

**VIT®****Vellore Institute of Technology**

(Deemed to be University under section 3 of UGC Act, 1956)

**School of Computer Science and Engineering
(SCOPE)****Fall Semester 2025-26****CBS3005 - Cloud, Microservices and Applications****LAB ASSESSMENT 5****Task 2: Analyze API Activities using AWS CloudTrail****Description:**

Enable AWS CloudTrail to monitor and log all API activities in the AWS account. Also, analyze events to detect unauthorized or unusual access.

Steps:

1. Go to CloudTrail Console → Trails → Create Trail.
2. Choose:
 - Trail name: MySecurityTrail
 - Apply trail to All regions
 - Store logs in a new S3 bucket
 - Enable CloudWatch Logs Integration (optional).
3. Perform a few activities in your AWS account:
 - Launch or stop an EC2 instance.
 - Create an S3 bucket.
4. Return to CloudTrail → Event History and view recent events.
5. Identify:
 - Who performed the action (IAM user or role)
 - Time of action
 - Source IP address
 - Affected resource

Submitted by-**YASH GARG****22BBS0183****So,****Answer 1)**

Creating Trail:

Trail details
Start logging management events by creating a trail with simplified settings. Logs are sent to an S3 bucket we create on your behalf. To choose a different bucket or additional events, go to the full [Create trail](#) workflow.

A trail created in the console is a multi-region trail. [Learn more](#)

Trail name
Enter a display name for your trail.

3-128 characters. Only letters, numbers, periods, underscores, and dashes are allowed.

Trail log bucket and folder

Logs will be stored in aws-cloudtrail-logs-533267317559-d5e38009/AWSLogs/533267317559

ⓘ Though there is no cost to log these events, you incur charges for the S3 bucket that we create to store your logs.

[Cancel](#) [Create trail](#)

Trail created successfully:

ⓘ Trail successfully created
Trail successfully deleted

ⓘ You can now enrich CloudTrail events with additional information by adding resource tags and IAM global keys in CloudTrail Lake. [Learn more](#)

Name	Home region	Multi-region trail	ARN	Insights	Organization trail	S3 bucket	Log file prefix	CloudWatch Logs log group	Status
MySecurityTrail	US East (N. Virginia)	Yes	arn:aws:cloudtrail:us-east-1:533267317559:trail/MySecurityTrail	Disabled	No	aws-cloudtrail-logs-533267317559-0f50ff8	-	-	Logging

Launched EC2 instance:

The screenshot shows the AWS EC2 Instances Launch an instance page. At the top, there's a green success message: "Success Successfully initiated launch of instance (i-0e993585eb10999dd)". Below this, there's a "Launch log" button. A "Next Steps" section follows, containing several cards with links to other AWS services: "Create billing and free tier usage alerts", "Connect to your instance", "Connect an RDS database", "Create EBS snapshot policy", "Manage detailed monitoring", "Create Load Balancer", "Create AWS budget", and "Manage CloudWatch alarms". The bottom of the page includes standard AWS navigation links like CloudShell, Feedback, and copyright information.

S3 bucket created:

The screenshot shows the AWS S3 Buckets page. It displays a green success message: "Successfully created bucket 'yashgarg-cloudtrail-demo'". Below this, there are tabs for "General purpose buckets" (selected) and "Directory buckets". The "General purpose buckets" section shows three buckets: "aws-cloudtrail-logs-533267317559-0f50ff8b", "aws-cloudtrail-logs-533267317559-d5e38009", and "yashgarg-cloudtrail-demo". Each bucket entry includes a "Copy ARN" button, an "Empty" button, a "Delete" button, and a "Create bucket" button. To the right of the bucket list, there are two informational boxes: "Account snapshot" (info) and "External access summary - new" (info). The bottom of the page includes standard AWS navigation links like CloudShell, Feedback, and copyright information.

Checking event history:

The screenshot shows the AWS CloudTrail Event history page. The left sidebar includes options like Dashboard, Event history (selected), Insights, Lake (Dashboards, Query, Event data stores, Integrations, Trails), Settings, Pricing, Documentation, Forums, and FAQs. The main content area displays a table of events with columns: Event name, Event time, User name, Event source, Resource type, and Resource name. The table lists several events related to CloudTrail operations, such as GenerateDataKey, ListManagedNotificat..., DescribeConfiguratio..., and LookupEvents, all occurring at 18:38:00 UTC on October 15, 2025. A blue banner at the top right says, "You can now enrich CloudTrail events with additional information by adding resource tags and IAM global keys in CloudTrail Lake. Learn more." Buttons for Download events, Query in Lake, and Create Athena table are also present.

The screenshot shows the AWS CloudTrail RunInstances event details page. The left sidebar includes options like Dashboard, Event history (selected), Insights, Lake (Dashboards, Query, Event data stores, Integrations, Trails), Settings, Pricing, Documentation, Forums, and FAQs. The main content area shows a detailed view of a single event named "RunInstances". It includes sections for Details (Event time: October 15, 2025, 18:34:05 (UTC+05:30); User name: root; Event name: RunInstances; Event source: ec2.amazonaws.com) and Resources referenced (7). The Resources referenced section lists seven resources: vpc-092a8cb38c9137b99, ami-052064a798f08f0d3, eni-095c525d15a640c27, i-0e993585eb10999dd, launch-wizard-1, sg-0c56416710fb07bb8, and subnets-0977d1599656410. Each resource has a link to "Enable AWS Config resource recording".

