



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:

aws

Search

[Option+S]

United States (N. Virginia)

Account ID: 5332-6731-7559

YASH GARG

CloudTrail

Quick trail create

Quick trail create

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.

MySecurityTrail

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

Trail log bucket and folder

aws-cloudtrail-logs-533267317559-d5e38009

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

CloudShell

Feedback

© 2025, Amazon Web Services, Inc. or its affiliates.

Privacy

Terms

Cookie preferences

Trail created successfully:

aws

Search

[Option+S]

United States (N. Virginia)

Account ID: 5332-6731-7559

YASH GARG

CloudTrail

Trails

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](#)

Trails

Copy events to Lake

Delete

Create trail

	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-533267317559-0f50ffb8	-	-	Logging

CloudShell

Feedback

© 2025, Amazon Web Services, Inc. or its affiliates.

Privacy

Terms

Cookie preferences

Launched EC2 instance:

Success
Successfully initiated launch of instance (i-0e993585eb10999dd)

► Launch log

Next Steps
What would you like to do next with this instance, for example "create alarm" or "create backup"

Create billing and free tier usage alerts
To manage costs and avoid surprise bills, set up email notifications for billing and free tier usage thresholds.
[Create billing alerts](#)

Connect to your instance
Once your instance is running, log into it from your local computer.
[Connect to instance](#)
[Learn more](#)

Connect an RDS database
Configure the connection between an EC2 instance and a database to allow traffic flow between them.
[Connect an RDS database](#)
[Create a new RDS database](#)
[Learn more](#)

Create EBS snapshot policy
Create a policy that automates the creation, retention, and deletion of EBS snapshots.
[Create EBS snapshot policy](#)

Manage detailed monitoring
Enable or disable detailed monitoring for the instance. If you enable detailed monitoring, the Amazon EC2 console displays monitoring graphs with a 1-minute period.

Create Load Balancer
Create an application, network gateway or classic Elastic Load Balancer.
[Create Load Balancer](#)

Create AWS budget
AWS Budgets allows you to create budgets, forecast spend, and take action on your costs and usage from a single location.

Manage CloudWatch alarms
Create or update Amazon CloudWatch alarms for the instance.
[Manage CloudWatch alarms](#)

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

S3 bucket created:

Successfully created bucket "yashgarg-cloudtrail-demo"
To upload files and folders, or to configure additional bucket settings, choose [View details](#).

General purpose buckets All AWS Regions Directory buckets

General purpose buckets (3) Info
Buckets are containers for data stored in S3.
[Find buckets by name](#)

Name	AWS Region	Creation date
aws-cloudtrail-logs-533267317559-0f50ffb8	US East (N. Virginia) us-east-1	October 15, 2025, 18:30:05 (UTC+05:30)
aws-cloudtrail-logs-533267317559-d5e38009	US East (N. Virginia) us-east-1	October 15, 2025, 18:20:37 (UTC+05:30)
yashgarg-cloudtrail-demo	US East (N. Virginia) us-east-1	October 15, 2025, 18:36:06 (UTC+05:30)

Account snapshot Info
Updated daily
Storage Lens provides visibility into storage usage and activity trends.
[View dashboard](#)

External access summary - new Info
Updated daily
External access findings help you identify bucket permissions that allow public access or access from other AWS accounts.

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

Checking event history:

CloudTrail

Dashboard

Event history

Insights

Lake

Dashboards

Query

Event data stores

Integrations

Trails

Settings

Pricing

Documentation

Forums

FAQs

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

Event history (250+) Info

Event history shows you the last 90 days of management events.

Lookup attributes

Select a lookup attribute key

Enter a lookup value

Filter by date and time

Clear filter

< 1 2 ... >

	Event name	Event time	User name	Event source	Resource type	Resource name
<input type="checkbox"/>	GenerateDataKey	October 15, 2025, 18:39:14 (UT...	-	kms.amazonaws.com	-	-
<input type="checkbox"/>	GenerateDataKey	October 15, 2025, 18:39:11 (UT...	-	kms.amazonaws.com	-	-
<input type="checkbox"/>	ListManagedNotificat...	October 15, 2025, 18:38:48 (UT...	root	notifications.amazona ws.com	-	-
<input type="checkbox"/>	DescribeConfiguratio...	October 15, 2025, 18:38:01 (UT...	root	config.amazonaws.com	-	-
<input type="checkbox"/>	LookupEvents	October 15, 2025, 18:38:00 (UT...	root	cloudtrail.amazonaws.c om	-	-
<input type="checkbox"/>	DescribeConfiguratio...	October 15, 2025, 18:38:00 (UT...	root	config.amazonaws.com	-	-
<input type="checkbox"/>	DescribeTrails	October 15, 2025, 18:37:59 (UT...	root	cloudtrail.amazonaws.c om	-	-
<input type="checkbox"/>	GetTrailStatus	October 15, 2025, 18:37:59 (UT...	root	cloudtrail.amazonaws.c om	AWS::CloudTrail::Trail	arn:aws:cloudtrail:us-east-1:5332-6731-7559:trail/trail-093fde1d590a56440
<input type="checkbox"/>	LookupEvents	October 15, 2025, 18:37:59 (UT...	root	cloudtrail.amazonaws.c	-	-

