SNS (Simple Notification Service) topic that will receive the notification.

☒ **Select an existing SNS topic**
☐ Create new topic
☐ Use topic ARN

Send a notification to...

Only email lists for this account are available.

Email (endpoints)
george.niece@digitaltransformationstrategies.net - [View in SNS Console](#)

Add notification

17. Add your Alarm name, for our experiment we should name it in the format ***name-cpu-alarm*** field and enter an Alarm description. Choose Next

Add name and description

Name and description

Alarm name

Alarm description - optional

Alarm for CPU utilization >= 60% in 1 minute intervals

Up to 1024 characters (54/1024)

Cancel

Previous

Next

18. On Preview and create screen choose Create alarm

Preview and create

Step 1: Specify metric and conditions Edit

Metric

Graph
This alarm will trigger when the blue line goes above the red line for 1 datapoints within 1 minute.

Percent

60.00

40.00

20.00

0

10:00 11:00 12:00

CPUUtilization

Namespace
AWS/EC2

Metric name
CPUUtilization

InstanceId
i-0a8e45e824d7e59d6

Instance name
geoniece Server

Statistic
Average

Copyright 2021, Innovation in Software, All Rights Reserved

Page 22

Preview and create

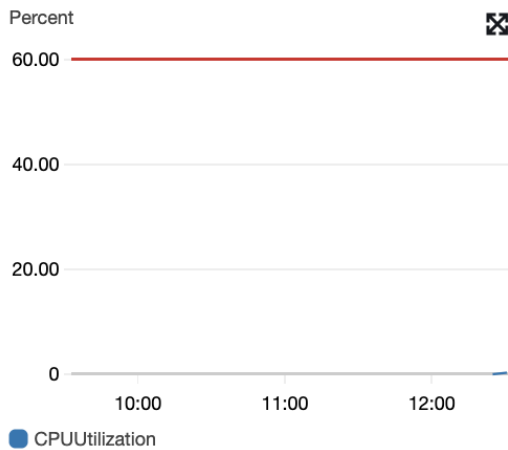
Step 1: Specify metric and conditions

[Edit](#)

Metric

Graph

This alarm will trigger when the blue line goes above the red line for 1 datapoints within 1 minute.



Namespace

AWS/EC2

Metric name

CPUUtilization

InstanceId

i-0a8e45e824d7e59d6

Instance name

geoniece Server

Statistic

Average

19. Our Alarm should be created.

✓ Successfully created alarm **geoniece-cpu-alarm**. View alarm ✕

ⓘ Some subscriptions are pending confirmation
Amazon SNS doesn't send messages to an endpoint until the subscription is confirmed View SNS Subscriptions ✕

CloudWatch > Alarms

Alarms (1)

☐ Hide Auto Scaling alarms Clear selection ↻ Create composite alarm Actions ▼

Create alarm

Any state ▼ Any type ▼ < 1 > ⚙

<input type="checkbox"/>	Name ▼	State ▼	Last state update ▼	Conditions
<input type="checkbox"/>	geoniece-cpu-alarm	ⓘ Insufficient data	2021-07-18 07:33:48	CPUUtilization >= 60 for 1 datapoints with minute