Viewing event record:

The screenshot shows the AWS CloudTrail Event history interface. On the left, there's a navigation sidebar with links like Dashboard, Event history, Insights, Lake, Pricing, Documentation, Forums, and FAQs. The main area displays an event record for a "RunInstances" operation. The event details include:

- eventVersion**: "1.10"
- userIdentity**: {
 - type**: "Root"
 - principalId**: "533267317559"
 - arn**: "arn:aws:iam::533267317559:root"
 - accountId**: "533267317559"
 - accessKeyId**: "ASIAXYKJVQM3ZQ27EE2Q"
 - sessionContext**: {
 - attributes**: {
 - creationDate**: "2025-10-15T11:44:04Z"
 - mfaAuthenticated**: "true"

- eventTime**: "2025-10-15T13:04:05Z"
- eventSource**: "ec2.amazonaws.com"
- eventName**: "RunInstances"
- awsRegion**: "us-east-1"
- sourceIPAddress**: "103.179.22.64"
- userAgent**: "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko)"
- requestParameters**: {
- instancesSet**: {
 - items**: [
 - imageId**: "ami-052064a798f08f0d3"
 - minCount**: 1
 - maxCount**: 1

JSON event record for one operation :

```
{
  "eventVersion": "1.10",
  "userIdentity": {
    "type": "Root",
    "principalId": "533267317559",
    "arn": "arn:aws:iam::533267317559:root",
    "accountId": "533267317559",
    "accessKeyId": "ASIAXYKJVQM3ZQ27EE2Q",
    "sessionContext": {
      "attributes": {
        "creationDate": "2025-10-15T11:44:04Z",
        "mfaAuthenticated": "true"
      }
    }
  },
  "eventTime": "2025-10-15T13:04:05Z",
  "eventSource": "ec2.amazonaws.com",
  "eventName": "RunInstances",
  "awsRegion": "us-east-1",
  "sourceIPAddress": "103.179.22.64",
  "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko)"}
```

```
"awsRegion": "us-east-1",

"sourceIPAddress": "103.179.22.64",
"userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/141.0.0.0 Safari/537.36",
"requestParameters": {
    "instancesSet": {
        "items": [
            {
                "imageId": "ami-052064a798f08f0d3",
                "minCount": 1,
                "maxCount": 1
            }
        ]
    },
    "instanceType": "t3.micro",
    "blockDeviceMapping": {},
    "monitoring": {
        "enabled": false
    },
    "disableApiTermination": false,
    "disableApiStop": false,
    "clientToken": "e8fad6e0-1cd6-4a40-98ac-de5bd5e7fbc0",
    "networkInterfaceSet": {
        "items": [
            {
                "deviceIndex": 0,
                "associatePublicIpAddress": true,
                "groupSet": {
                    "items": [
                        {
                            "groupId": "sg-0c56416710fb07bb8"
                        }
                    ]
                }
            }
        ]
    }
}
```

```
        }
    ]
}

},
"ebsOptimized": true,
"tagSpecificationSet": {
    "items": [
        {
            "resourceType": "instance",
            "tags": [
                {
                    "key": "Name",
                    "value": "22bbs0183"
                }
            ]
        }
    ]
},
"creditSpecification": {
    "cpuCredits": "unlimited"
},
"metadataOptions": {
    "httpTokens": "required",
    "httpPutResponseHopLimit": 2,
    "httpEndpoint": "enabled"
},
"privateDnsNameOptions": {
    "hostnameType": "ip-name",
    "enableResourceNameDnsARecord": true,
```

```
"enableResourceNameDnsAAAARecord": false
}

},
"responseElements": {
  "requestId": "eea6ccf1-c5ac-405b-9ba1-f4f880a8f22a",
  "reservationId": "r-06907711cc9423577",
  "ownerId": "533267317559",
  "groupSet": {},
  "instancesSet": {
    "items": [
      {
        "instanceId": "i-0e993585eb10999dd",
        "imageId": "ami-052064a798f08f0d3",
        "bootMode": "uefi-preferred",
        "currentInstanceBootMode": "uefi",
        "instanceState": {
          "code": 0,
          "name": "pending"
        },
        "privateDnsName": "ip-172-31-20-104.ec2.internal",
        "operator": {
          "managed": false
        },
        "amiLaunchIndex": 0,
        "productCodes": {},
        "instanceType": "t3.micro",
        "launchTime": 1760533444000,
        "placement": {
          "availabilityZone": "us-east-1c",
          "availabilityZoneId": "use1-az4",
          "tenancy": "default"
        }
      }
    ]
  }
}
```

```
        },
        "monitoring": {
            "state": "disabled"
        },
        "subnetId": "subnet-091cdc1d599a66440",
        "vpcId": "vpc-092a8cb38c9137b99",
        "privateIpAddress": "172.31.20.104",
        "stateReason": {
            "code": "pending",
            "message": "pending"
        },
        "architecture": "x86_64",
        "rootDeviceType": "ebs",
        "rootDeviceName": "/dev/xvda",
        "blockDeviceMapping": {},
        "virtualizationType": "hvm",
        "hypervisor": "xen",
        "tagSet": {
            "items": [
                {
                    "key": "Name",
                    "value": "22bbs0183"
                }
            ]
        },
        "clientToken": "e8fad6e0-1cd6-4a40-98ac-de5bd5e7fbc0",
        "groupSet": {
            "items": [
                {
                    "groupId": "sg-0c56416710fb07bb8",
                    "groupName": "launch-wizard-1"
                }
            ]
        }
    }
}
```

```
        }
    ],
},
"sourceDestCheck": true,
"networkInterfaceSet": {

    "items": [
        {
            "networkInterfaceId": "eni-095c525d15a640c27",
            "subnetId": "subnet-091cdc1d599a66440",
            "vpcId": "vpc-092a8cb38c9137b99",
            "ownerId": "533267317559",
            "operator": {
                "managed": false
            },
            "status": "in-use",
            "macAddress": "0a:ff:f7:4f:79:4f",
            "privateIpAddress": "172.31.20.104",
            "privateDnsName": "ip-172-31-20-104.ec2.internal",
            "sourceDestCheck": true,
            "interfaceType": "interface",
            "groupSet": {
                "items": [
                    {
                        "groupId": "sg-0c56416710fb07bb8",
                        "groupName": "launch-wizard-1"
                    }
                ]
            },
            "attachment": {
                "attachmentId": "eni-attach-0c9c7ae31e5e22f8c",
                "deviceIndex": 0,
                "status": "attached"
            }
        }
    ]
}
```

```
        "networkCardIndex": 0,  
        "status": "attaching",  
        "attachTime": 1760533444000,  
        "deleteOnTermination": true  
    },  
    "privateIpAddressesSet": {  
  
        "item": [  
            {  
                "privateIpAddress": "172.31.20.104",  
                "privateDnsName": "ip-172-31-20-104.ec2.internal",  
                "primary": true  
            }  
        ]  
    },  
    "ipv6AddressesSet": {},  
    "tagSet": {}  
}  
]  
},  
"ebsOptimized": true,  
"enaSupport": true,  
"cpuOptions": {  
    "coreCount": 1,  
    "threadsPerCore": 2  
},  
"capacityReservationSpecification": {  
    "capacityReservationPreference": "open"  
},  
"enclaveOptions": {  
    "enabled": false  
},
```

```
    "metadataOptions": {  
        "state": "pending",  
        "httpTokens": "required",  
        "httpPutResponseHopLimit": 2,  
        "httpEndpoint": "enabled",  
        "httpProtocolIpv4": "enabled",  
        "httpProtocolIpv6": "disabled",  
  
        "instanceMetadataTags": "disabled"  
    },  
    "maintenanceOptions": {  
        "autoRecovery": "default",  
        "rebootMigration": "default"  
    },  
    "privateDnsNameOptions": {  
        "hostnameType": "ip-name",  
        "enableResourceNameDnsARecord": true,  
        "enableResourceNameDnsAAAARecord": false  
    }  
},  
]  
},  
{"  
    "requestID": "eea6ccf1-c5ac-405b-9ba1-f4f880a8f22a",  
    "eventID": "104d0d32-a1d6-44e9-a416-233fcacb45fb",  
    "readOnly": false,  
    "resources": [  
        {  
            "accountId": "533267317559",  
            "type": "AWS::EC2::Instance",  
            "ARN": "arn:aws:ec2:us-east-1:533267317559:instance/i-  
0e993585eb10999dd"
```

```
        },  
        ],  
        "eventType": "AwsApiCall",  
        "managementEvent": true,  
        "recipientAccountId": "533267317559",  
        "eventCategory": "Management",  
        "tlsDetails": {  
            "tlsVersion": "TLSv1.3",  
  
            "cipherSuite": "TLS_AES_128_GCM_SHA256",  
            "clientProvidedHostHeader": "ec2.us-east-1.amazonaws.com"  
        },  
        "sessionCredentialFromConsole": "true"  
    }  
}
```