0 / 5 events selected

CloudShell

Feedback

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

CloudTrail

Dashboard

Event history

Insights

Lake

Dashboards

Query

Event data stores

Integrations

Trails

Settings

Pricing

Documentation

Forums

FAQs

RunInstances Info

Details Info

Event time
October 15, 2025, 18:34:05 (UTC+05:30)

User name
root

Event name
RunInstances

Event source
ec2.amazonaws.com

AWS access key
ASIAXYKJVM3ZQ27EE2Q

Source IP address
103.179.22.64

Event ID
104d0d32-a1d6-44e9-a416-233fcac45fb

Request ID
eea6ccf1-c5ac-405b-9ba1-f4f880a8f22a

AWS region
us-east-1

Error code
-

Read-only
false

Resources referenced (7) Info

Resources referenced describes the name or ID of resources that were read or changed by an event

Resource type	Resource name	AWS Config resource timeline
AWS::EC2::VPC	vpc-092a8cb38c9137b99	Enable AWS Config resource recording
AWS::EC2::Ami	ami-052064a798f08f0d3	Enable AWS Config resource recording
AWS::EC2::NetworkInterface	eni-095c525d15a640c27	Enable AWS Config resource recording
AWS::EC2::Instance	i-0e993585eb10999dd	Enable AWS Config resource recording
AWS::EC2::SecurityGroup	launch-wizard-1	Enable AWS Config resource recording
AWS::EC2::SecurityGroup	sg-0c56416710fb07bb8	Enable AWS Config resource recording
AWS::EC2::Subnet	subnet-093fde1d590a56440	Enable AWS Config resource recording

CloudShell

Feedback

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

Viewing event record:

The screenshot shows the AWS CloudTrail console interface. On the left is a navigation menu with options like Dashboard, Event history, Insights, Lake, Dashboards, Query, Event data stores, Integrations, Trails, Settings, Pricing, Documentation, Forums, and FAQs. The main area displays an 'Event record' for the 'RunInstances' operation. The event details are shown in a JSON view, with line numbers 1 through 29. The JSON object contains fields for eventVersion, userIdentity (with type, principalId, arn, accountId, and accessKeyId), sessionContext (with attributes like creationDate and mfaAuthenticated), eventTime, eventSource, eventName, awsRegion, sourceIPAddress, userAgent, requestParameters (including instancesSet with imageId, minCount, and maxCount), and eventTime.

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) 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,
```

```
        "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:
 - CPU utilization
 - Memory usage
 - Disk I/O

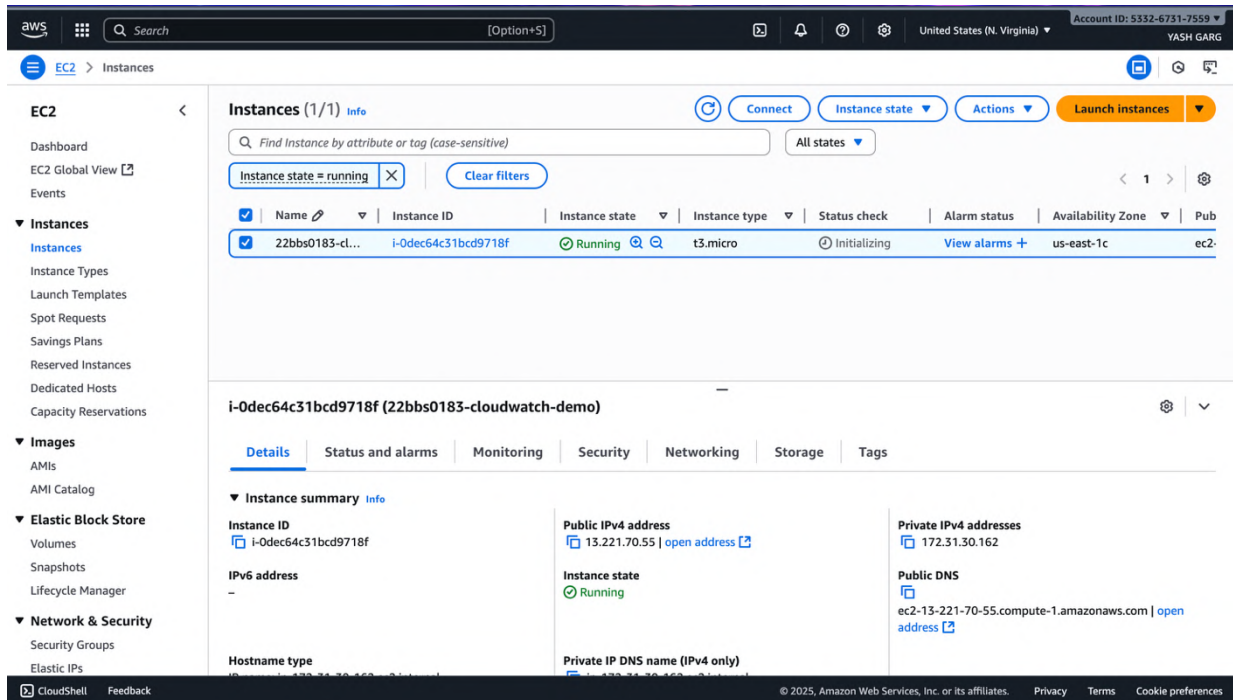
4. Start the CloudWatch agent:

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

Answer2)

Launched EC2 instance:



The screenshot shows the AWS Management Console for the 'Instances' page. The instance '22bbs0183-cloudwatch-demo' is listed with the ID 'i-0dec64c31bcd9718f' and is in the 'Running' state. The instance details are shown below the list, including its ID, state, type, and various addresses.

