



VIT®

Vellore Institute of Technology

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

SCOPE

FALL SEMESTER 2025-2026

LAB ASSESSMENT -5

Slot: L13+L14

Class: VL2025260105679

Programme Name & Branch: B.
Tech CSBS

Course code & Title: CBS3005-
CLOUD, MICROSERVICES AND
APPLICATIONS LAB BASED
COMPONENTS

Faculty Name: NITHYA K

SUBMITTED BY: -DIPANGSHU
KUNDU

REGISTRATION NUMBER: -
22BBS0148

QUESTION:


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.

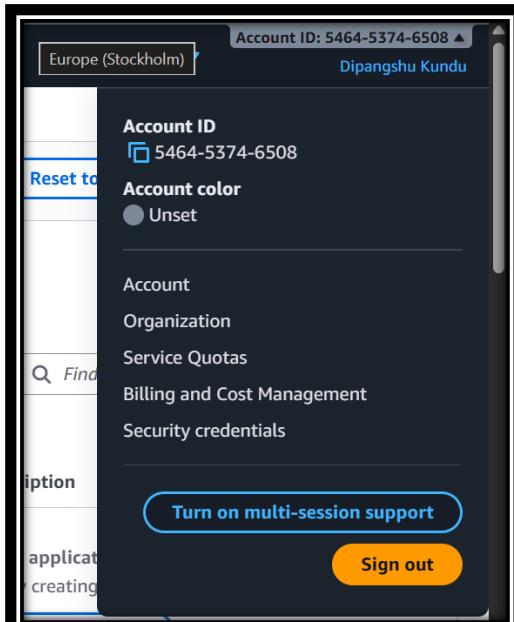
Steps:

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

Expected Output:

- Screenshot of CloudTrail event list.
- Sample JSON event record for one operation.
- Short explanation of how CloudTrail supports auditing and incident investigation.

SOLUTION: -



STEP 1: -

Go to CloudTrail Console → Trails → Create Trail

Choose:

- Trail name: MySecurityTrail
- Apply trail to All regions or Store logs in a new S3 bucket
- Enable CloudWatch Logs Integration (optional).

The screenshot shows the AWS CloudTrail Dashboard. On the left, there's a sidebar with options like Event history, Insights, Lake (Dashboards, Query, Event data stores, Integrations), Trails, Settings, Pricing, Documentation, and Forums. The main area has a heading 'Trails Info' with a 'Create trail' button. Below it, it says 'No trails' and 'No trails to display.' At the bottom, there's a 'CloudTrail Insights' section with a note that it's not enabled and a 'Create a trail' button.

This screenshot shows the 'Choose trail attributes' step of the 'Create trail' wizard. It's step 1 of 3. The left sidebar shows 'Step 2 Choose log events' and 'Step 3 Review and create'. The main area has a 'General details' section where the 'Trail name' is set to 'MySecurityTrail'. There's also a checkbox for enabling the trail for all accounts in the organization. The 'Storage location' section shows 'Create new S3 bucket' selected, with a prefix 'aws-cloudtrail-logs-546453746508-a15c82b6'. The 'Trail log bucket and folder' section shows the same prefix. At the bottom, there's a 'Log file SSE-KMS encryption' section and a note about AWS Lambda function logs.

The screenshot shows the 'Choose log events' step of creating a new CloudTrail trail. The navigation bar at the top indicates 'CloudTrail > Dashboard > Create trail'. On the left, a sidebar lists three steps: Step 1 (Choose trail attributes), Step 2 (Choose log events, which is selected and highlighted in blue), and Step 3 (Review and create). The main content area is titled 'Choose log events' and contains two sections: 'Events' (Info) and 'Management events' (Info). Under 'Events', there is a note about recording API activity for individual resources or all current and future resources in the AWS account, with a link for 'Additional charges apply'. Below this, under 'Event type', the 'Management events' checkbox is checked, with a description: 'Capture management operations performed on your AWS resources.' Other event types like 'Data events', 'Insights events', and 'Network activity events' are also listed with their descriptions. At the bottom of the page, there are links for 'CloudShell', 'Feedback', and copyright information: '© 2025, Amazon Web Services, Inc. or its affiliates.' followed by 'Privacy', 'Terms', and 'Cookie preferences'.