Explanation of how CloudTrail supports auditing and incident investigation:

AWS CloudTrail records all API activity and actions performed in your AWS account, including who performed each action, when it occurred, and from which IP address. This detailed logging allows organizations to **track changes, detect unauthorized access, and investigate security incidents**. By analyzing CloudTrail logs, auditors and security teams can **reconstruct events**, identify suspicious activities, and ensure compliance with internal policies and regulatory requirements.

Task 2: Configure CloudWatch for EC2 Instance Monitoring**Description:**

Create and monitor a simple EC2 instance using **Amazon CloudWatch**, configure alarms, monitor system metrics, and analyze performance data to understand how CloudWatch helps in proactive threat and performance monitoring.

Steps:

1. Launch a **t2.micro EC2 instance** (Free Tier eligible) running Amazon Linux 2.
2. Install and configure the **CloudWatch Agent** using:

```
sudo yum install amazon-cloudwatch-agent -y  
sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-config-wizard
```

3. Choose to monitor:
 - o CPU utilization
 - o Memory usage
 - o Disk I/O

4. Start the CloudWatch agent:

```
sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-ctl \  
-a fetch-config -m ec2 -c file:/opt/aws/amazon-cloudwatch-agent/bin/config.json -s
```

5. Go to **CloudWatch Console → Metrics → EC2** and verify data collection.

6. Create a **CloudWatch Alarm**:

- o Metric: CPUUtilization
- o Condition: >70% for 2 consecutive periods
- o Notification: via **SNS topic** (send email alert).

Answer2)

Launched EC2 instance:

The screenshot shows the AWS EC2 Instances page. On the left, there's a navigation sidebar with sections like Dashboard, EC2 Global View, Events, Instances (selected), Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations, Images, AMIs, AMI Catalog, Elastic Block Store, Volumes, Snapshots, Lifecycle Manager, Network & Security, Security Groups, and Elastic IPs. The main content area shows a table of instances with one row selected. The selected instance is '22bbs0183-cl...', with details: Instance ID 'i-0dec64c31bcd9718f', Instance state 'Running' (green), Instance type 't3.micro', Status check 'Initializing' (yellow), Alarm status 'View alarms +', Availability Zone 'us-east-1c', and Public IP '13.221.70.55'. Below the table, there's a detailed view for the selected instance, showing its summary, public and private IP addresses, and DNS names.

Installing and configuring CloudWatch agent:

```

# Amazon Linux 2023
# https://aws.amazon.com/linux/amazon-linux-2023
Last login: Wed Oct 15 13:39:09 2025 from 18.206.107.28
[ec2-user@ip-172-31-30-162 ~]$ sudo yum install amazon-cloudwatch-agent -y
Amazon Linux 2023 Kernel Livepatch repository
Dependencies resolved.
=====
Package           Architecture      Version          Repository      Size
=====
Installing:
amazon-cloudwatch-agent   x86_64        1.300057.2-1.amzn2023    amazonlinux      135 M
Transaction Summary
=====
Install 1 Package

Total download size: 135 M
Installed size: 471 M
Downloading Packages:
amazon-cloudwatch-agent-1.300057.2-1.amzn2023.x86_64.rpm
66 MB/s | 135 MB  00:02
Total
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
Preparing : 1/1
i-0dec64c31bcd9718f (22bbs0183-cloudwatch-demo)
PublicIPs: 13.221.70.55 PrivateIPs: 172.31.30.162

```

The terminal window shows the command `sudo yum install amazon-cloudwatch-agent -y` being run on an Amazon Linux 2023 instance. The output includes the package details, transaction summary, and the final status message indicating the agent is installed on the instance with public and private IP addresses.