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Pub
22bbs0183-cl...	i-0dec64c31bcd9718f	Running	t3.micro	Initializing	View alarms +	us-east-1c	ec2-

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

Details | Status and alarms | Monitoring | Security | Networking | Storage | Tags

Instance summary

Instance ID: i-0dec64c31bcd9718f

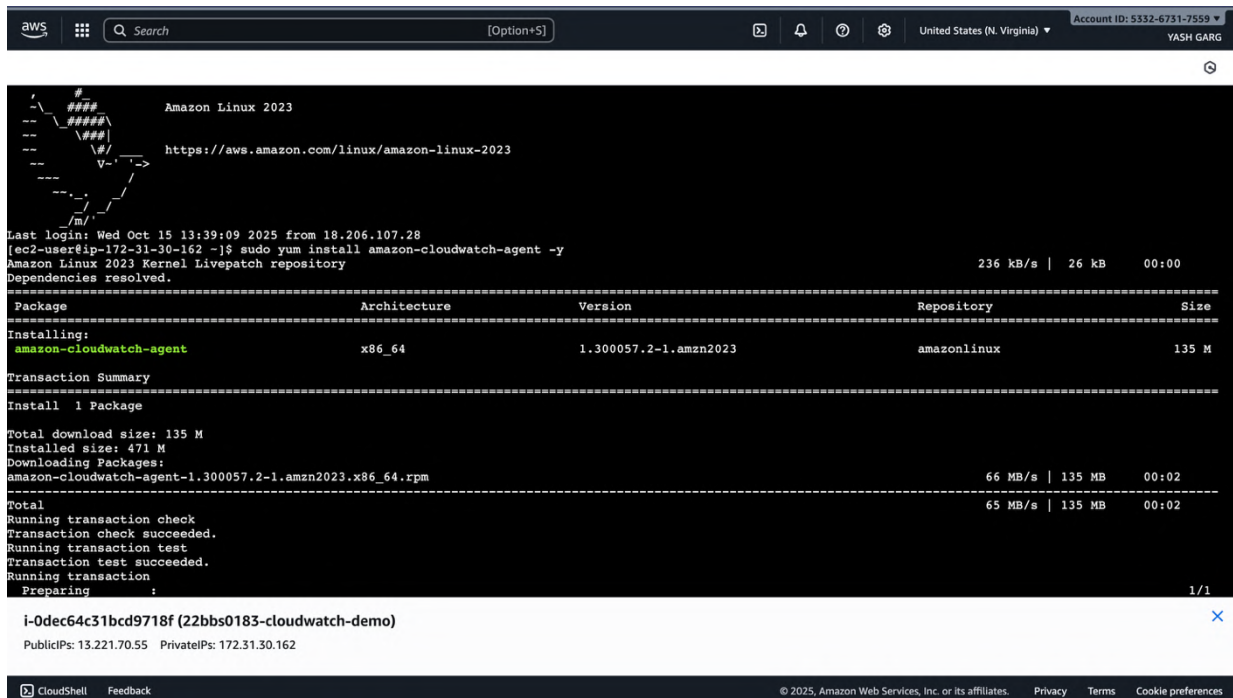
Public IPv4 address: 13.221.70.55 | open address

Private IPv4 addresses: 172.31.30.162

Public DNS: ec2-13-221-70-55.compute-1.amazonaws.com | open address

Private IP DNS name (IPv4 only): i-0dec64c31bcd9718f

Installing and configuring CloudWatch agent:



The screenshot shows the AWS CloudShell terminal output for installing the Amazon CloudWatch agent on an Amazon Linux 2023 instance. The terminal output shows the command to install the agent, the package details, and the successful completion of the transaction.






```
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 65 MB/s | 135 MB 00:02
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
Preparing
1/1
```



```
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...
If 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]:
2

i-0dec64c31bcd9718f (22bbs0183-cloudwatch-demo)
PublicIPs: 13.221.70.55 PrivateIPs: 172.31.30.162
```

```
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": [
          "*"
        ]
      }
    }
  }
}
```



[Option+S]United States (N. Virginia)Account ID: 5332-6731-7559YASH 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]:
1
Do you want the CloudWatch agent to also retrieve X-ray traces?
1. yes
2. no
default choice: [1]:
1
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)