The screenshot shows the 'Review and create' step of creating a new CloudTrail trail. The navigation bar at the top indicates 'CloudTrail > Dashboard > Create trail'. On the left, a sidebar lists three steps: Step 1 (Choose trail attributes), Step 2 (Choose log events), and Step 3 (Review and create, which is selected and highlighted in blue). The main content area is titled 'Review and create' and contains two sections: 'Step 1: Choose trail attributes' and 'CloudWatch Logs'. The 'Step 1' section includes an 'Edit' button. It displays general details for the trail, such as the 'Trail name' (MySecurityTrail), 'Multi-region trail' (Yes), and 'Apply trail to my organization' (Not enabled). It also shows the 'Trail log location' (aws-cloudtrail-logs-546453746508-a15c82b6/AWSLogs/546453746508/), 'Log file SSE-KMS encryption' (Enabled), and 'AWS KMS key alias' (alias/MySecurityTrailAlias). The 'CloudWatch Logs' section shows the 'Log group' (aws-cloudtrail-logs-546453746508-4989908d) and the 'IAM Role' (CloudTrailToCloudWatchLogsRole). At the bottom of the page, there are links for 'CloudShell', 'Feedback', and copyright information: '© 2025, Amazon Web Services, Inc. or its affiliates.' followed by 'Privacy', 'Terms', and 'Cookie preferences'.

The screenshot shows the AWS CloudTrail Trails page. At the top, there are two success notifications: one about a trail being successfully created and another about enriching CloudTrail events. Below this, the 'Trails' table lists a single trail:

Name	Home region	Multi-region trail	ARN	Insights	Organization trail	S3 bucket	Log file prefix	CloudWatch Logs log group	Status
MySecurityTrail	Europe (Stockholm)	Yes	arn:aws:cloudtrail:eu-north-1:54645374:trail/MySecurityTrail	Disabled	No	aws-cloudtrail-logs-54645374-6508-a15c82b6	-	arn:aws:loggroup:aws-cloudtrail-logs-54645374-6508-6508-	Logging

STEP 2: -

Perform a few activities in your AWS account:

- Launch or stop an EC2 instance.
- Create an S3 bucket.

The screenshot shows the AWS EC2 Instances page. A green success notification at the top indicates that a new instance has been successfully launched. Below this, there's a 'Launch log' button and a 'Next Steps' section with several options:

- 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. Includes a 'Create billing alerts' button.
- Connect to your instance**: Once your instance is running, log into it from your local computer. Includes a 'Connect to instance' button.
- Connect an RDS database**: Configure the connection between an EC2 instance and a database to allow traffic flow between them. Includes a 'Connect an RDS database' button.
- Create EBS snapshot policy**: Create a policy that automates the creation, retention, and deletion of EBS snapshots. Includes a 'Create EBS snapshot policy' button.

The screenshot shows the AWS S3 console with the URL [https://eu-north-1.console.aws.amazon.com/s3/home?region=eu-north-1#buckets](#). A green success message at the top states: "Successfully created bucket 'cloudtrailaws2'". Below it, a note says: "To upload files and folders, or to configure additional bucket settings, choose View details." There are tabs for "General purpose buckets" and "Directory buckets", with "General purpose buckets" selected. A table lists three buckets: "aws-cloudtrail-logs-546453746508-a15c82b6", "cloudtrailaws2", and "dipangshu". On the right, there are two cards: "Account snapshot" (updated daily) and "External access summary - new" (updated daily). The bottom of the page includes links for CloudShell, Feedback, and navigation icons.

STEP 3: -

- Go back to CloudTrail.
- Click Event history on the left menu.
- We will now see a list of recent events from our account.

The screenshot shows the AWS CloudTrail console with the URL [https://eu-north-1.console.aws.amazon.com/cloudtrail/home?region=eu-north-1#eventHistory](#). The left sidebar has "Event history" selected. The main area displays "Event history (50+)" with a note: "Event history shows you the last 90 days of management events." It includes a "Lookup attributes" section with a dropdown set to "Read-only" and a search bar with "false". A table lists five events: "PutBucketEncryption", "PutBucketVersioning", "PutBucketPublicAcce...", "CreateBucket", and "RegisterManagedInst...". At the bottom, it says "0 / 5 events selected".