Complete!

```
[ec2-user@ip-172-31-30-162 ~]$ sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-config-wizard
=====
= Welcome to the Amazon CloudWatch Agent Configuration Manager =
=                                                               =
= CloudWatch Agent allows you to collect metrics and logs from =
= your host and send them to CloudWatch. Additional CloudWatch =
= charges may apply.                                            =
=====
On which OS are you planning to use the agent?
1. linux
2. windows
3. darwin
default choice: [1]:
1
Trying to fetch the default region based on ec2 metadata...
! imds retry client will retry 1 timesAre you using EC2 or On-Premises hosts?
1. EC2
2. On-Premises
default choice: [1]:
1
Which user are you planning to run the agent?
1. cwagent
2. root
3. others
default choice: [1]:
1
Do you want to turn on StatsD daemon?
1. yes
2. no
default choice: [1]:
2
Do you want to monitor metrics from CollectD? WARNING: CollectD must be installed or the Agent will fail to start
1. yes
2. no
default choice: [1]:
1
i-0dec64c31bcd9718f (22bbs0183-cloudwatch-demo)
```

Public IPs: 13.221.70.55 Private IPs: 172.31.30.162

[CloudShell](#) [Feedback](#)

© 2025, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

Which default metrics config do you want?

```
1. Basic
2. Standard
3. Advanced
4. None
default choice: [1]:
2
Current config as follows:
{
    "agent": {
        "metrics_collection_interval": 60,
        "run_as_user": "cwagent"
    },
    "metrics": {
        "aggregation_dimensions": [
            {
                "InstanceId"
            }
        ],
        "append_dimensions": {
            "AutoScalingGroupName": "${aws:AutoScalingGroupName}",
            "ImageId": "${aws:ImageId}",
            "InstanceId": "${aws:InstanceId}",
            "InstanceType": "${aws:InstanceType}"
        },
        "metrics_collected": {
            "cpu": {
                "measurement": [
                    "cpu_usage_idle",
                    "cpu_usage_iowait",
                    "cpu_usage_user",
                    "cpu_usage_system"
                ],
                "metrics_collection_interval": 60,
                "resources": [
                    "*"
                ]
            }
        }
    }
}
```

i-0dec64c31bcd9718f (22bbs0183-cloudwatch-demo)

Public IPs: 13.221.70.55 Private IPs: 172.31.30.162

[CloudShell](#) [Feedback](#)

© 2025, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

AWS Search [Option+S] United States (N. Virginia) ▾ Account ID: 5332-6731-7559 ▾ YASH GARG

```

        },
        "swap": {
            "measurement": [
                "swap_used_percent"
            ],
            "metrics_collection_interval": 60
        }
    }
}

Are you satisfied with the above config? Note: it can be manually customized after the wizard completes to add additional items.
1. yes
2. no
default choice: [1]:
1
Do you have any existing CloudWatch Log Agent (http://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/AgentReference.html) configuration file to import for migration?
1. yes
2. no
default choice: [2]:
2
Do you want to monitor any log files?
1. yes
2. no
default choice: [1]:
2
Do you want the CloudWatch agent to also retrieve X-ray traces?
1. yes
2. no
default choice: [1]:
2
Existing config JSON identified and copied to: /opt/aws/amazon-cloudwatch-agent/etc/backup-configs
Saved config file to /opt/aws/amazon-cloudwatch-agent/bin/config.json successfully.
Current config as follows:
{
    "agent": {
        "metrics_collection_interval": 60
    }
}

```

i-0dec64c31bcd9718f (22bbs0183-cloudwatch-demo)

Public IPs: 13.221.70.55 Private IPs: 172.31.30.162

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

AWS Search [Option+S] United States (N. Virginia) ▾ Account ID: 5332-6731-7559 ▾ YASH GARG

```

        },
        "swap": {
            "measurement": [
                "swap_used_percent"
            ],
            "metrics_collection_interval": 60
        }
    }
}

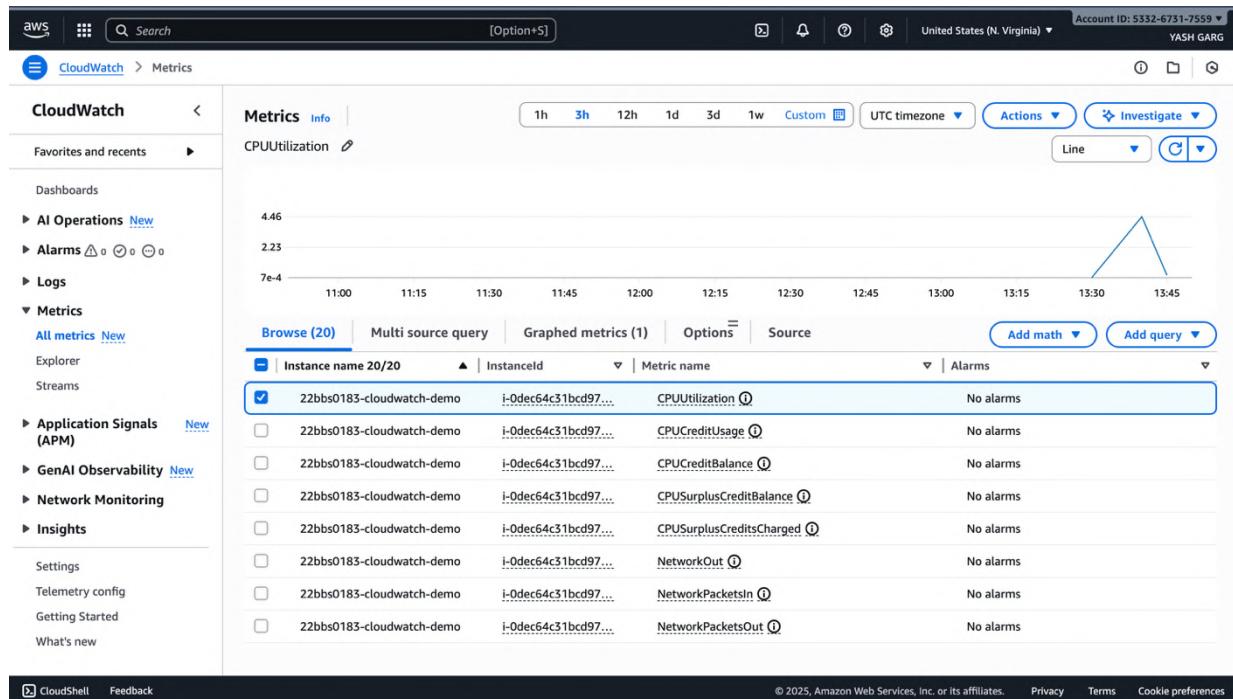
Please check the above content of the config.
The config file is also located at /opt/aws/amazon-cloudwatch-agent/bin/config.json.
Edit it manually if needed.
Do you want to store the config in the SSM parameter store?
1. yes
2. no
default choice: [1]:
2
Program exits now.
[ec2-user@ip-172-31-30-162 ~]$ sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-ctl \
-a fetch-config -m ec2 -c file:/opt/aws/amazon-cloudwatch-agent/bin/config.json -s
***** processing amazon-cloudwatch-agent *****
I! Trying to detect region from ec2 D! [EC2] Found active network interface I! imds retry client will retry 1 timesSuccessfully fetched the config and saved in /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.d/file_config.json.tmp
Start configuration validation...
2025/10/15 13:50:50 Reading json config file path: /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.d/file_config.json.tmp ...
2025/10/15 13:50:50 I! Valid Json input schema.
2025/10/15 13:50:50 D! ec2tagger processor required because append_dimensions is set
2025/10/15 13:50:50 D! delta processor required because metrics with diskio or net are set
2025/10/15 13:50:50 D! ec2tagger processor required because append_dimensions is set
2025/10/15 13:50:50 Configuration validation first phase succeeded
I! Detecting run as user.
I! Trying to detect region from ec2
D! [EC2] Found active network interface
I! imds retry client will retry 1 times
/opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent -schematest -config /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.toml
Configuration validation second phase succeeded
Configuration validation succeeded
amazon-cloudwatch-agent has already been stopped
Created symlink /etc/systemd/system/multi-user.target.wants/amazon-cloudwatch-agent.service → /etc/systemd/system/amazon-cloudwatch-agent.service.
[ec2-user@ip-172-31-30-162 ~]$ 
```