PublicIPs: 13.221.70.55 PrivateIPs: 172.31.30.162

 CloudShell  Feedback

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



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

```
    "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)

PublicIPs: 13.221.70.55 PrivateIPs: 172.31.30.162

 CloudShell  Feedback

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

Choosing CPU utilization from CloudWatch metrics:

The screenshot shows the AWS CloudWatch Metrics console. The left sidebar contains navigation links for CloudWatch, Metrics, Favorites and recents, Dashboards, AI Operations, Alarms, Logs, Metrics, All metrics, Explorer, Streams, Application Signals (APM), GenAI Observability, Network Monitoring, and Insights. The main content area displays the 'Metrics' page for 'CPUUtilization' on instance '22bbs0183-cloudwatch-demo'. A line graph shows the CPU utilization over time, with a peak around 13:30. Below the graph, a table lists various metrics for the instance, including CPUUtilization, CPUCreditUsage, CPUCreditBalance, CPUSurplusCreditBalance, CPUSurplusCreditsCharged, NetworkOut, NetworkPacketsIn, and NetworkPacketsOut. The 'CPUUtilization' metric is selected, and its details are shown in the right pane.

Instance name	Instance ID	Metric name	Alarms
22bbs0183-cloudwatch-demo	i-0dec64c31bcd97...	CPUUtilization	No alarms
22bbs0183-cloudwatch-demo	i-0dec64c31bcd97...	CPUCreditUsage	No alarms
22bbs0183-cloudwatch-demo	i-0dec64c31bcd97...	CPUCreditBalance	No alarms
22bbs0183-cloudwatch-demo	i-0dec64c31bcd97...	CPUSurplusCreditBalance	No alarms
22bbs0183-cloudwatch-demo	i-0dec64c31bcd97...	CPUSurplusCreditsCharged	No alarms
22bbs0183-cloudwatch-demo	i-0dec64c31bcd97...	NetworkOut	No alarms
22bbs0183-cloudwatch-demo	i-0dec64c31bcd97...	NetworkPacketsIn	No alarms
22bbs0183-cloudwatch-demo	i-0dec64c31bcd97...	NetworkPacketsOut	No alarms

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

