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-

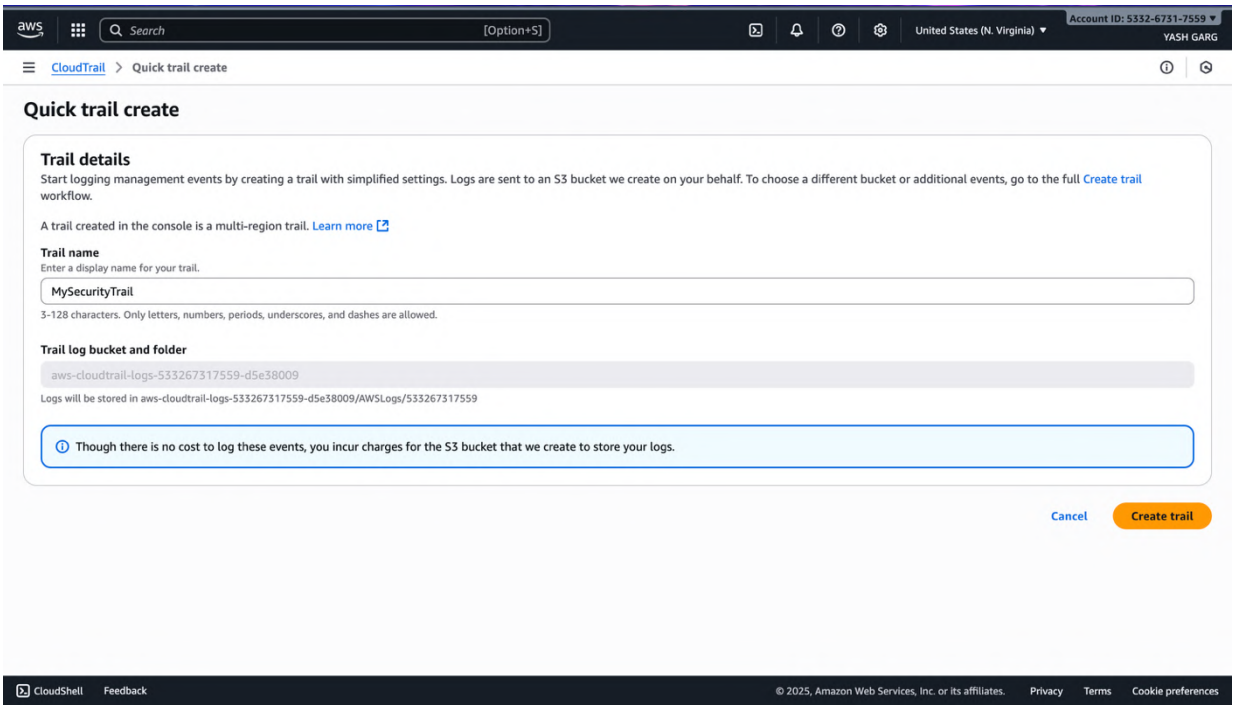
YASH GARG

22BBS0183

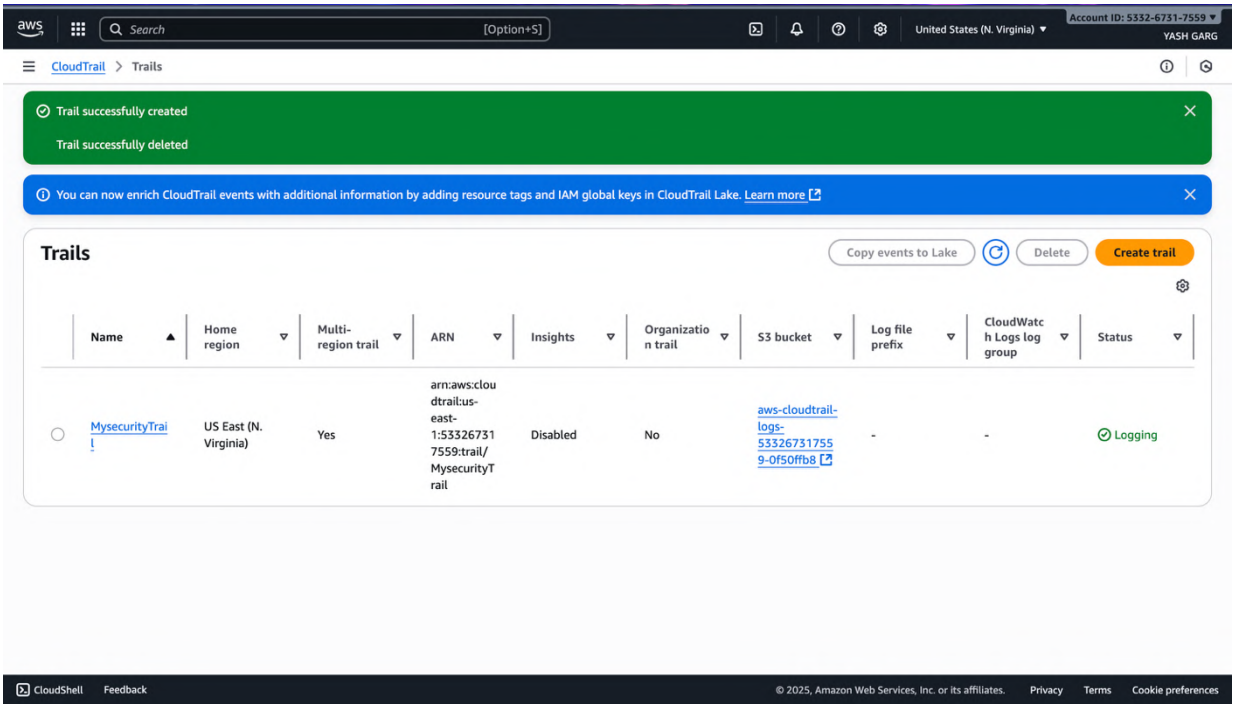
So,

Answer 1)

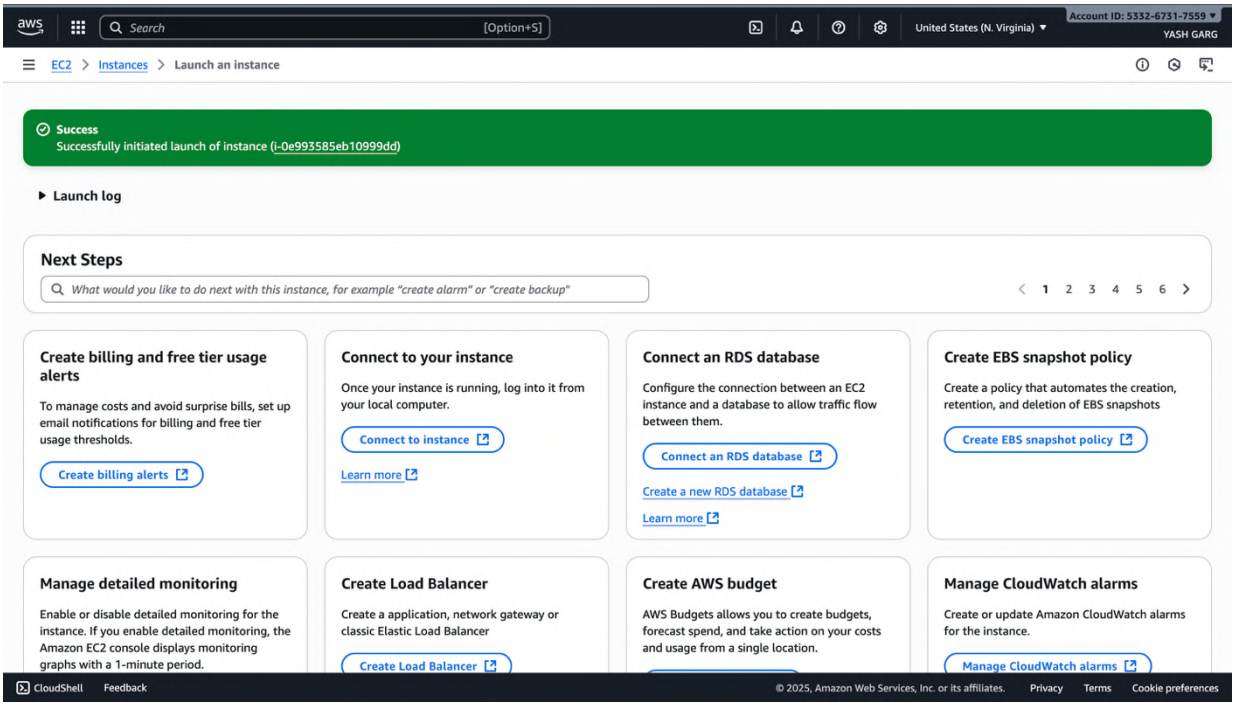
Creating Trail:



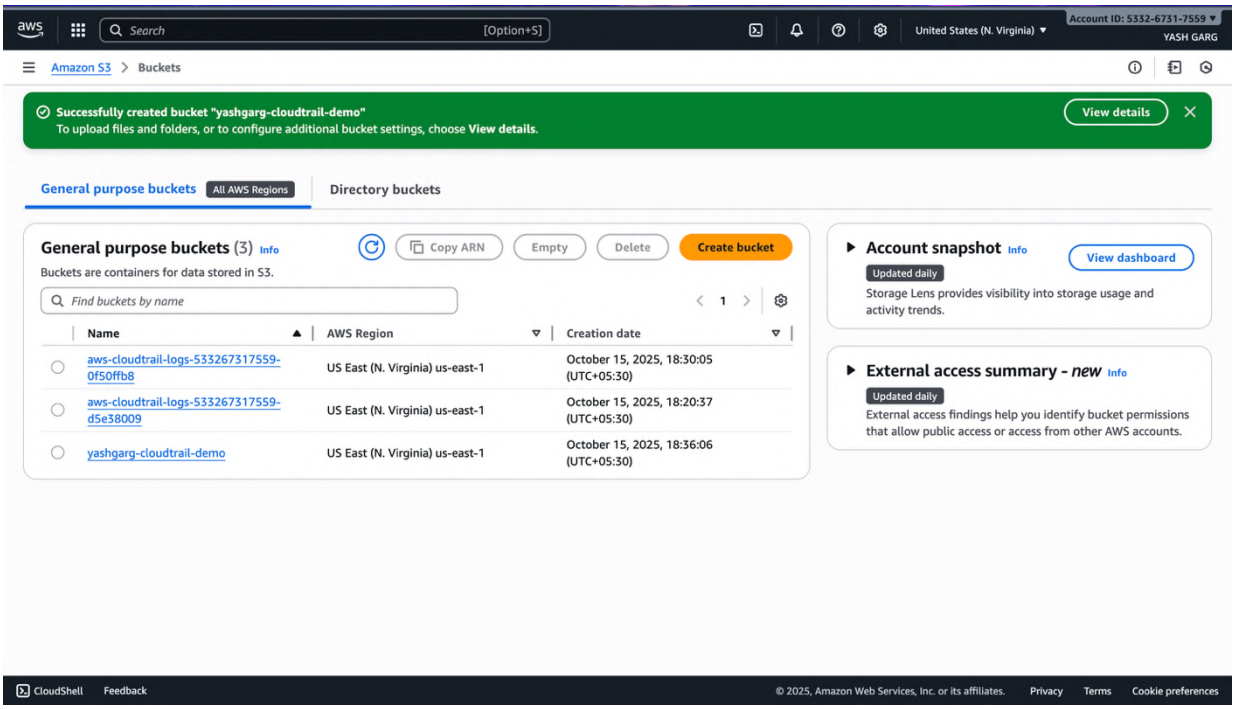
Trail created successfully:



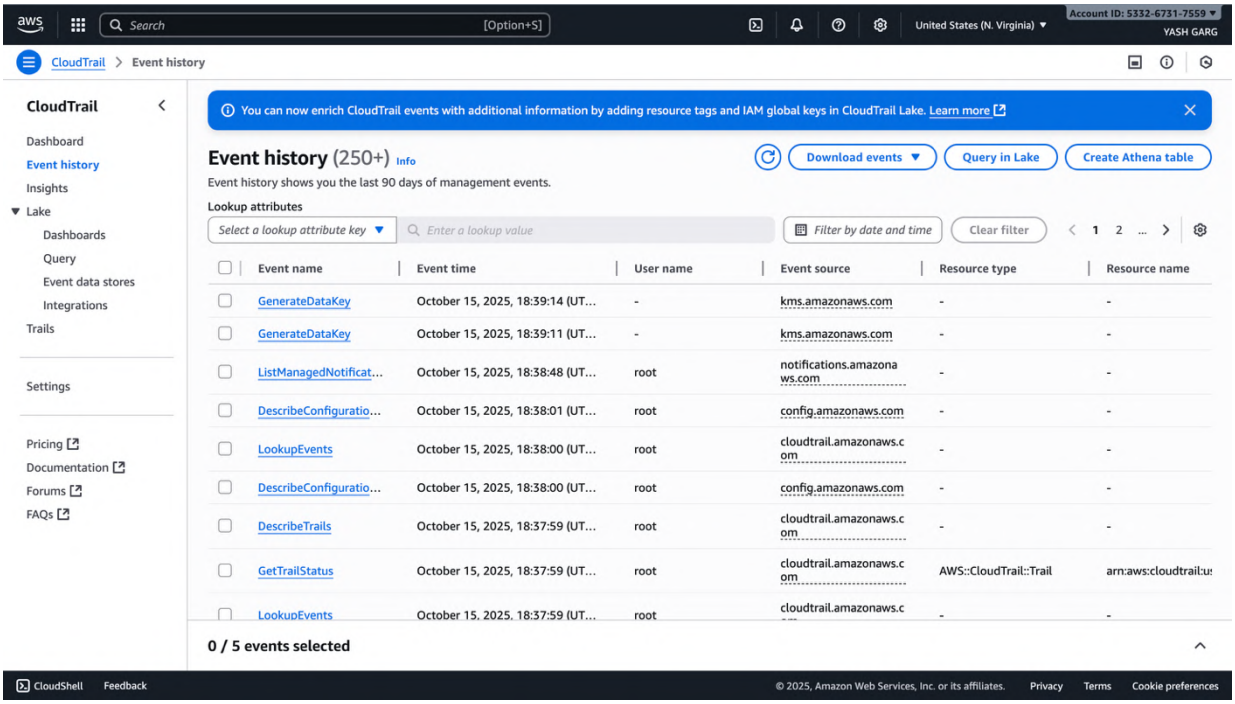
Launched EC2 instance:

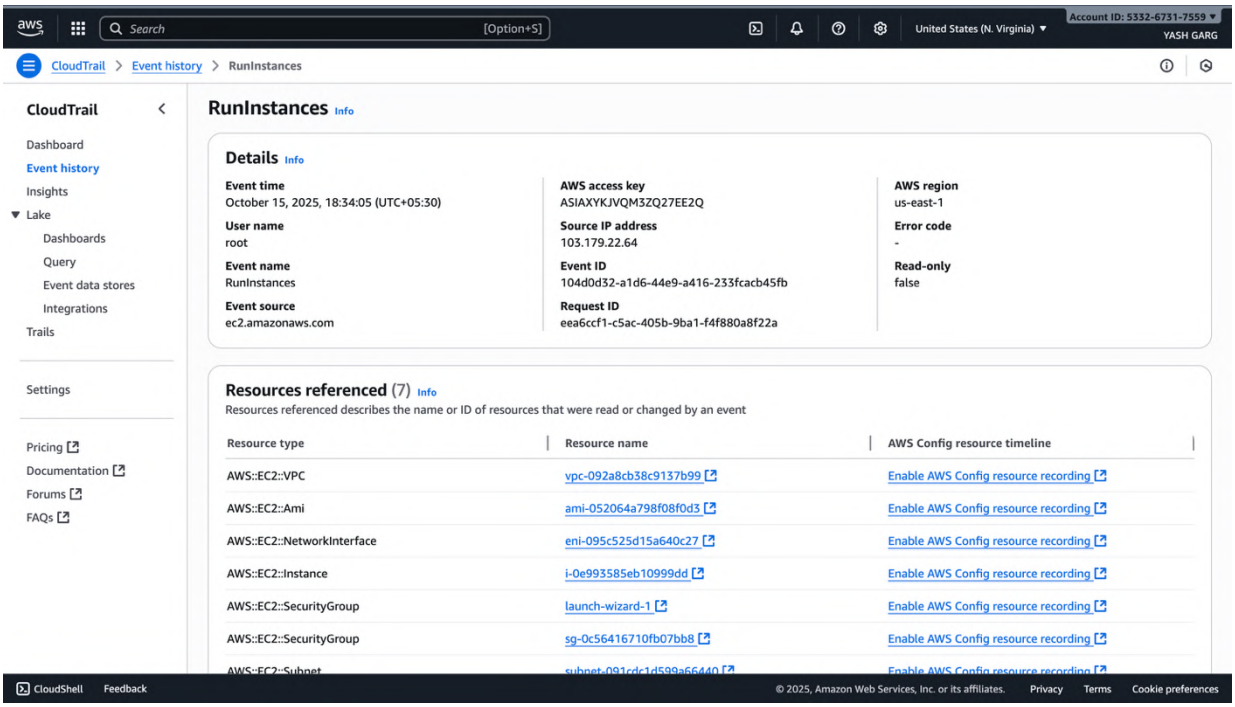


S3 bucket created:

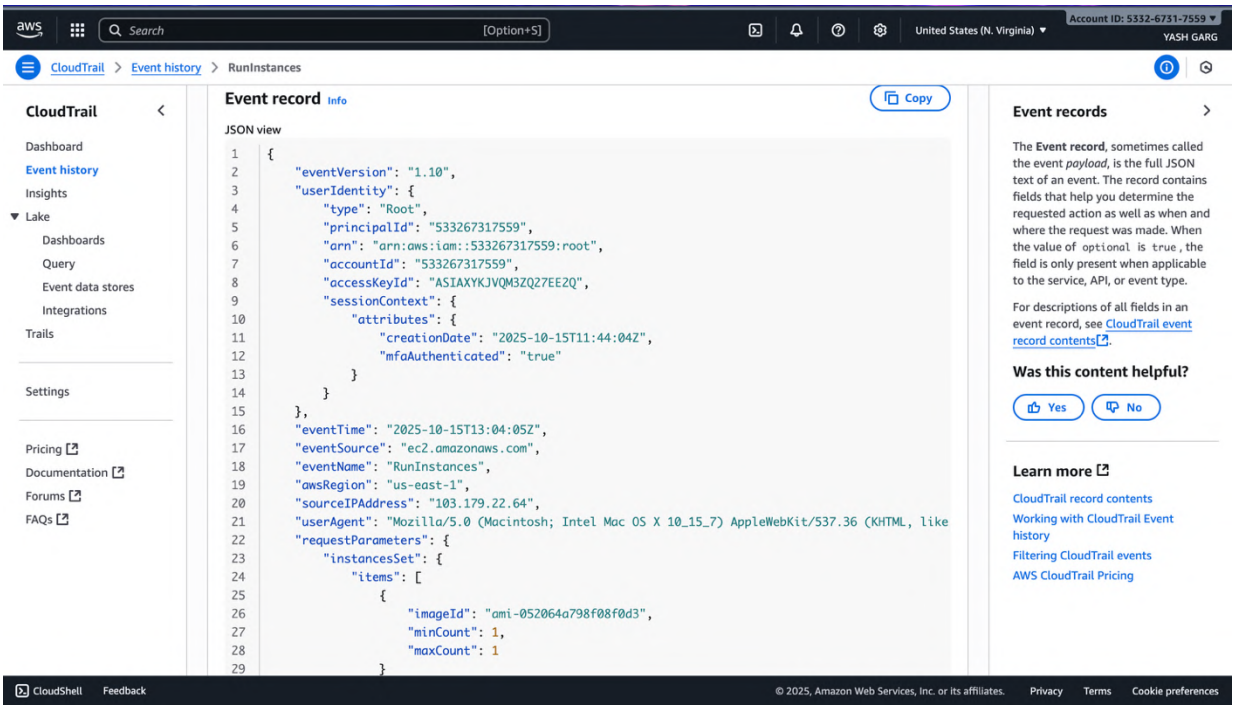


Checking event history:





Viewing event record:



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:

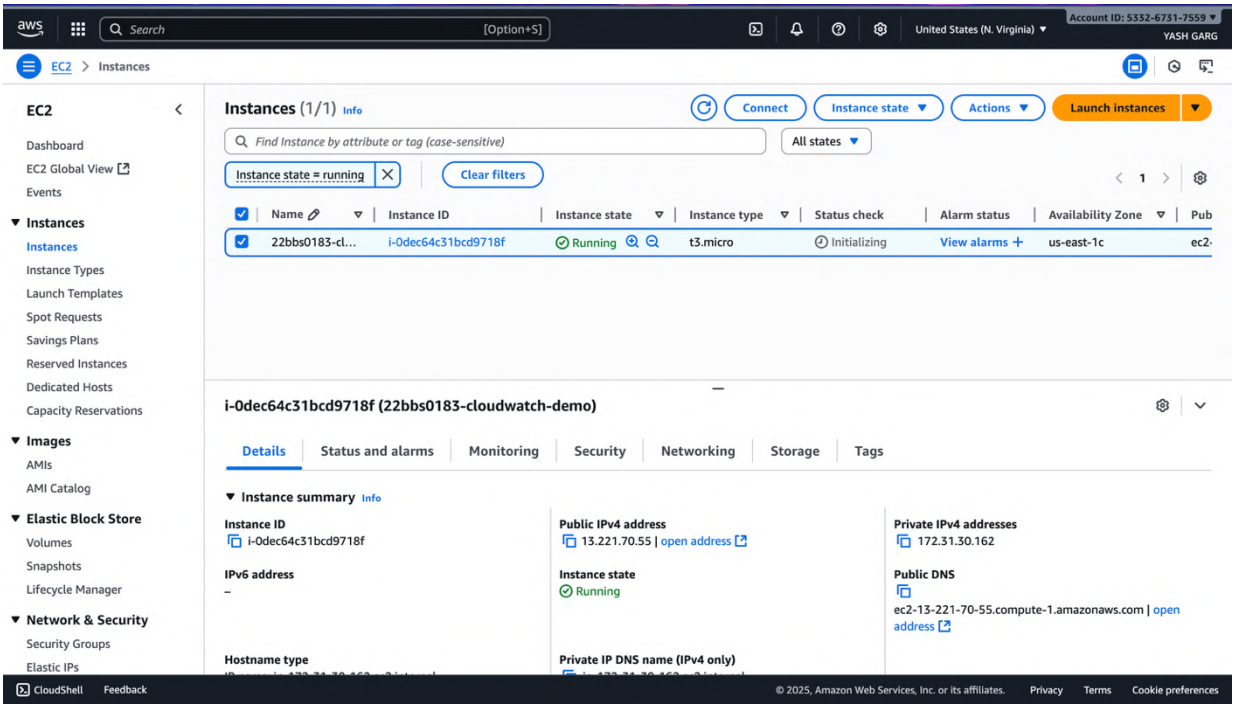
   ```
   sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-ctl \
   -a fetch-config -m ec2 -c file:/opt/aws/amazon-cloudwatch-agent/bin/config.json -s
   ```

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

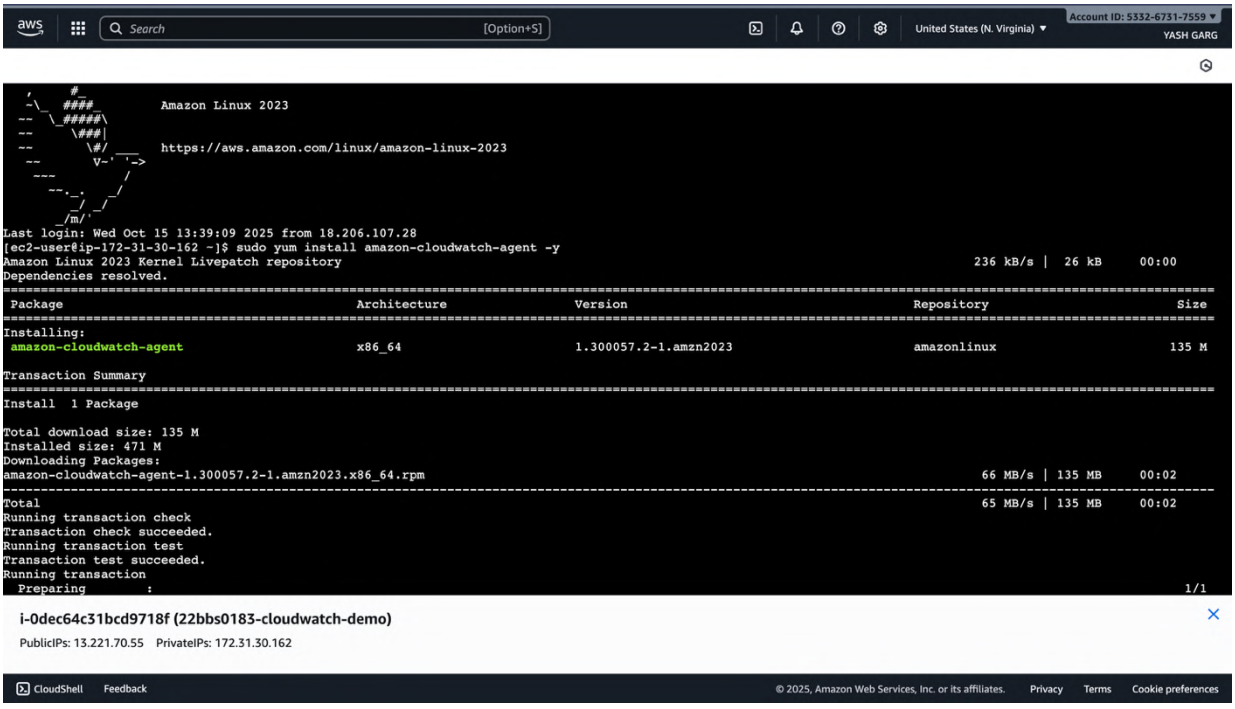
6. Create a **CloudWatch Alarm**:
   - Metric: CPUUtilization
   - Condition: >70% for 2 consecutive periods
   - Notification: via **SNS topic** (send email alert).

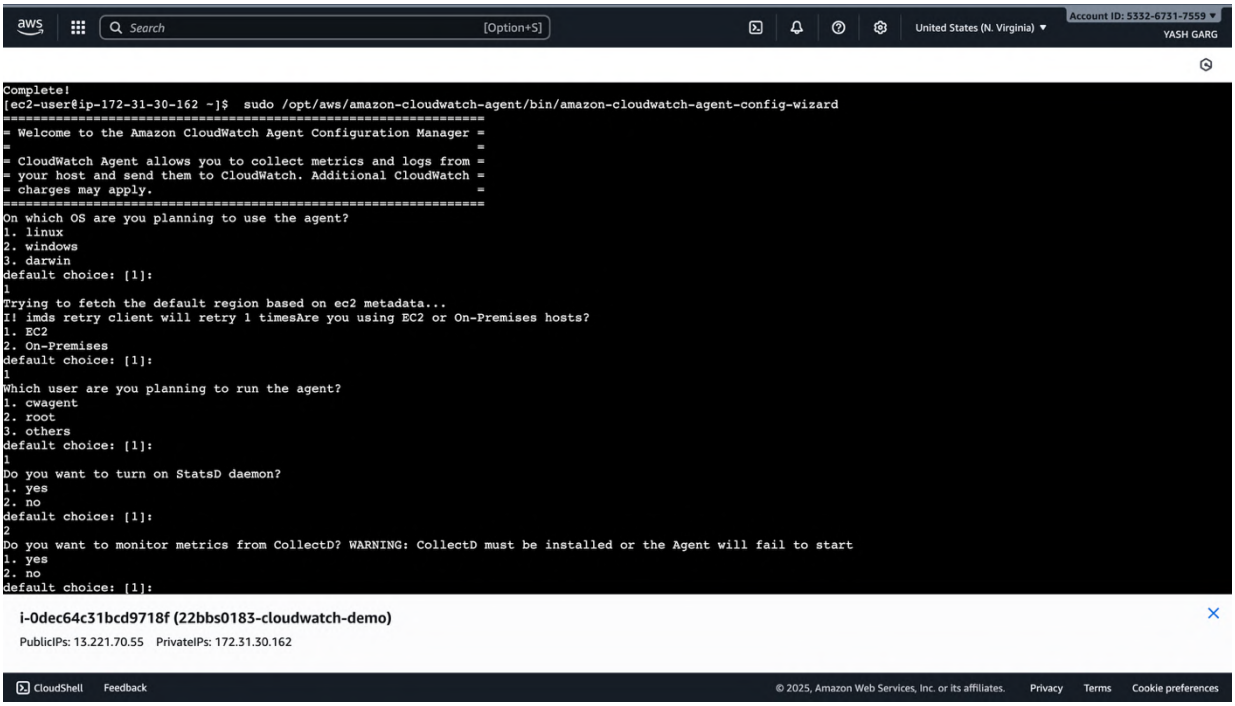
Answer2)