i-0dec64c31bcd9718f (22bbs0183-cloudwatch-demo)

Public IPs: 13.221.70.55 Private IPs: 172.31.30.162

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Choosing CPU utilization from CloudWatch metrics:



Specifying conditions for alarm “>70% for 2 consecutive periods”

The screenshot shows the 'Create alarm' wizard in the AWS CloudWatch Alarms console. The steps are: Step 1 (selected), Step 2 (Configure actions), Step 3 (Add alarm details), and Step 4 (Preview and create). A blue banner at the top says 'Alarm recommendations available. Turn on Recommendations to pre-populate the wizard with the recommended alarms.' The main area is titled 'Specify metric and conditions'.

Metric

Graph
This alarm will trigger when the blue line goes above the red line for 1 datapoints within 5 minutes.

Percent

Namespace
AWS/EC2

Metric name
CPUUtilization

InstanceId
i-0dec64c31bcd9718f

Instance name
22bbs0183-cloudwatch-demo

Statistic
Average

Period
5 minutes

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.

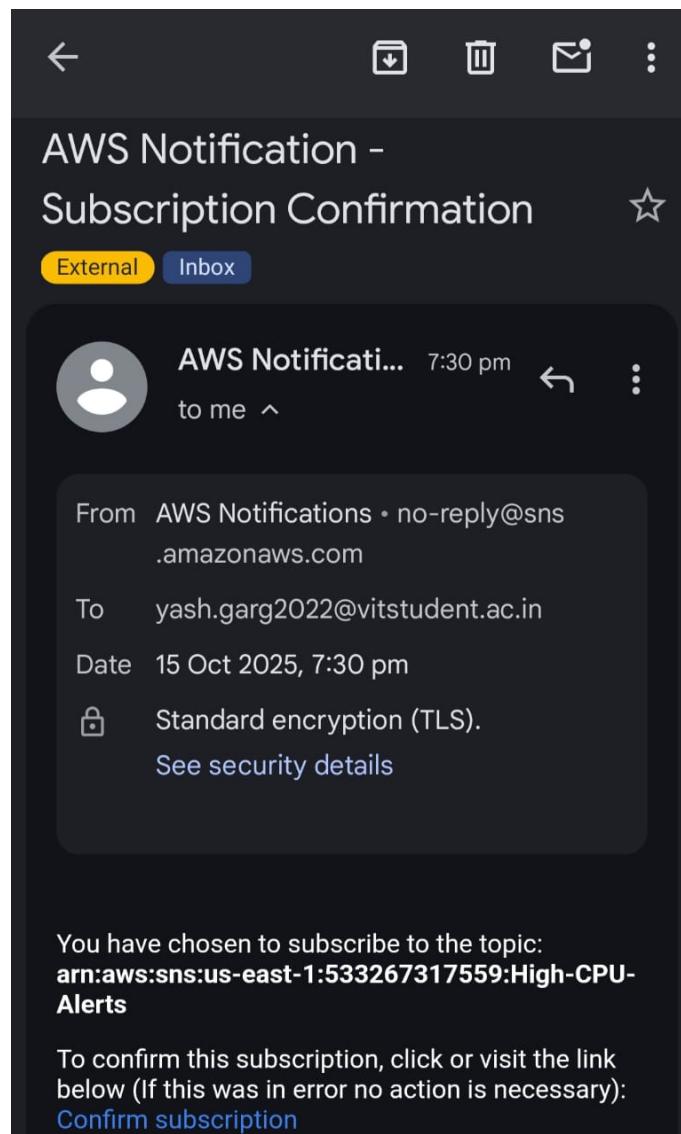
Additional configuration

Datapoints to alarm
Define the number of datapoints within the evaluation period that must be breaching to cause the alarm to go to ALARM state.
 out of