Validate our CloudWatch Alarm

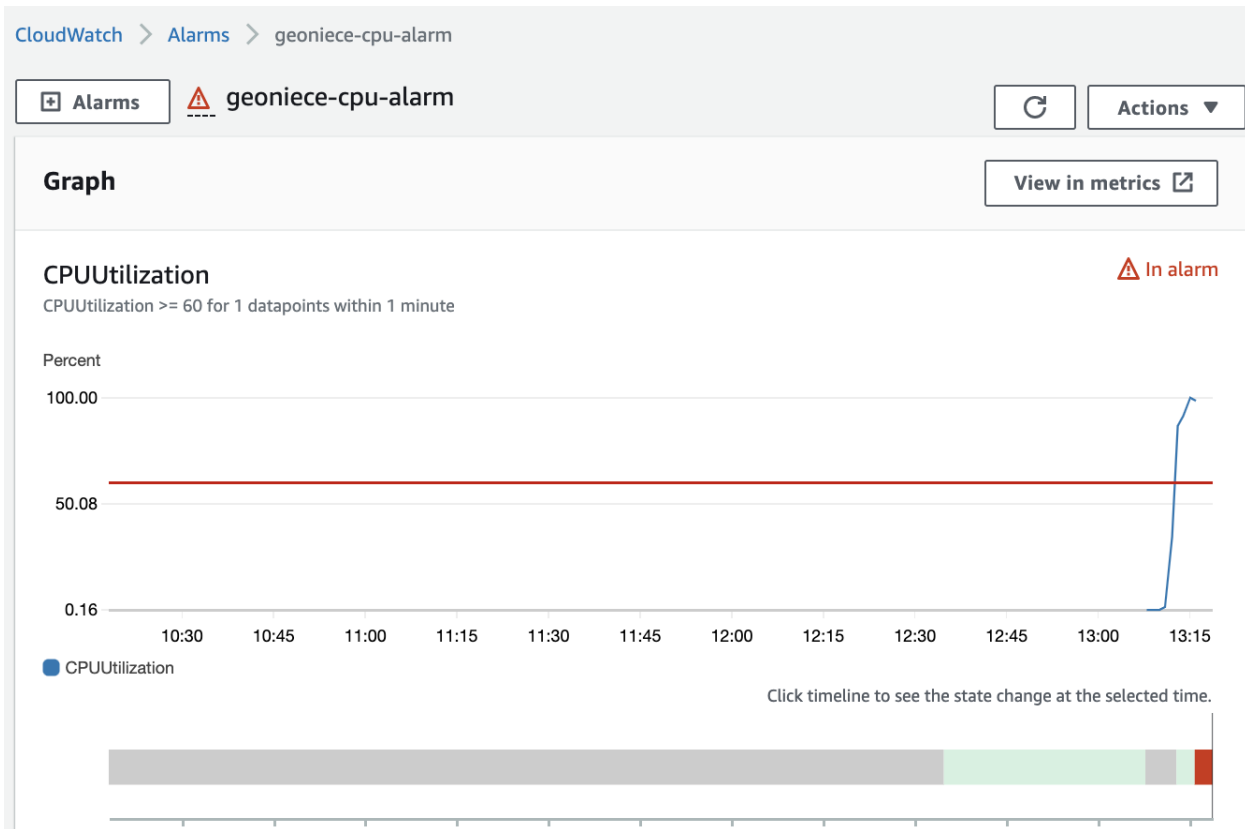
1. Navigate back to the main screen for CloudWatch Alarms.
2. Click Alarms in the left pane of the Console and check the State of your alarm. It most likely says INSUFFICIENT_DATA because you just created it.

Create Alarm Modify Copy Delete ↻ ⚙ ?

Filter: State is INSUFFICIENT ▼ ✕ ⏪ < 1 to 1 of 1 Alarms > ⏩

State ▼	Name ▼	Threshold ▼	Config Status ▼
INSUFFICIENT_DATA	johndoe-awsec2-i-071219f5b783539b9-CPU-Utilization	CPUUtilization >= 60 for 1 minute	

3. In the CloudWatch Console. Select Metrics. 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.



- After 5 minutes, the stress tool will begin to simulate CPU workload and trigger the Alarm once the threshold is reached.


CloudWatch > Alarms

Alarms (2)

☐ Hide Auto Scaling alarms Clear selection Refresh Create composite alarm Actions