The screenshot shows the AWS CloudWatch Alarms console. The left sidebar contains navigation links for CloudWatch, Alarms, and Create alarm. The main content area displays the 'Specify metric and conditions' step of the alarm creation wizard. A line graph shows the CPU utilization over time, with a peak around 13:30. The right pane contains the configuration for the alarm, including the namespace 'AWS/EC2', metric name 'CPUUtilization', instance ID 'i-0dec64c31bcd9718f', instance name '22bbs0183-cloudwatch-demo', statistic 'Average', and period '5 minutes'.

Specify metric and conditions

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

Metric

Percent

4.46

2.23

7e-4

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

■ CPUUtilization

Namespaces
AWS/EC2

Metric name
CPUUtilization

Instance ID
i-0dec64c31bcd9718f

Instance name
22bbs0183-cloudwatch-demo

Statistic
Average

Period
5 minutes

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

CloudWatch Alarms Create alarm

Conditions

Threshold type

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

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

Whenever CPU utilization is...
Define the alarm condition.

☒ **Greater**
> threshold

☐ **Greater/Equal**
≥ threshold

☐ **Lower/Equal**
≤ threshold

☐ **Lower**
< threshold

than...
Define the threshold value.

70

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.

2 out of 2

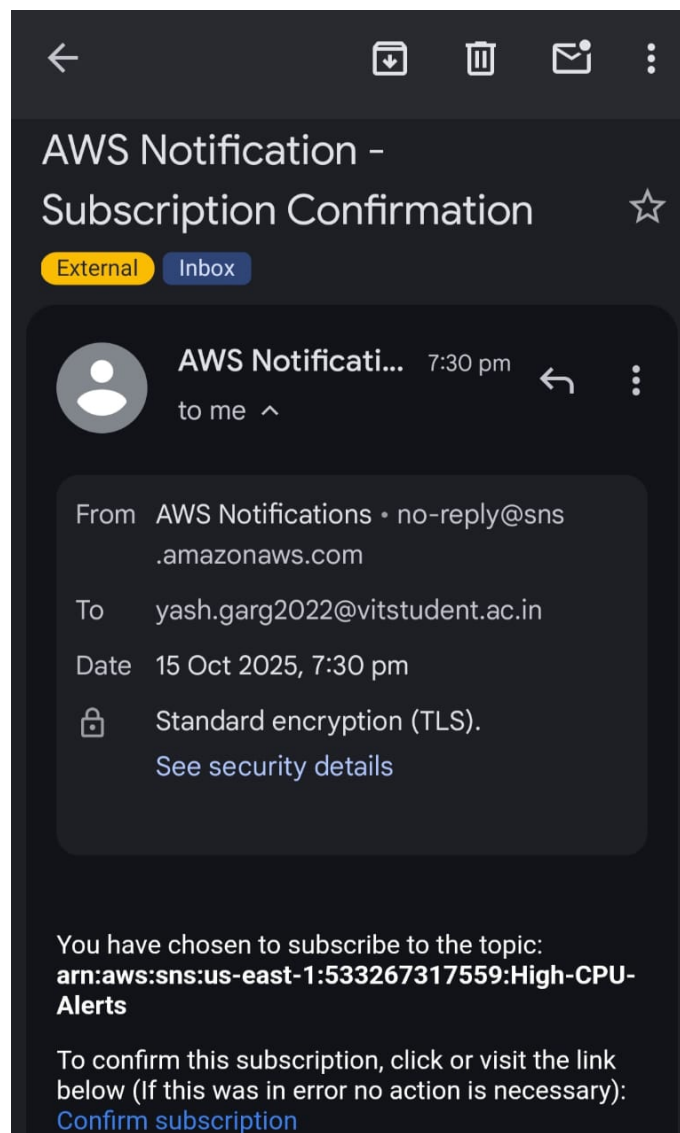
Missing data treatment
How to treat missing data when evaluating the alarm.

Treat missing data as missing

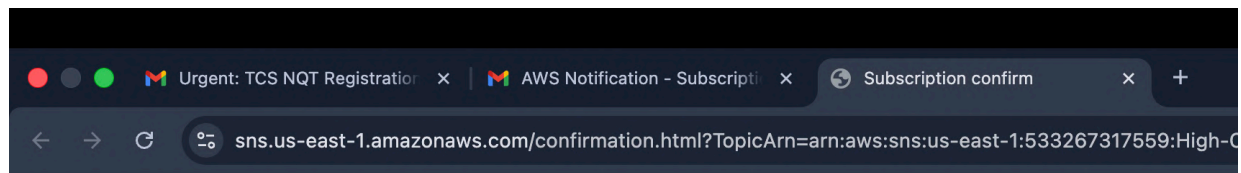
Cancel Next

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

Email received:



Confirmed Subscription:



Simple Notification Service

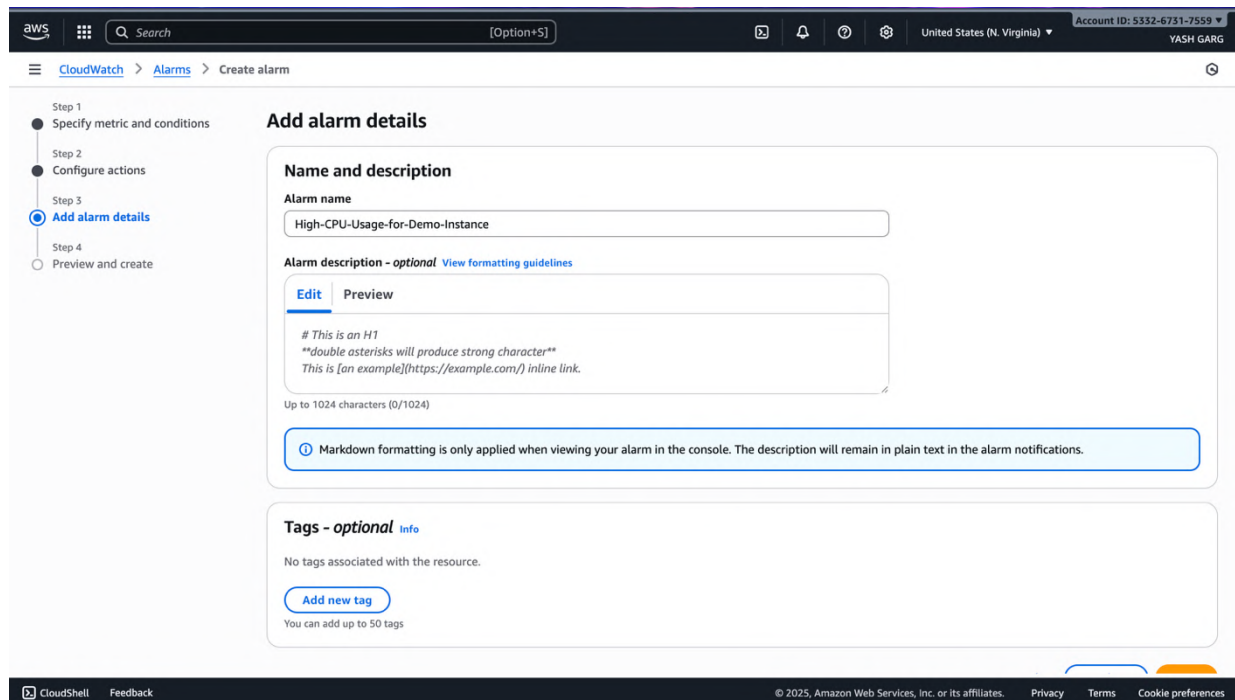
Subscription confirmed!

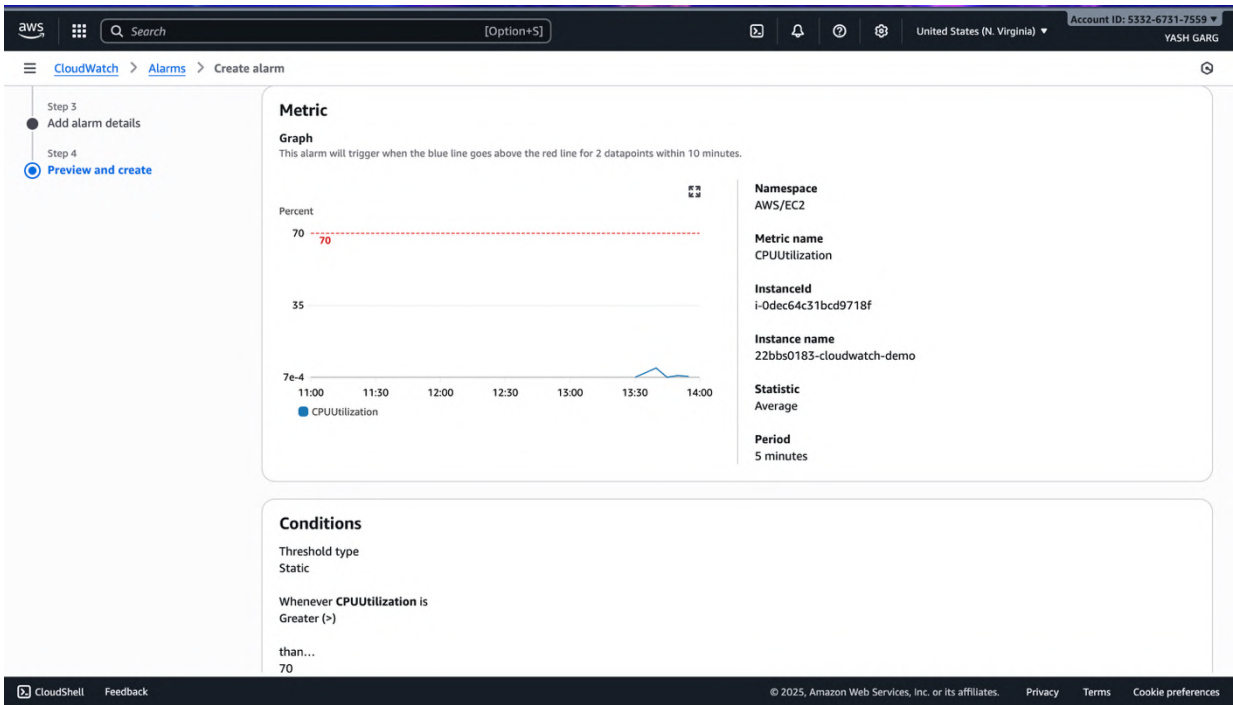
You have successfully subscribed.

Your subscription's id is:

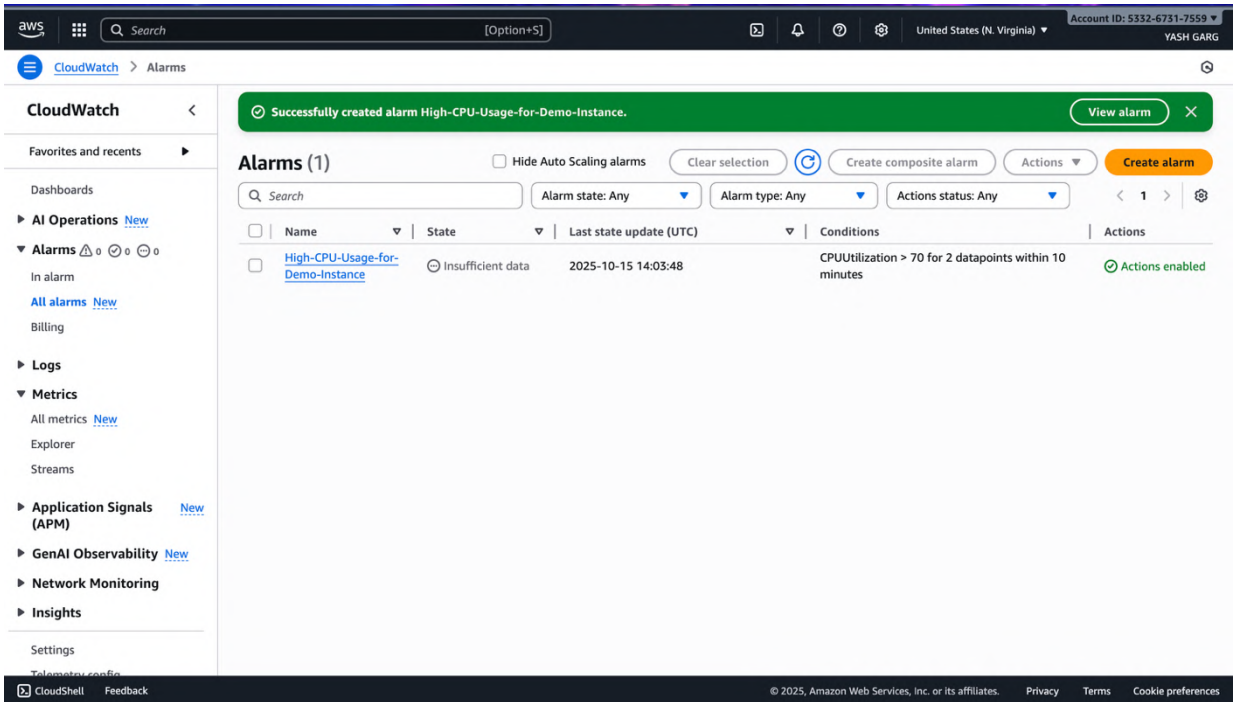
arn:aws:sns:us-east-1:533267317559:High-CPU-Alerts:f1491ec6-1d5e-4adc-a6c3-f8c3c110cbc5

If it was not your intention to subscribe, [click here to unsubscribe](#).

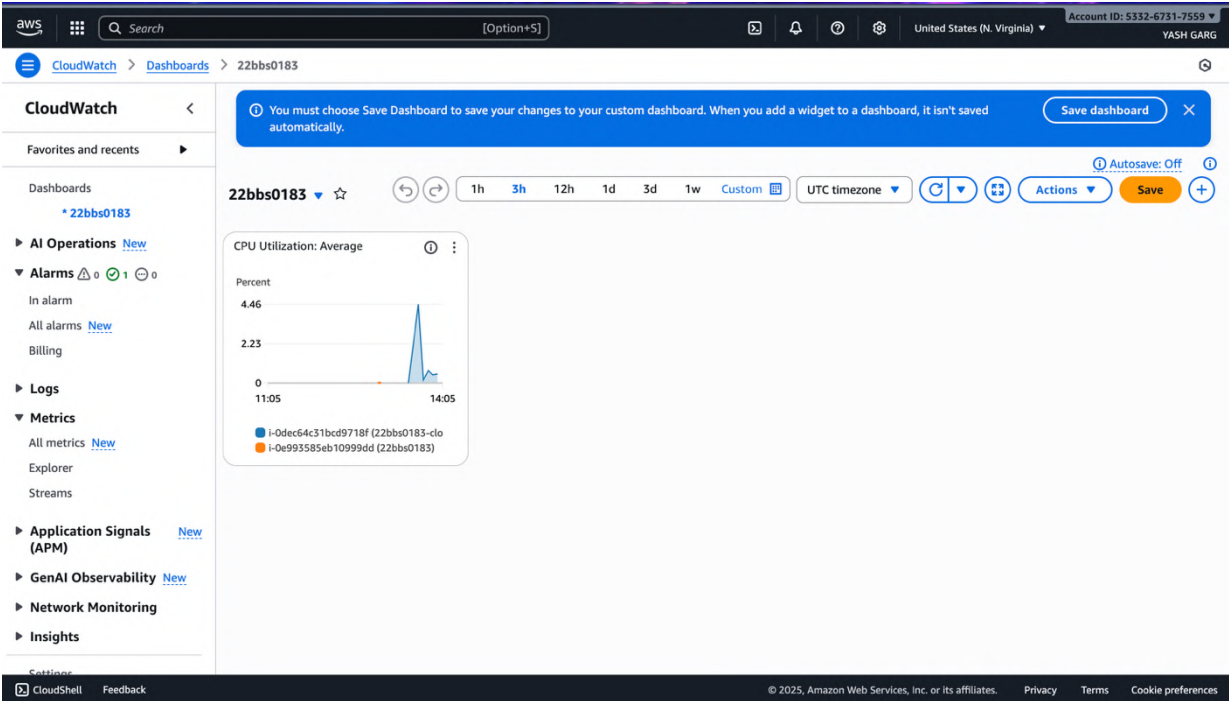
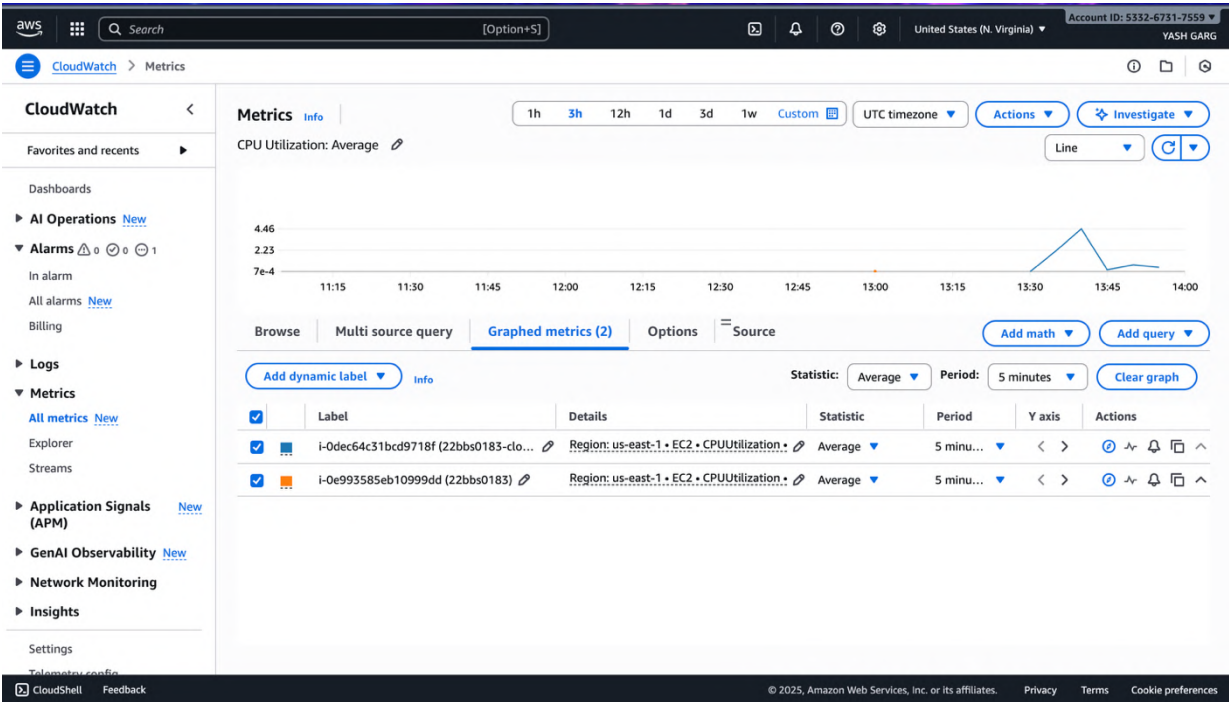