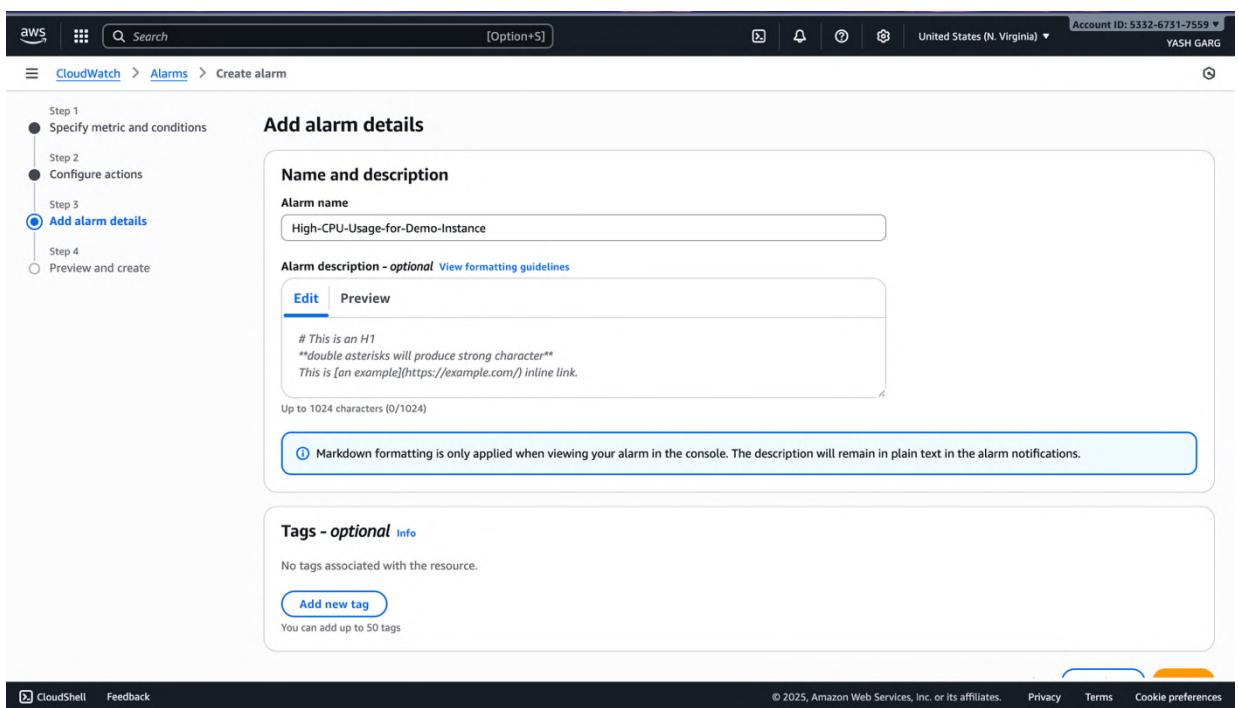
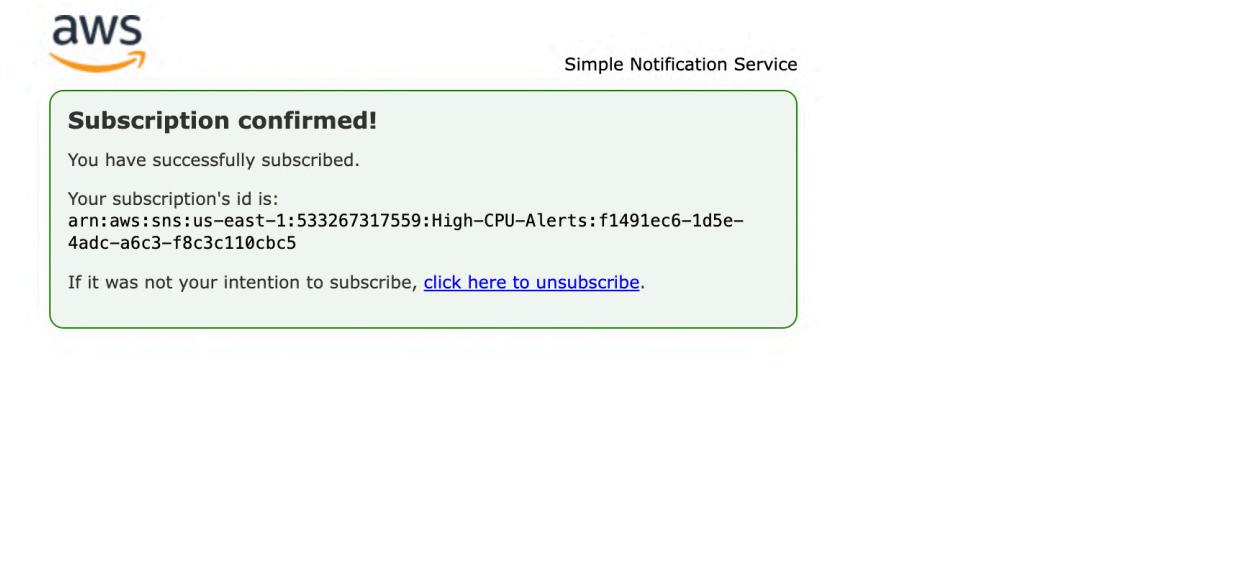
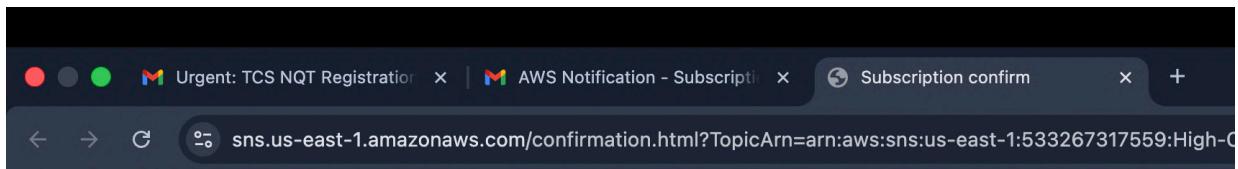
Missing data treatment
How to treat missing data when evaluating the alarm.

Cancel **Next**

Email received:



Confirmed Subscription:



Metric

Graph
This alarm will trigger when the blue line goes above the red line for 2 datapoints within 10 minutes.