Create alarm

In alarm Any type

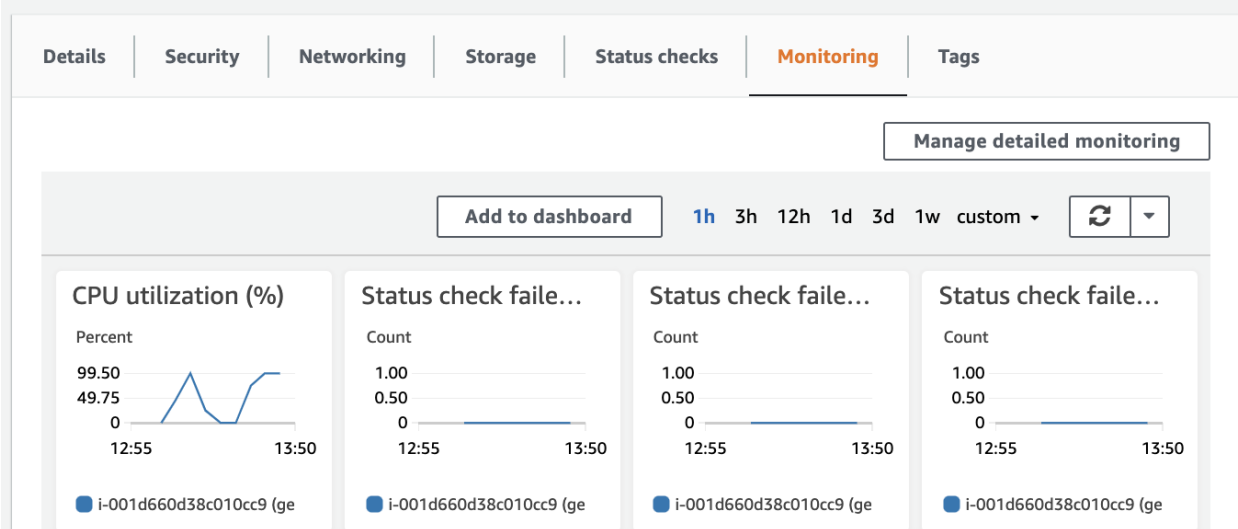
<input type="checkbox"/>	Name	State	Last state update	Conditions
<input type="checkbox"/>	geoniece-cpu-alarm	 In alarm	2021-07-18 08:15:48	CPUUtilization >= 60 for 1 datapoints within 1 minute

- You can view the Alarm state in the CloudWatch console under Alarms.

6. We setup an email notification and you will receive an email alert when the Alarm is triggered.

Use EC2 Connect

1. Navigate back to our EC2 Console
2. Select our instance and the Monitoring Tab, we'll see a graph showing that our instance is getting crushed.



3. Select our instance and click Connect. This will invoke the EC2 Connect Tool and we'll see a new browser window with a Terminal session on our instance. Note that since we didn't assign a keypair for this instance this is the only way to connect.

Instances (1/4) Info			
<input type="text" value="Filter instances"/>			
<input type="checkbox"/>	Name	Instance ID	Instan
<input checked="" type="checkbox"/>	geoniece Server	i-001d660d38c010cc9	✓ Ru

4. Enter the top command to view our instance performance details.

```
$ top
```

5. This will show us a screen similar to the one shown with the stress tool beating the heck out of our instance

```

top - 13:27:05 up 3 min, 1 user, load average: 1.06, 0.52, 0.21
Tasks: 95 total, 3 running, 52 sleeping, 0 stopped, 0 zombie
%Cpu(s):100.0 us, 0.0 sy, 0.0 ni, 0.0 id, 0.0 wa, 0.0 hi, 0.0 si, 0.0 st
KiB Mem : 1006892 total, 377988 free, 116820 used, 512084 buff/cache
KiB Swap: 0 total, 0 free, 0 used. 745224 avail Mem

  PID USER      PR  NI   VIRT   RES   SHR  S  %CPU  %MEM     TIME+ COMMAND
 7391 root        20   0    7572    96     0  R   99.7   0.0   1:58.81 stress
 3145 root        20   0   729116 27756 13376  S    0.3   2.8   0:00.10 ssm-agent-worke
 7836 ec2-user    20   0   170896  4376  3828  R    0.3   0.4   0:00.01 top
    1 root        20   0   125640  5444  3820  S    0.0   0.5   0:01.87 systemd
    2 root        20   0        0     0     0  S    0.0   0.0   0:00.00 kthreadd
    3 root        20   0        0     0     0  I    0.0   0.0   0:00.00 kworker/0:0

```

6. Noted PID for the stress tool that is running in this instance. For example, “7391”

7. Quit the top tool

Press the letter **q** on your keyboard

8. Kill the stress job

\$ sudo kill -9 7391

9. End our EC2 Connect session

\$ exit

You have successfully configured a SNS Topic, EC2 Instance, Stress test, CloudWatch Alarm, validated our alarm on the instance and notification, and connected to your instance being monitored!