Alarm created:



CloudWatch Dashboard:



Amazon

Search

Option+S

United States (N. Virginia)

Account ID: 5332-6731-7559

YASH GARG

Transaction test succeeded.

Running transaction

Preparing

:

1/1

Installing

:

lksctp-tools-1.0.18-9.amzn2023.0.3.x86_64

1/4

Installing

:

libbsd-0.10.0-7.amzn2023.0.2.x86_64

2/4

Installing

:

Judy-1.0.5-25.amzn2023.0.3.x86_64

3/4

Installing

:

stress-ng-0.15.05-1.amzn2023.x86_64

4/4

Running scriptlet:

:

stress-ng-0.15.05-1.amzn2023.x86_64

4/4

Verifying

:

Judy-1.0.5-25.amzn2023.0.3.x86_64

1/4

Verifying

:

libbsd-0.10.0-7.amzn2023.0.2.x86_64

2/4

Verifying

:

lksctp-tools-1.0.18-9.amzn2023.0.3.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

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

PublicIPs: 13.221.70.55 PrivateIPs: 172.31.30.162

CloudShell

Feedback

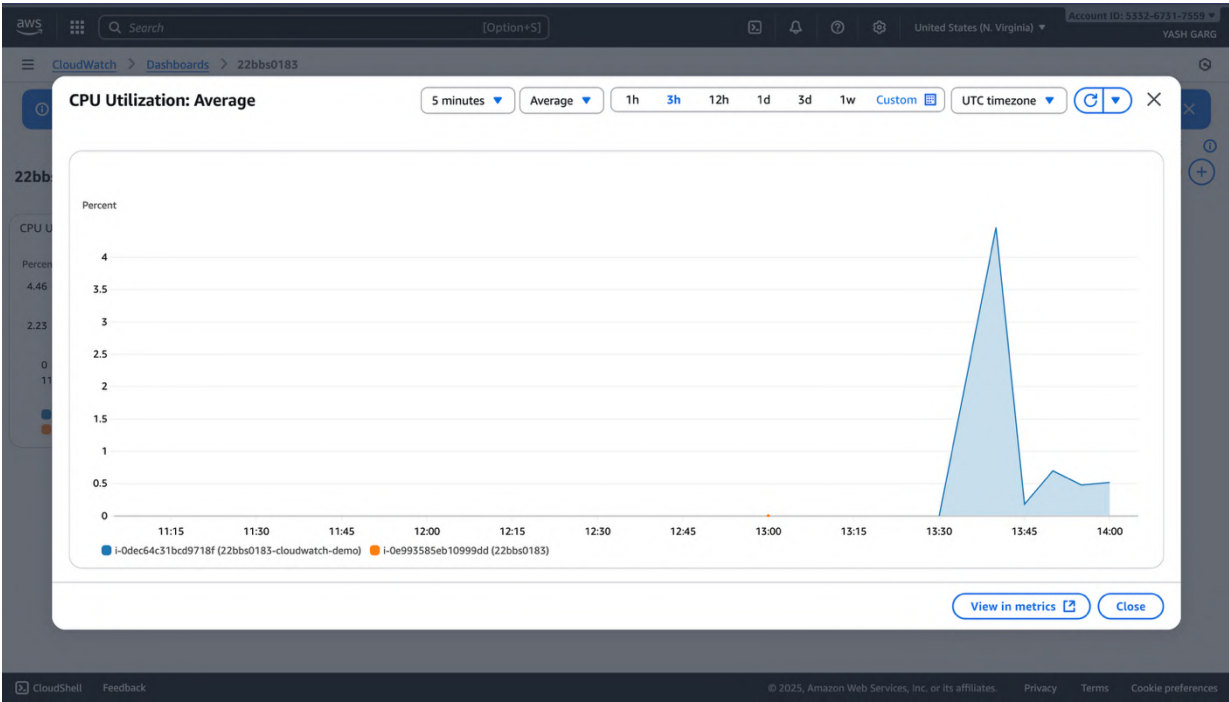
© 2025, Amazon Web Services, Inc. or its affiliates.

Privacy

Terms

Cookie preferences

CPU Utilization Graph (widget):



THANK YOU!