Percent

70

35

7e-4

11:00 11:30 12:00 12:30 13:00 13:30 14:00

CPUUtilization

Namespace
AWS/EC2

Metric name
CPUUtilization

InstanceId
i-0dec64c31bcd9718f

Instance name
22bbs0183-cloudwatch-demo

Statistic
Average

Period
5 minutes

Conditions

Threshold type
Static

Whenever CPUUtilization is
Greater (>)

than...
70

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Alarm created:

CloudWatch

Favorites and recents

CloudWatch > Alarms

Alarms (1)

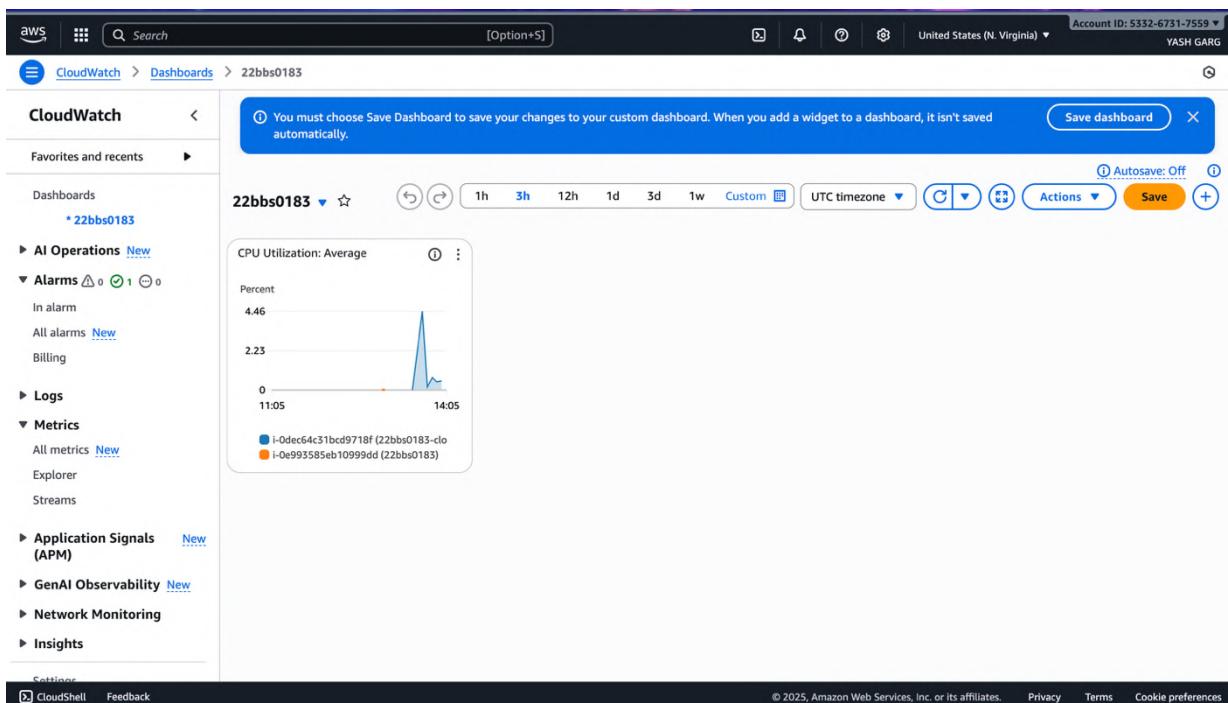
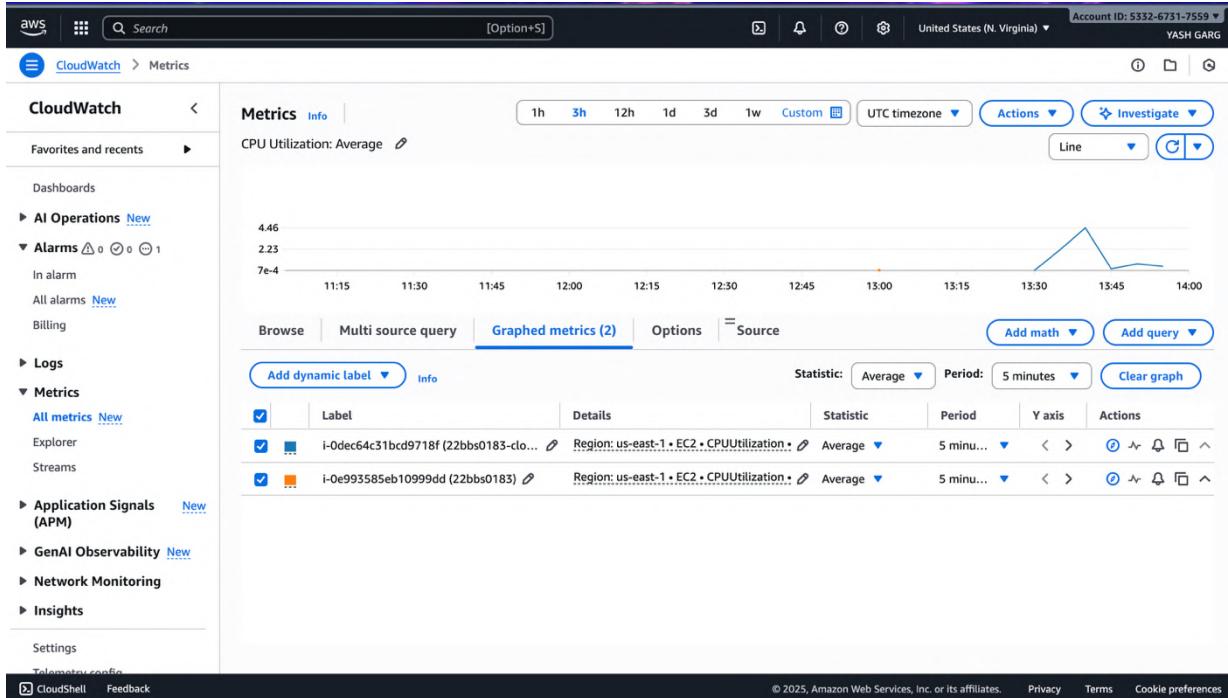
Successfully created alarm High-CPU-Usage-for-Demo-Instance.