View Notification

1. Browse to your email used for the notification and view your alarm.

ALARM: "geoniece-cpu-alarm" in US East (N. Virginia)

Monitoring Topic for Experiment <no-reply@sns.amazonaws.com>

to me ▾

You are receiving this email because your Amazon CloudWatch Alarm "geoniece-cpu-alarm" "Threshold Crossed: 1 out of the last 1 datapoints [77.3333333333335 (18/07/21 13:36:00)] > ALARM transition)." at "Sunday 18 July, 2021 13:38:48 UTC".

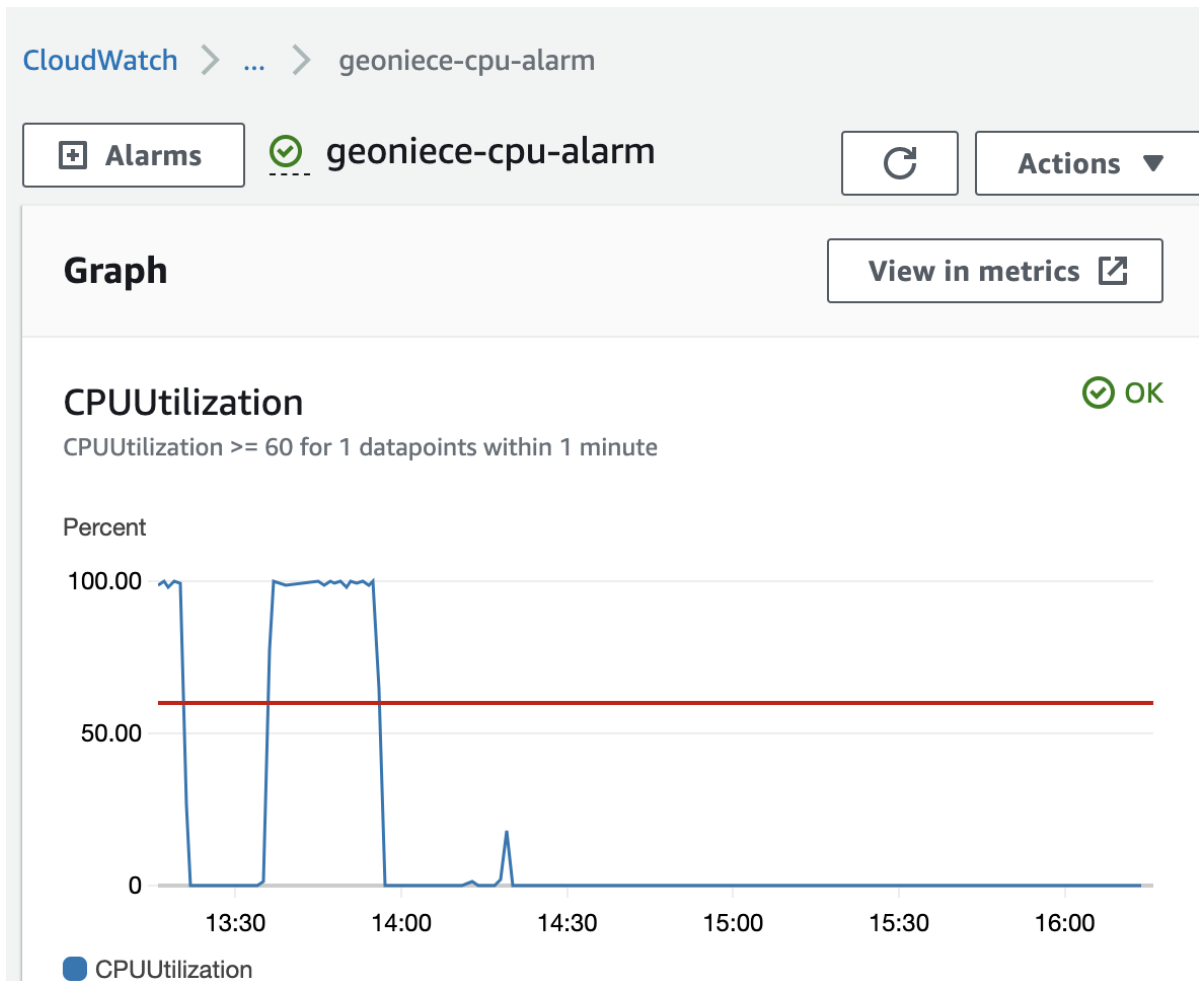
View this alarm in the AWS Management Console:

<https://us-east-1.console.aws.amazon.com/cloudwatch/deeplink.js?region=us-east-1#alarm:>

Alarm Details:

- Name: geoniece-cpu-alarm
- Description: Alarm for CPU >= 60 in 1 minute intervals
- State Change: OK -> ALARM
- Reason for State Change: Threshold Crossed: 1 out of the last 1 datapoints [77.3333333 (minimum 1 datapoint for OK -> ALARM transition)]

2. Click on the deep link to be redirected to the alarm view in the AWS Management Console



3. Note that after we killed the stress test that our alarm will come back to the OK state.

Clean Up

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

1. Select Delete on your alarm after you are finished.

Navigate to the Cloud Alarms console, select the checkbox for our alarm, from the Actions drop down select Delete. Choose Delete to permanently delete our alarm.

CloudWatch > Alarms

Alarms (1/1)

☐ Hide Auto Scaling alarms

[Clear selection](#) [Refresh](#)

[Create composite alarm](#) [Actions ▲](#) [Create alarm](#)

[Any type ▼](#)

[Delete](#) [Add to dashboard](#)

<input checked="" type="checkbox"/>	Name ▼	State ▼	Last state update ▼
<input checked="" type="checkbox"/>	geoniece-cpu-alarm	OK	2021-07-18 08:59:48

2. Stop and terminate your EC2 instance.

Navigate to the EC2 console, choose Instances, select the checkbox for our instance, from the Actions menu choose Manage State

Instances (1/1) [Info](#) [Refresh](#) [Connect](#) [Instance state ▼](#) [Actions ▲](#) [Launch](#)

[Instance state: running X](#) [Clear filters](#)

<input checked="" type="checkbox"/>	Name ▼	Instance ID ▼
<input checked="" type="checkbox"/>	geoniece Server	i-001d660d38c010

- Connect
- View details
- Manage instance state
- Instance settings
- Networking
- Security
- Image and templates
- Monitor and troubleshoot

Choose the Terminate radio and choose Change state

[EC2](#) > [Instances](#) > [i-001d660d38c010cc9](#) > Manage instance state

Manage instance state

Instance details

i-001d660d38c010cc9
(geoniece Server)

running

Instance state settings

- ☐ Start
Available when the instance is stopped
- ☐ Stop
- ☐ Hibernate
This instance did not have Stop - Hibernate enabled at launch
- ☐ Reboot
- ☒ Terminate



Note that when your instances are terminated:

On an EBS-backed instance, the default action is for the root EBS volume to be deleted when the instance is terminated. Storage on any local drives will be lost.




Cancel


Change state

Choose Terminate

Terminate instance? ×

 On an EBS-backed instance, the default action is for the root EBS volume to be deleted when the instance is terminated. Storage on any local drives will be lost.

Are you sure you want to terminate these instances?

 i-001d660d38c010cc9 (geoniece Server)

To confirm that you want to terminate the instances, choose the terminate button below. Terminating the instance cannot be undone.

Cancel Terminate

3. Delete your SNS topic.

Navigate to the Simple Notification Service (SNS) console, choose Topics, select the checkbox for our topic, choose Delete

Amazon SNS > Topics

Topics (2) Edit Delete Publish message Create topic

☒

geoniece-topic

Standard

arn:aws:sns:us-east-1:124926150123:geoniece-topic

Enter "delete me" in the input and Choose Delete

Delete topic geoniece-topic

×

Are you sure you want to delete topic **geoniece-topic** permanently? **You can't undo this action.**

To confirm deletion, enter the phrase **delete me**.

delete me

Cancel

Delete

Congratulations