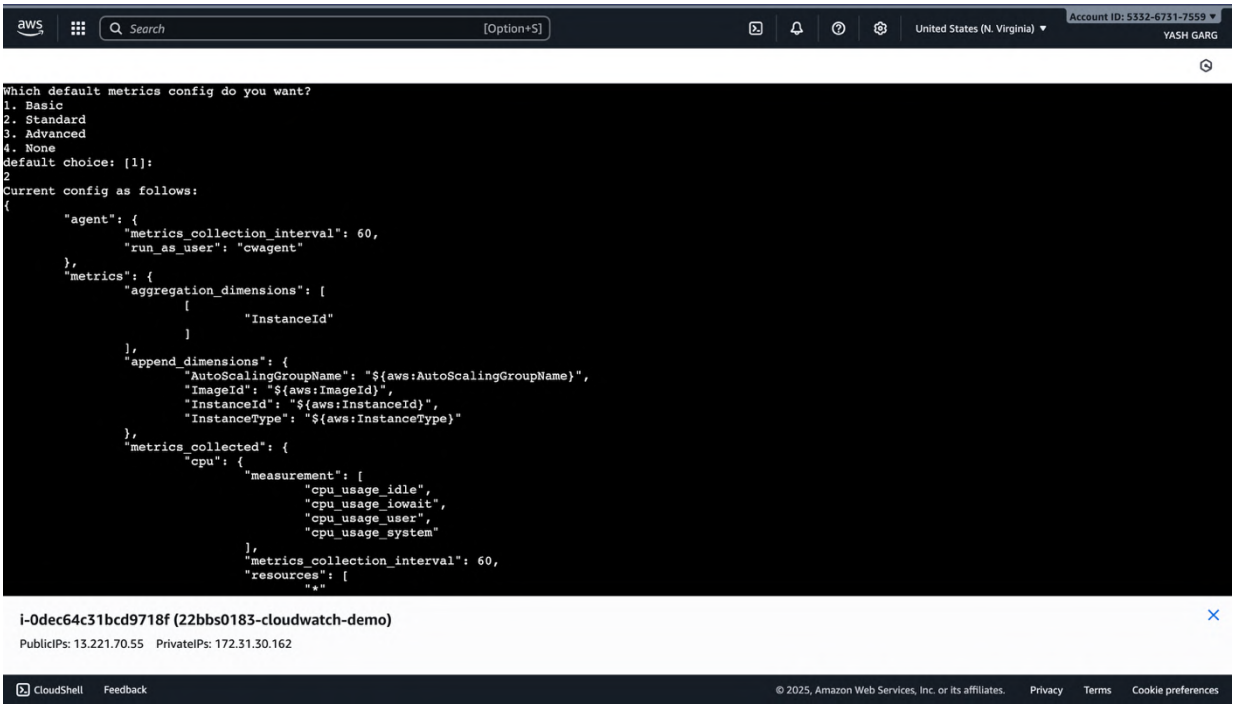
Launched EC2 instance:

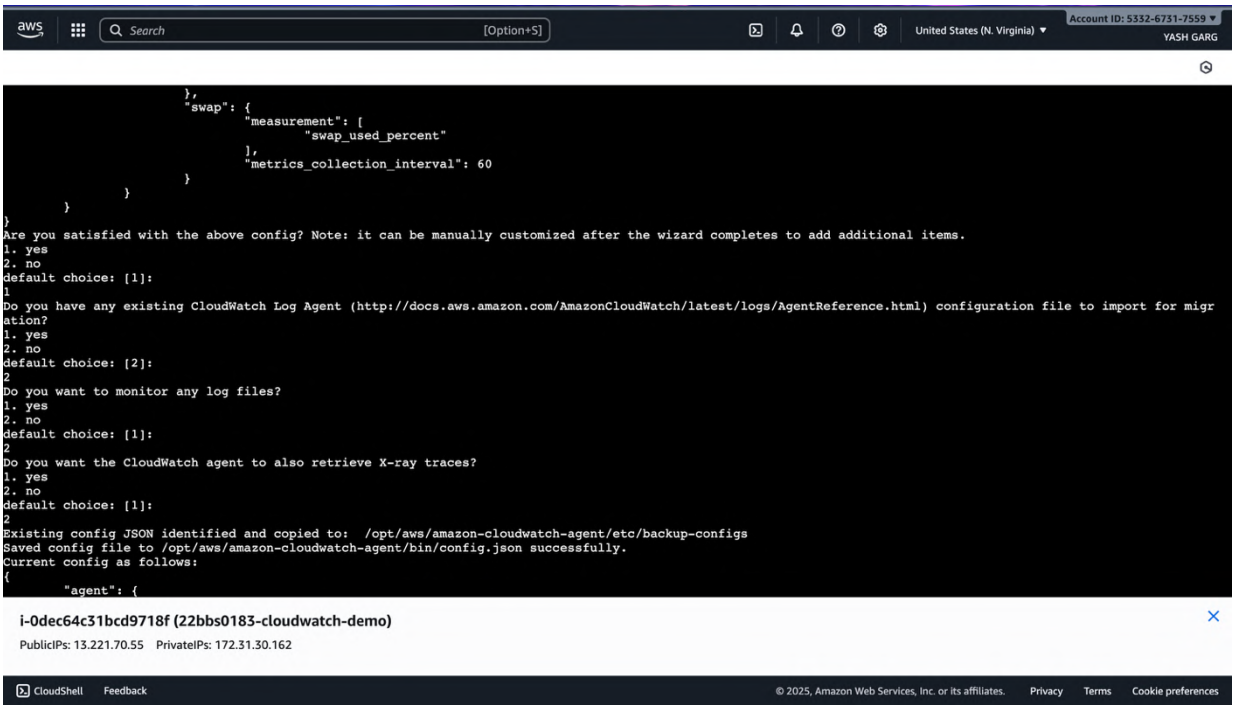


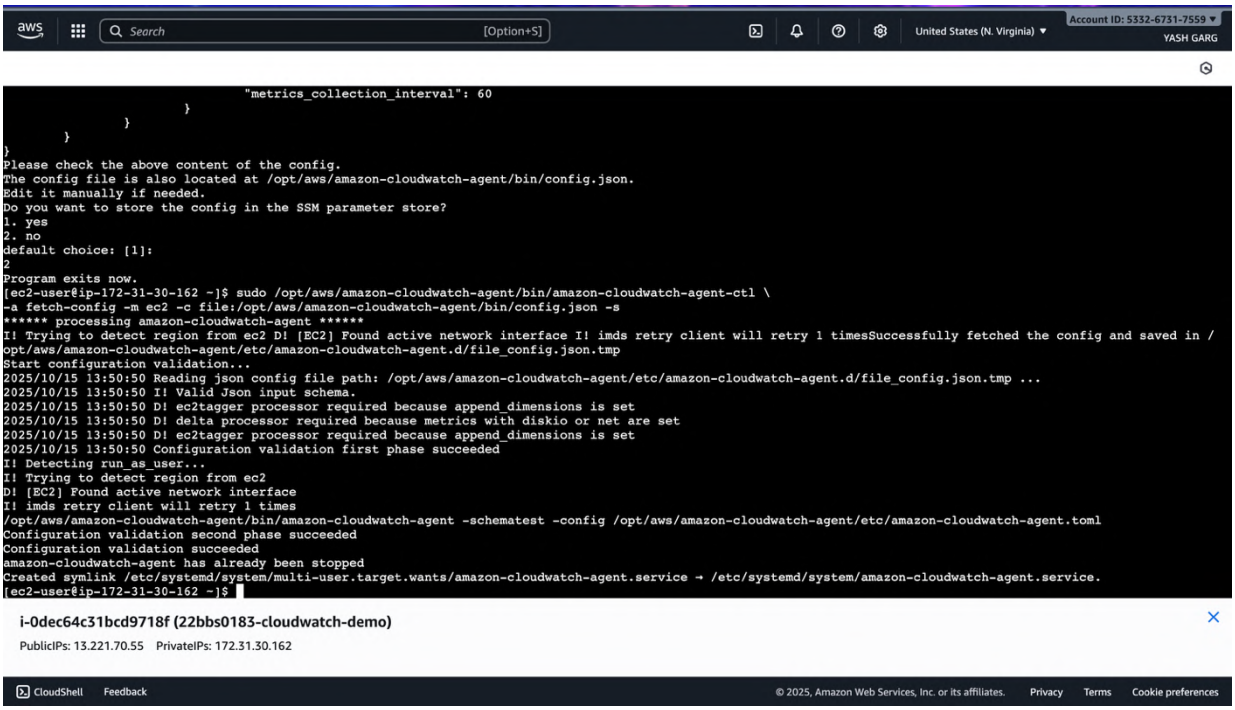
Installing and configuring CloudWatch agent:



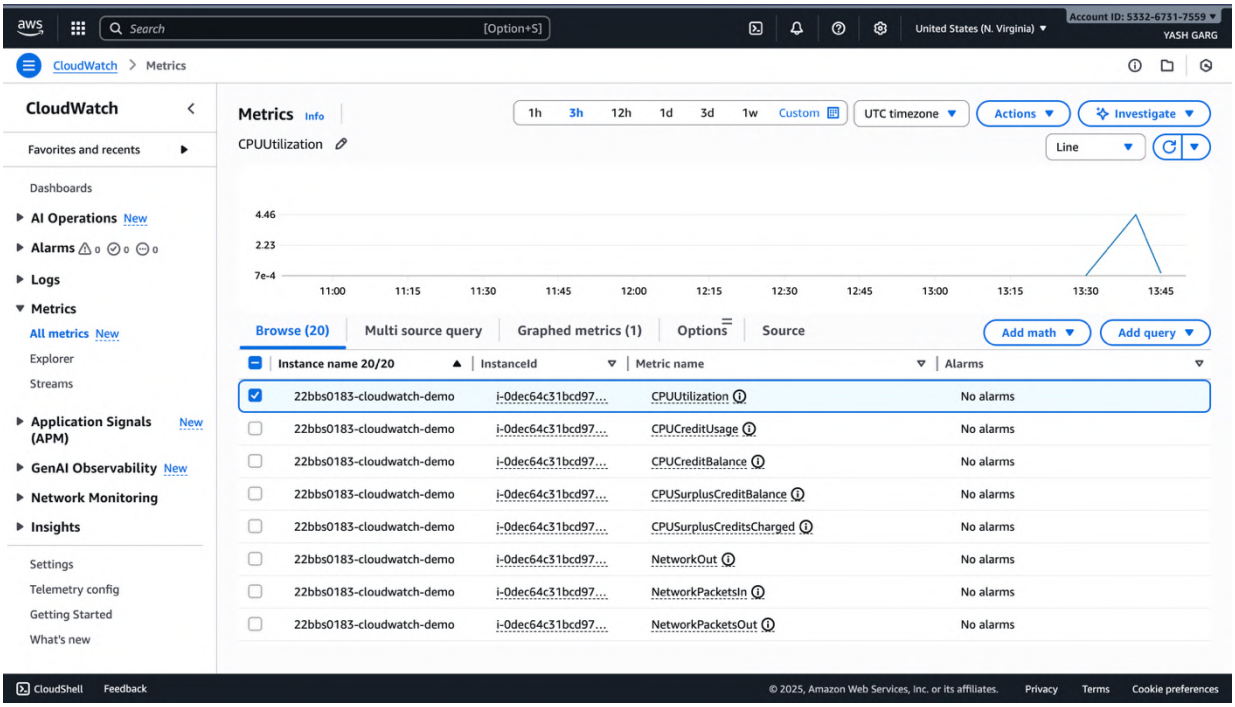

aws
Search
[Option+S]
United States (N. Virginia)
Account ID: 5332-6731-7559
YASH GARG
Complete!
[ec2-user@ip-172-31-30-162 ~]$ sudo /opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-config-wizard
= Welcome to the Amazon CloudWatch Agent Configuration Manager =
= CloudWatch Agent allows you 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...
I! 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]:
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


aws
Search
[Option+S]
United States (N. Virginia)
Account ID: 5332-6731-7559
YASH GARG
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)
PublicIPs: 13.221.70.55 PrivateIPs: 172.31.30.162
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

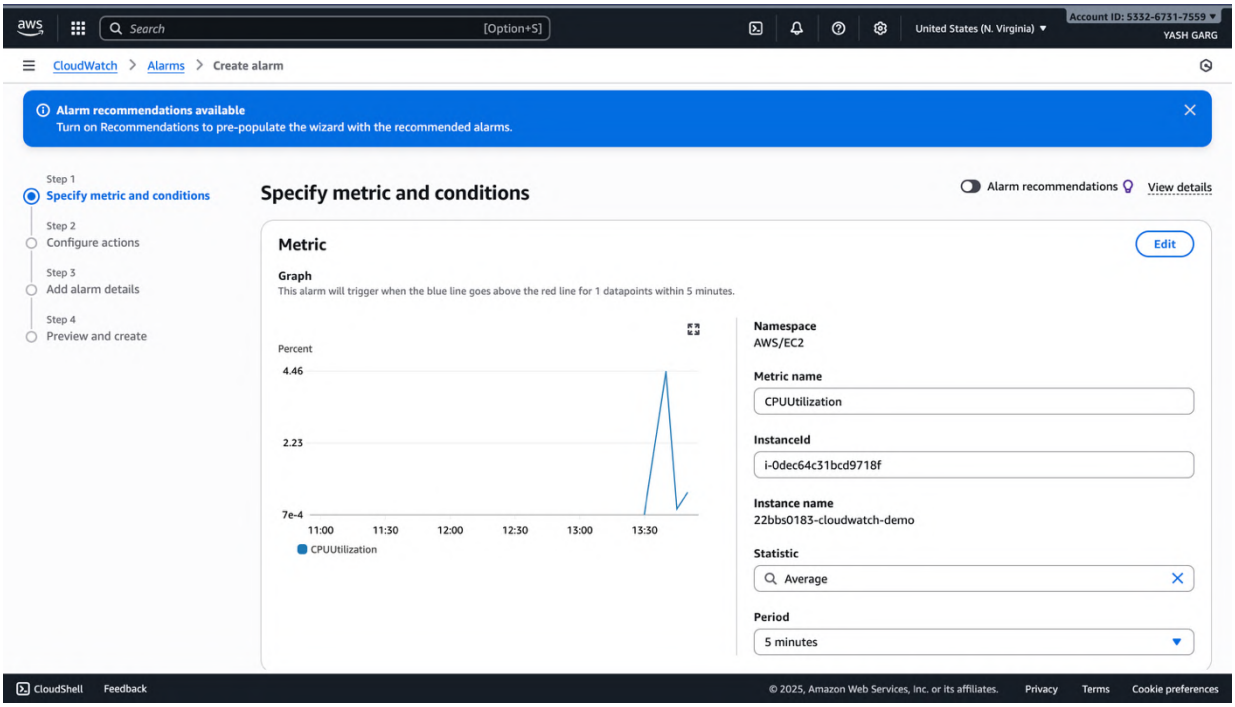

aws
Search
[Option+S]
United States (N. Virginia)
Account ID: 5332-6731-7559
YASH GARG
},
"swap": {
"measurement": [
"swap_used_percent"
],
"metrics_collection_interval": 60
}
}
}
}
Are you satisfied with the above config? Note: it can be manually customized after the wizard completes to add additional 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": {
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

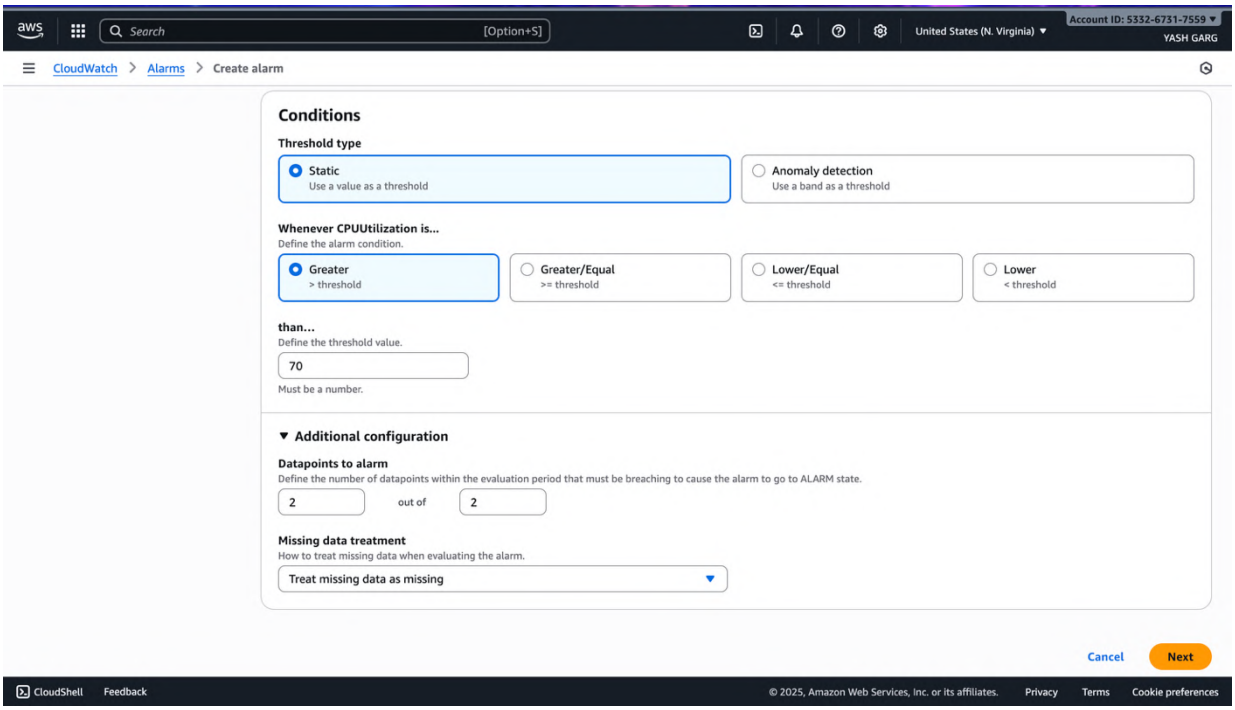

aws
Search
[Option+S]
United States (N. Virginia)
Account ID: 5332-6731-7559
YASH GARG
"metrics_collection_interval": 60
}
}
}
}
Please check the above content of the config.
The config file is also located at /opt/aws/amazon-cloudwatch-agent/bin/config.json.
Edit it manually if needed.
Do you want to 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:

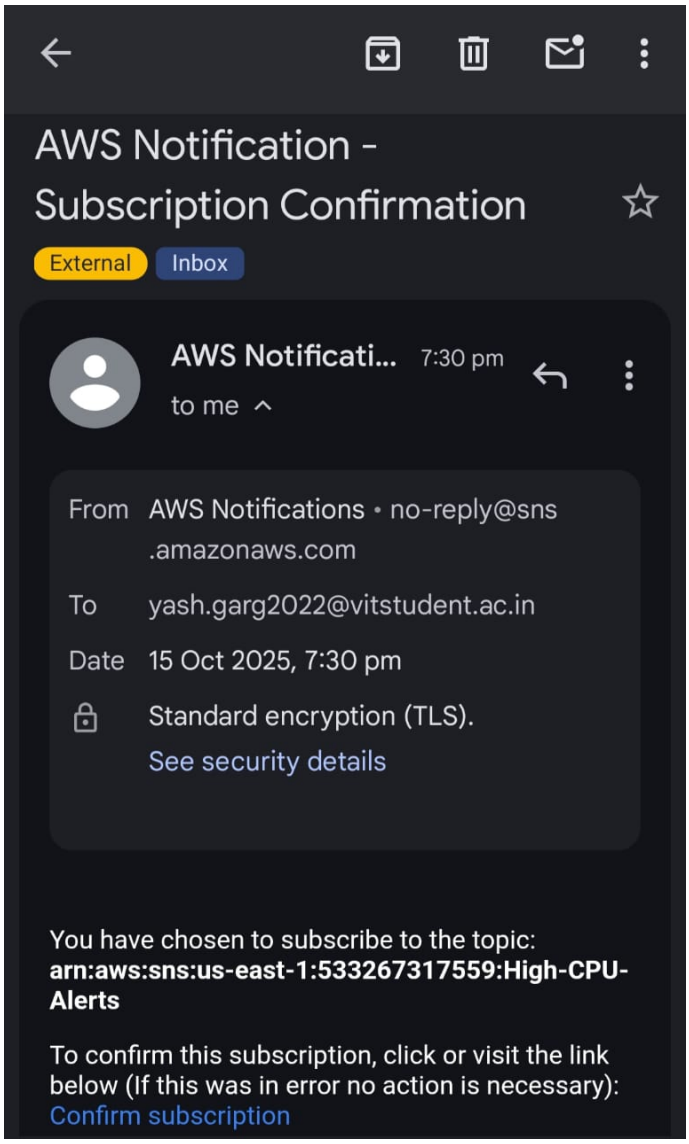


Specifying conditions for alarm “>70% for 2 consecutive periods”

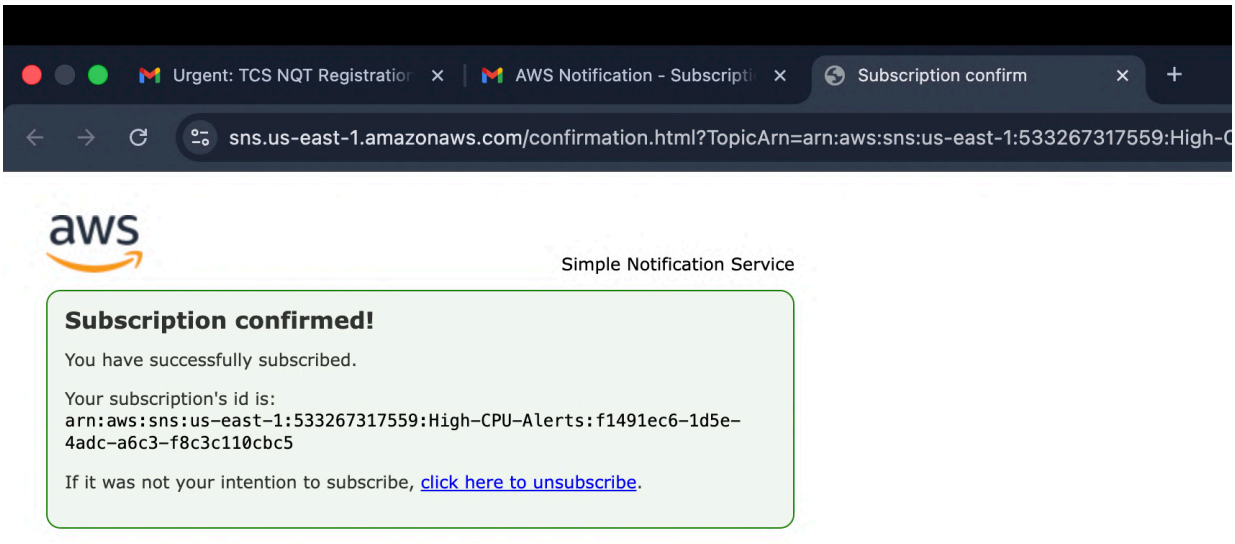


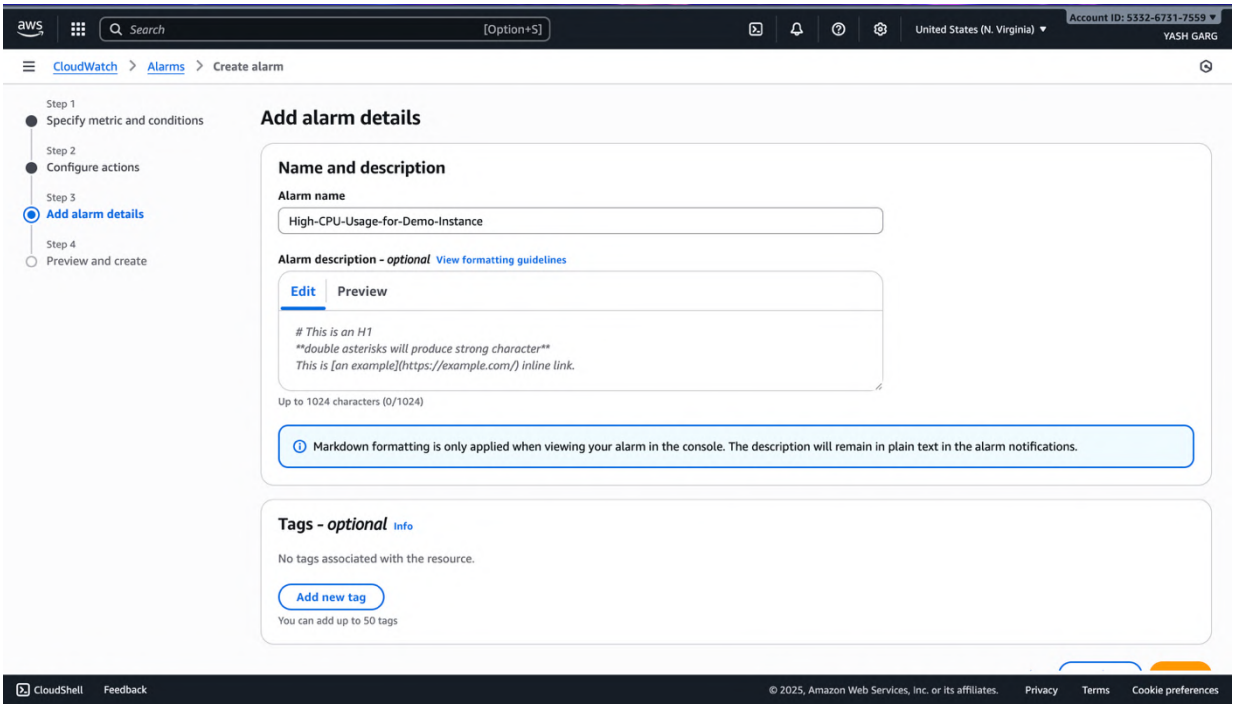


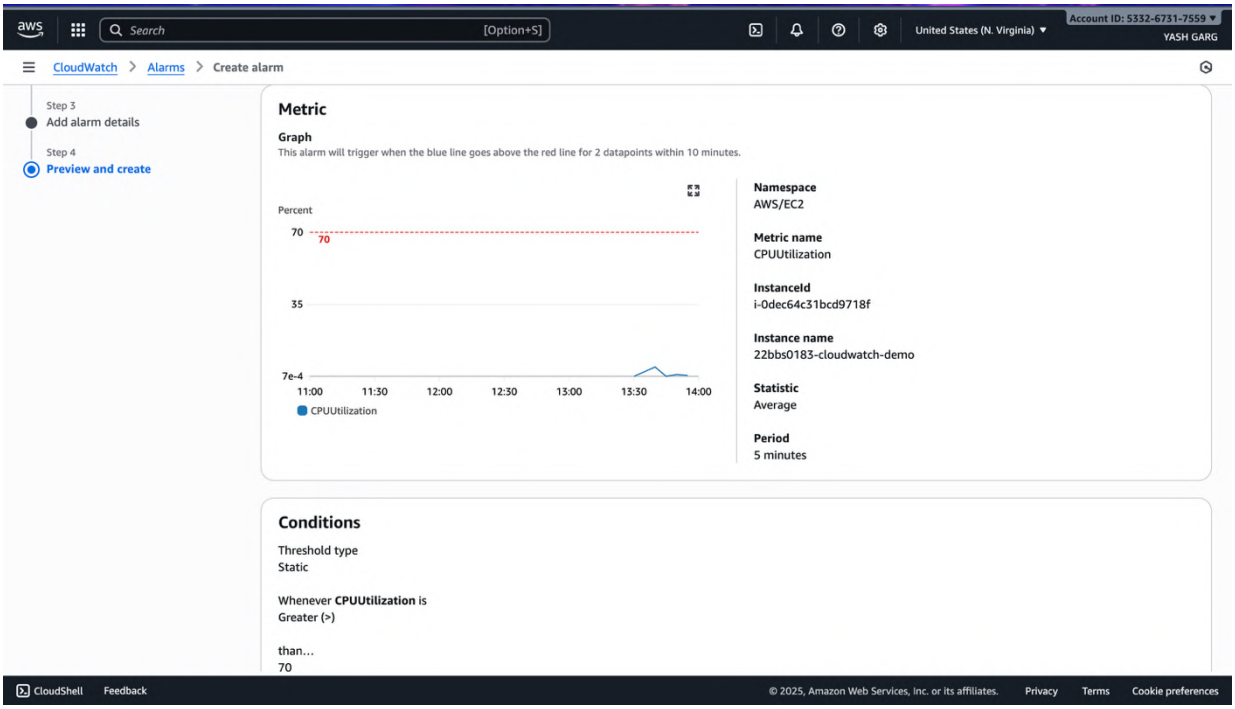
Email received:



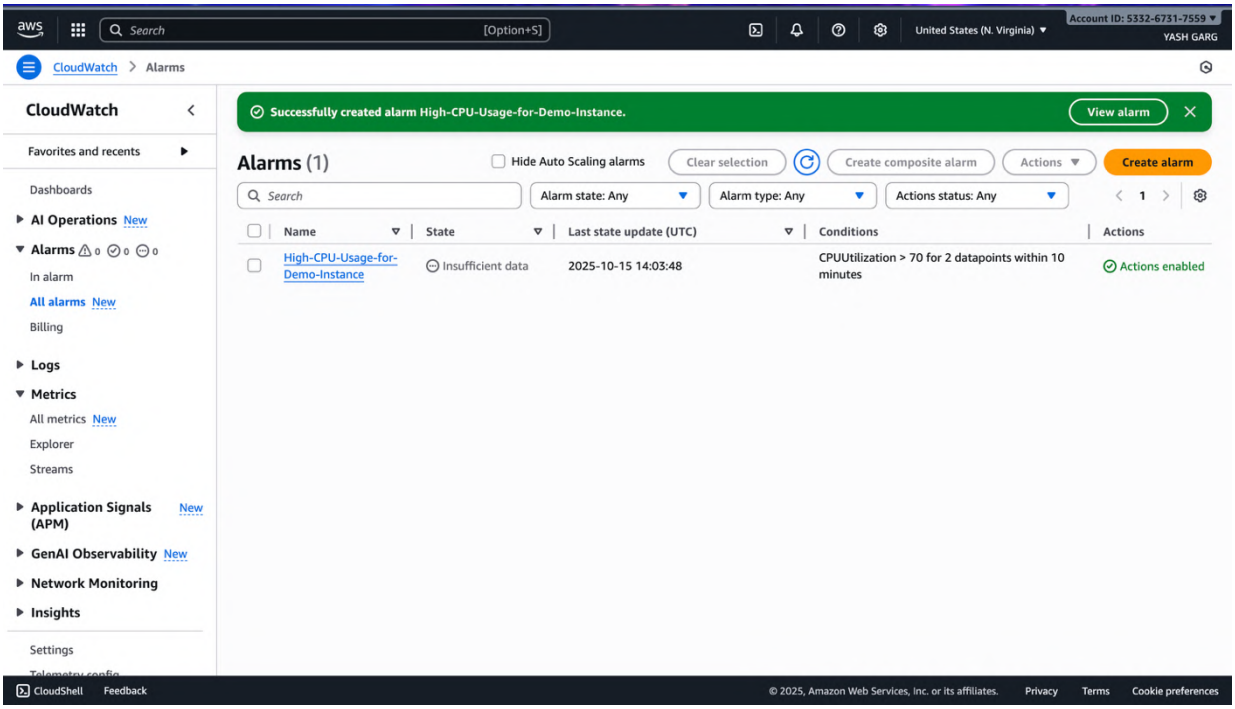
Confirmed Subscription:



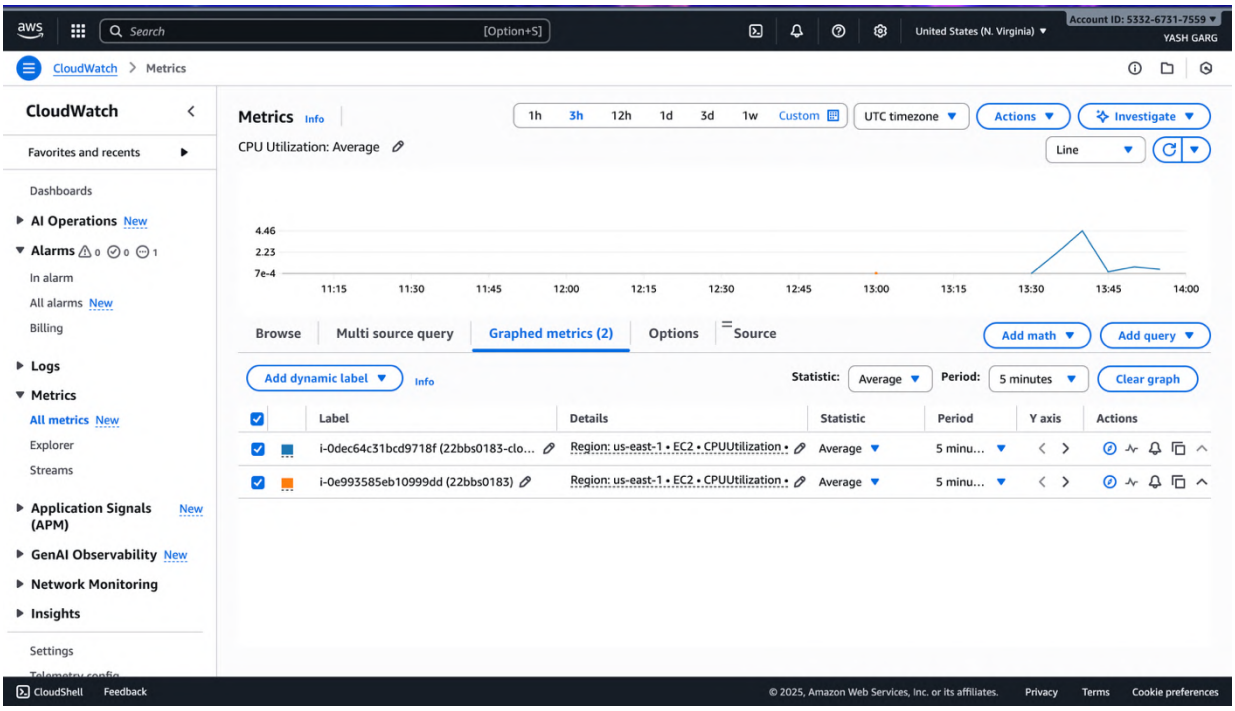


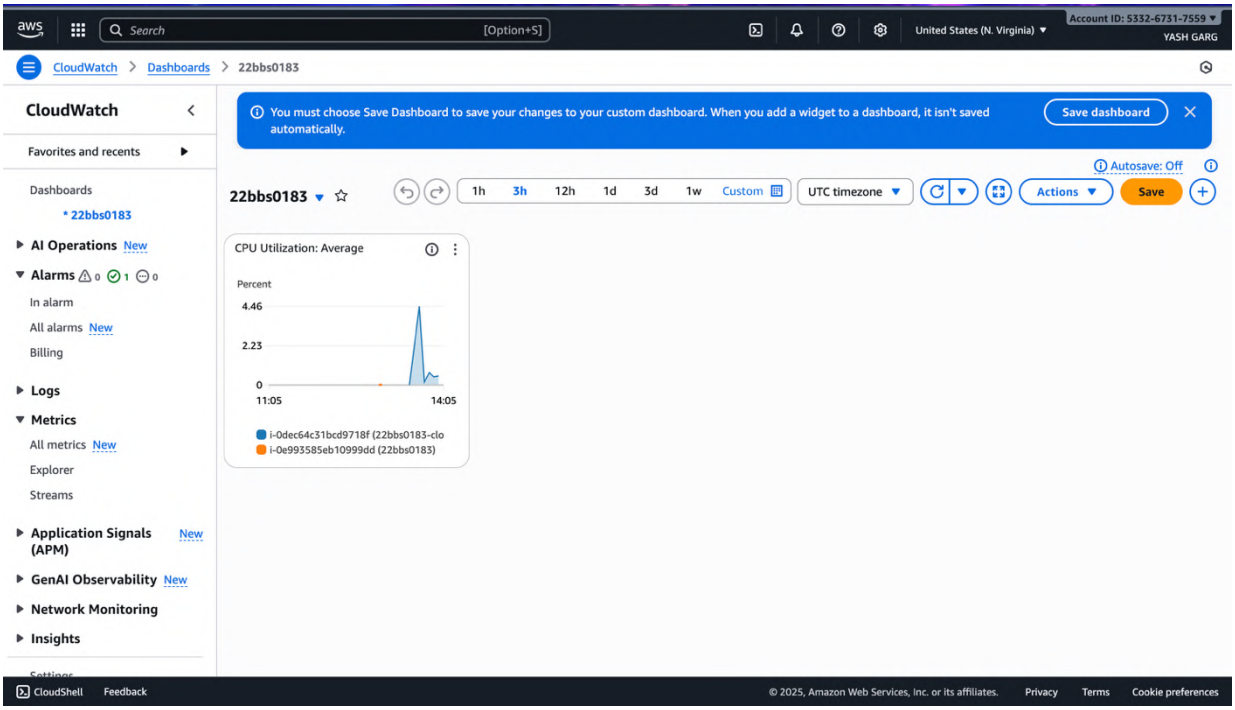


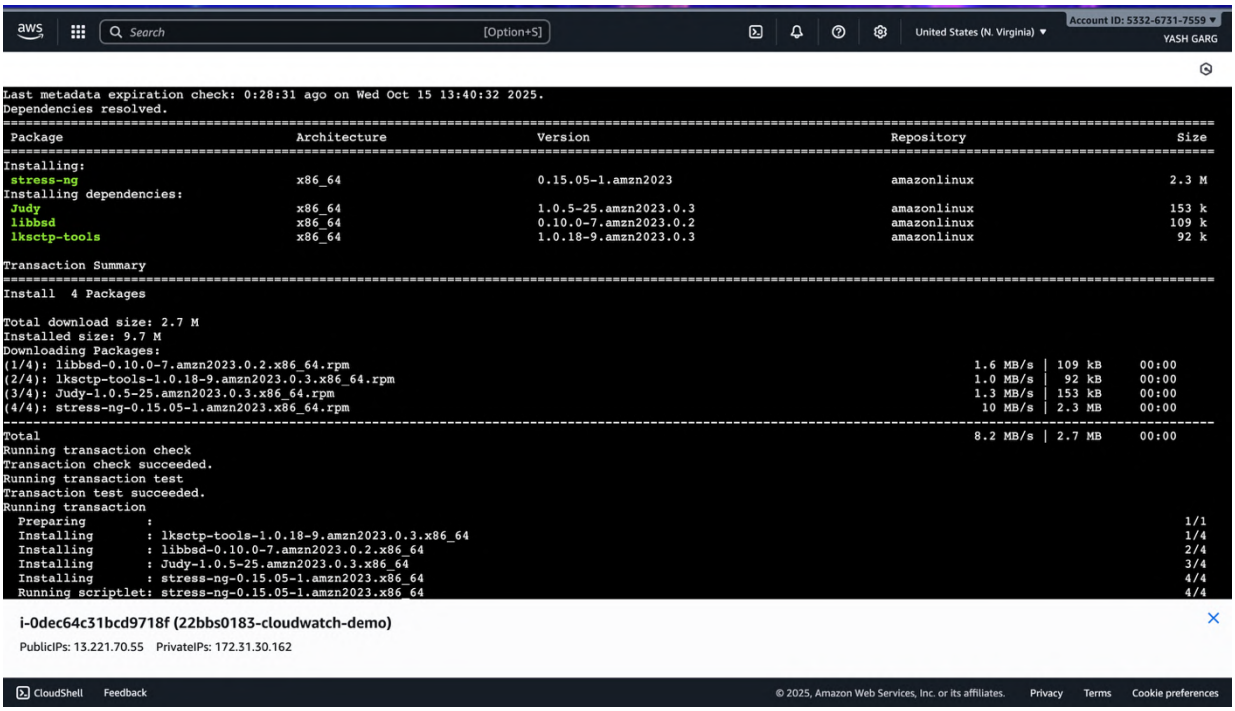
Alarm created:

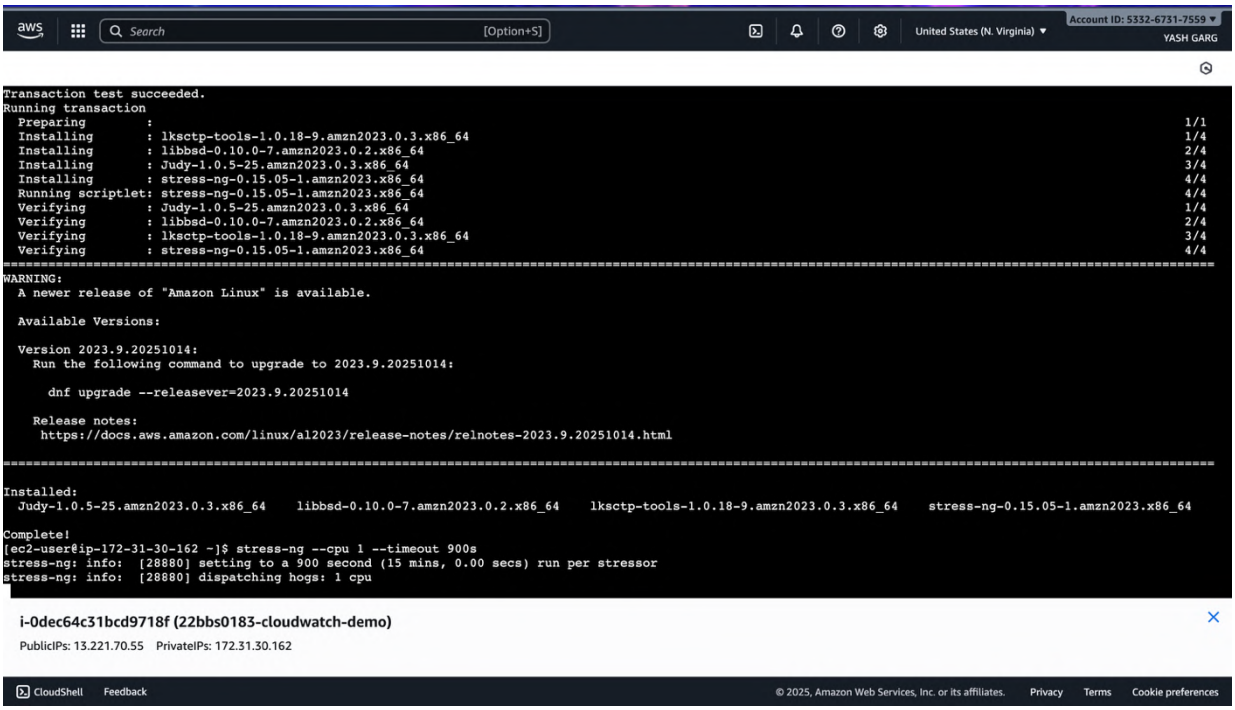


CloudWatch Dashboard:

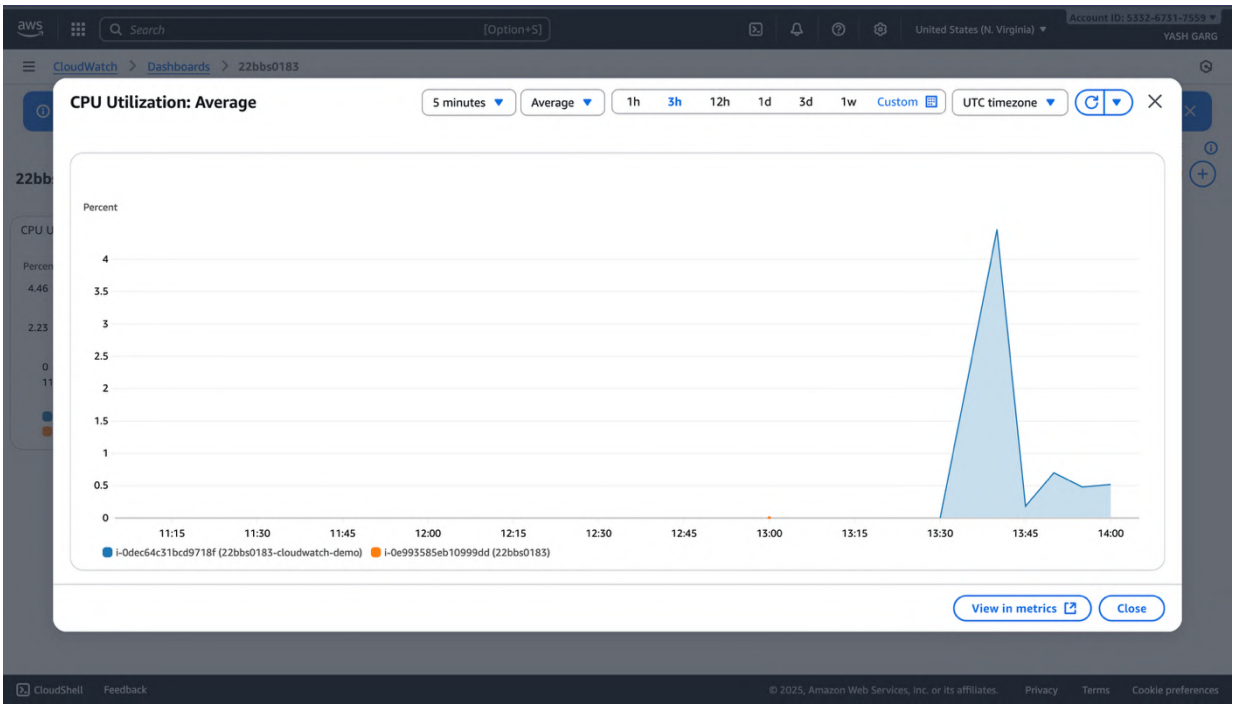





aws
Search
[Option+S]
United States (N. Virginia)
Account ID: 5332-6731-7559
YASH GARG
Last metadata expiration check: 0:28:31 ago on Wed Oct 15 13:40:32 2025.
Dependencies resolved.
Package Architecture Version Repository Size
Installing:
stress-ng x86_64 0.15.05-1.amzn2023 amazonlinux 2.3 M
Installing dependencies:
Judy x86_64 1.0.5-25.amzn2023.0.3 amazonlinux 153 k
libbsd x86_64 0.10.0-7.amzn2023.0.2 amazonlinux 109 k
lksctp-tools x86_64 1.0.18-9.amzn2023.0.3 amazonlinux 92 k
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.rpm 1.3 MB/s | 153 kB 00:00
(4/4): stress-ng-0.15.05-1.amzn2023.x86_64.rpm 10 MB/s | 2.3 MB 00:00
Total 8.2 MB/s | 2.7 MB 00:00
Running transaction check
Transaction check succeeded.
Running transaction test
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
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


aws
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!