Create alarm

Name	State	Last state update (UTC)	Conditions	Actions
High-CPU-Usage-for-Demo-Instance	Insufficient data	2025-10-15 14:03:48	CPUUtilization > 70 for 2 datapoints within 10 minutes	Actions enabled

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

CloudWatch Dashboard:



```
Last metadata expiration check: 0:28:31 ago on Wed Oct 15 13:40:32 2025.
Dependencies resolved.
=====
Package          Architecture Version      Repository  Size
=====
Installing:
 stress-ng        x86_64      0.15.05-1.amzn2023
Installing dependencies:
 Judy             x86_64      1.0.5-25.amzn2023.0.3
 libbsd           x86_64      0.10.0-7.amzn2023.0.2
 lksctp-tools     x86_64      1.0.18-9.amzn2023.0.3
=====
Transaction Summary
=====
Install 4 Packages
Total download size: 2.7 M
Installed size: 9.7 M
Downloading Packages:
(1/4): libbsd-0.10.0-7.amzn2023.0.2.x86_64.rpm          1.6 MB/s | 109 kB   00:00
(2/4): lksctp-tools-1.0.18-9.amzn2023.0.3.x86_64.rpm    1.0 MB/s | 92 kB   00:00
(3/4): Judy-1.0.5-25.amzn2023.0.3.x86_64               1.3 MB/s | 153 kB   00:00
(4/4): stress-ng-0.15.05-1.amzn2023.x86_64            10 MB/s | 2.3 MB   00:00
=====
Total
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
  Preparing           :
  Installing         : lksctp-tools-1.0.18-9.amzn2023.0.3.x86_64  1/1
  Installing         : libbsd-0.10.0-7.amzn2023.0.2.x86_64       1/4
  Installing         : Judy-1.0.5-25.amzn2023.0.3.x86_64       2/4
  Installing         : stress-ng-0.15.05-1.amzn2023.x86_64       3/4
  Running scriptlets: stress-ng-0.15.05-1.amzn2023.x86_64       4/4
=====
i-0dec64c31bcd9718f (22bbs0183-cloudwatch-demo) X
Public IPs: 13.221.70.55 Private IPs: 172.31.30.162
```

[CloudShell](#) [Feedback](#)

© 2025, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

```
Transaction test succeeded.
Running transaction
  Preparing           :
  Installing         : lksctp-tools-1.0.18-9.amzn2023.0.3.x86_64  1/1
  Installing         : libbsd-0.10.0-7.amzn2023.0.2.x86_64       1/4
  Installing         : Judy-1.0.5-25.amzn2023.0.3.x86_64       2/4
  Installing         : stress-ng-0.15.05-1.amzn2023.x86_64       3/4
  Running scriptlets: stress-ng-0.15.05-1.amzn2023.x86_64       4/4
  Verifying          : Judy-1.0.5-25.amzn2023.0.3.x86_64       4/4
  Verifying          : libbsd-0.10.0-7.amzn2023.0.2.x86_64       1/4
  Verifying          : lksctp-tools-1.0.18-9.amzn2023.0.3.x86_64  2/4
  Verifying          : stress-ng-0.15.05-1.amzn2023.x86_64       3/4
  Verifying          : stress-ng-0.15.05-1.amzn2023.x86_64       4/4
=====
WARNING:
  A newer release of "Amazon Linux" is available.

Available Versions:
  Version 2023.9.20251014:
    Run the following command to upgrade to 2023.9.20251014:
      dnf upgrade --releasever=2023.9.20251014

  Release notes:
    https://docs.aws.amazon.com/linux/al2023/release-notes/relnotes-2023.9.20251014.html
=====

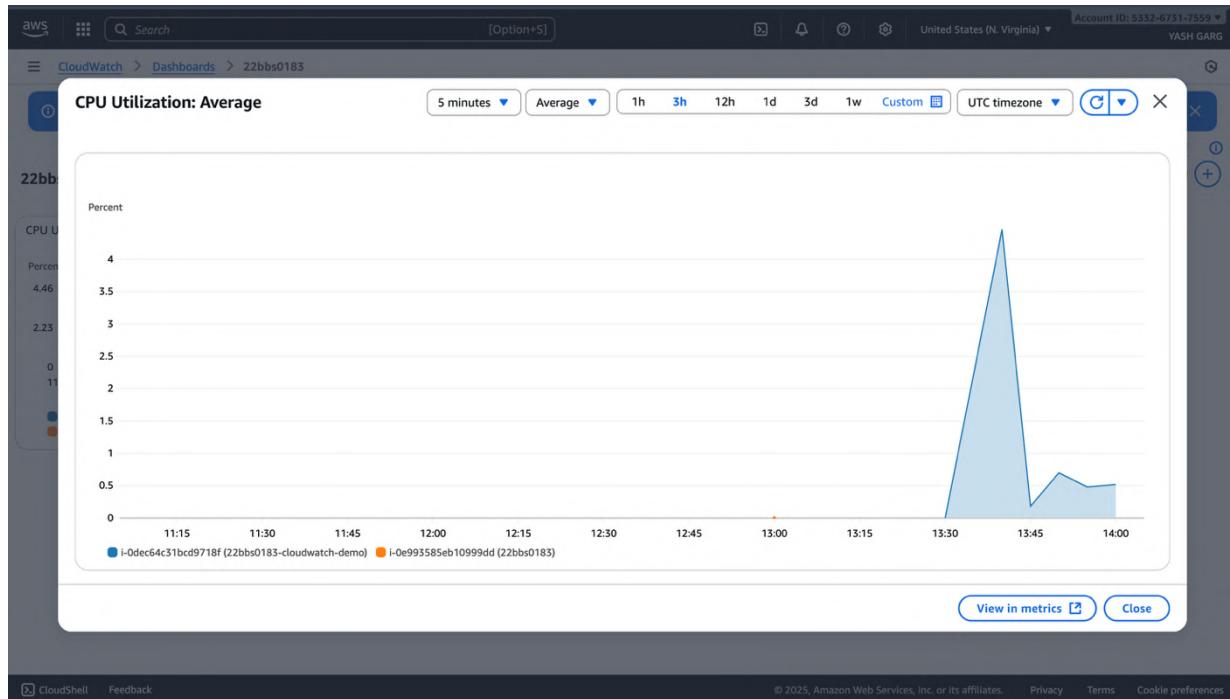
Installed:
  Judy-1.0.5-25.amzn2023.0.3.x86_64   libbsd-0.10.0-7.amzn2023.0.2.x86_64   lksctp-tools-1.0.18-9.amzn2023.0.3.x86_64   stress-ng-0.15.05-1.amzn2023.x86_64

Complete!
[ec2-user@ip-172-31-30-162 ~]$ stress-ng --cpu 1 --timeout 900s
stress-ng: info: [28880] setting to a 900 second (15 mins, 0.00 secs) run per stressor
stress-ng: info: [28880] dispatching hogs: 1 cpu
```

[CloudShell](#) [Feedback](#)

© 2025, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

CPU Utilization Graph (widget):



THANK YOU!