The screenshot shows the AWS CloudTrail Event history interface. On the left, there's a navigation sidebar with options like Dashboard, Event history (which is selected), Insights, Lake, Trails, Settings, Pricing, Documentation, and Forums. The main area displays a table of audit logs with columns for Action, Time, Service, User, and Resource. There are 5 events listed, all from October 15, 2025, at various times between 02:25:18 and 02:25:48 UTC. The actions include TerminateInstances, RunInstances, CreateView, AssociateDefaultView, CreateServiceLinked..., CreateIndex, UpdateTrail, and StartLogging. The service column shows AutoScaling, EC2, and CloudTrail. The user column shows root or IAM users. The resource column shows various AWS URLs.

Action	Time	Service	User	Resource
TerminateInstances	October 15, 2025, 02:25:48 (UT...)	AutoScaling	ec2.amazonaws.com	AWS::EC2::Instance
RunInstances	October 15, 2025, 02:25:48 (UT...)	AutoScaling	ec2.amazonaws.com	AWS::EC2::VPC, AW
TerminateInstances	October 15, 2025, 02:25:36 (UT...)	root	ec2.amazonaws.com	AWS::EC2::Instance
CreateView	October 15, 2025, 02:25:19 (UT...)	onboarding	resource-explorer-2.amazonaws.com	-
AssociateDefaultView	October 15, 2025, 02:25:19 (UT...)	onboarding	resource-explorer-2.amazonaws.com	-
CreateServiceLinked...	October 15, 2025, 02:25:19 (UT...)	-	cloudtrail.amazonaws.com	-
CreateIndex	October 15, 2025, 02:25:18 (UT...)	onboarding	resource-explorer-2.amazonaws.com	-
UpdateTrail	October 15, 2025, 02:22:12 (UT...)	root	cloudtrail.amazonaws.com	AWS::CloudTrail::Tr
StartLogging	October 15, 2025, 02:22:12 (UT...)	root	cloudtrail.amazonaws.com	AWS::CloudTrail::Tr

0 / 5 events selected

STEP 4: -

Click on any event to view full details. We should note:

Detail

Who performed the action

Time of action

Source IP address

Affected resource

Meaning

Shows the IAM user, root user, or role who triggered the event.

Timestamp when the action was performed.

Location/IP where the request came from (like your network IP).

Which AWS resource was changed (e.g. EC2 ID, S3 bucket name).

Example output when clicking an event:

- **User:** arn:aws:iam::123456789012:user/Alice
- **Event time:** 2025-10-15 09:23:11 UTC
- **Source IP:** 203.122.14.55
- **Resource:** i-0abc123xyz456def

DETAILS OF CREATING BUCKET

Screenshot of the AWS CloudTrail Event history page showing the details of a 'CreateBucket' event.

Details

Event time	AWS access key	AWS region
October 15, 2025, 02:31:29 (UTC+05:30)	ASIAAX60ZOONGCV5J2MRH	eu-north-1
User name	Source IP address	Error code
root	223.237.184.58	-
Event name	Event ID	Read-only
CreateBucket	2f38bb656-ec93-40c6-b9fb-e42ba9e9f025	false
Event source	Request ID	
s3.amazonaws.com	MSNVGH38PAPE35ME	

Resources referenced (1)

Resource type	Resource name	AWS Config resource timeline
AWS::S3::Bucket	cloudtrailaws2	Enable AWS Config resource recording

Screenshot of the AWS CloudTrail Event history page showing the resources referenced and the event record in JSON view.

Resources referenced (1)

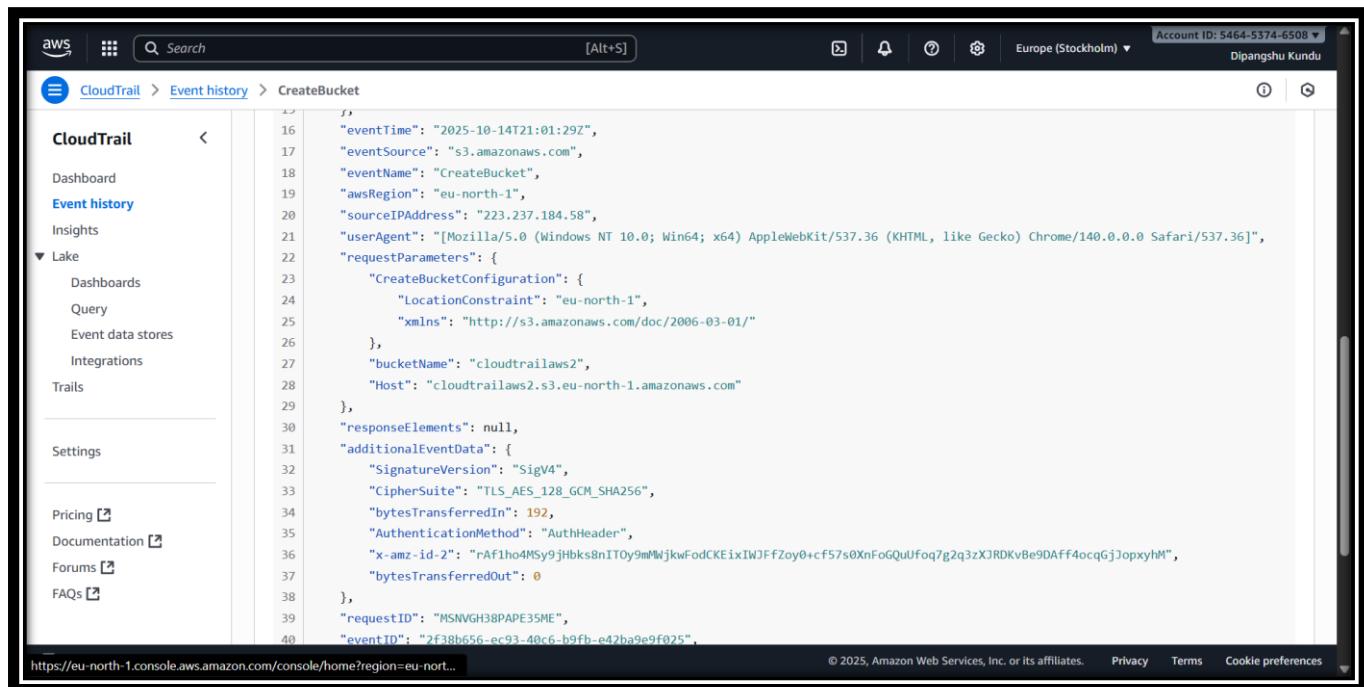
Resource type	Resource name	AWS Config resource timeline
AWS::S3::Bucket	cloudtrailaws2	Enable AWS Config resource recording

Event record

JSON view

```

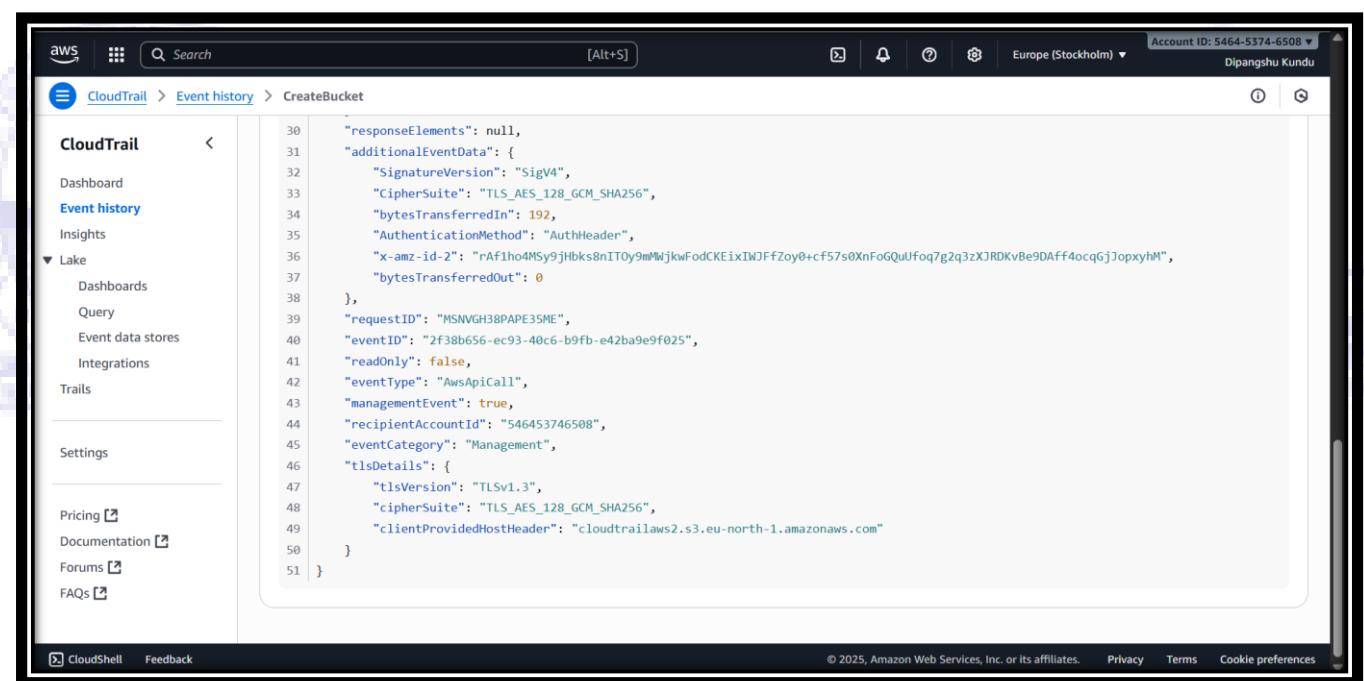
1  {
2      "eventVersion": "1.11",
3      "userIdentity": {
4          "type": "Root",
5          "principalId": "546453746508",
6          "arn": "arn:aws:iam::546453746508:root",
7          "accountId": "546453746508",
8          "accessKeyId": "ASIAAX60ZOONGCV5J2MRH",
9          "sessionContext": {
10              "attributes": {
11                  "creationDate": "2025-10-14T20:41:06Z",
12                  "mfaAuthenticated": "true"
13              }
14          }
15      }
16  }
  
```



```

CloudTrail < 16 "eventTime": "2025-10-14T21:01:29Z",
              17 "eventSource": "s3.amazonaws.com",
              18 "eventName": "CreateBucket",
              19 "awsRegion": "eu-north-1",
              20 "sourceIPAddress": "223.237.184.58",
              21 "userAgent": "[Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36]",
              22 "requestParameters": {
                  23     "CreateBucketConfiguration": {
                      24         "LocationConstraint": "eu-north-1",
                      25         "xmlns": "http://s3.amazonaws.com/doc/2006-03-01/"
                  },
                  26         "bucketName": "cloudtrailaws2",
                  27         "Host": "cloudtrailaws2.s3.eu-north-1.amazonaws.com"
              },
              28     "responseElements": null,
              29     "additionalEventData": {
                  30         "SignatureVersion": "SigV4",
                  31         "CipherSuite": "TLS_AES_128_GCM_SHA256",
                  32         "bytesTransferredIn": 192,
                  33         "AuthenticationMethod": "AuthHeader",
                  34         "x-amz-id-2": "RAfIho4MSy9jHbks8nIT0y9mWjkwFodCKEixIWJFFZoy+c5f57s0XnFoGQuUfoq7g2q3zXJRDkvBe9DAff4ocqGjJopxyhM",
                  35         "bytesTransferredOut": 0
              },
              36     "requestID": "MSNVGH38PAP35ME",
              37     "eventID": "2f38b656-ec93-40c6-b9fb-e42ba9e9f025",
              38 },
              39     "eventVersion": "1.11",
              40     "userIdentity": {
                  41         "type": "Root",
                  42         "principalId": "546453746508",
                  43         "arn": "arn:aws:iam::546453746508:root",
                  44         "accountId": "546453746508",
              }
          }
      
```

https://eu-north-1.console.aws.amazon.com/console/home?region=eu-nort... © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences



```

CloudTrail < 30     "responseElements": null,
                     "additionalEventData": {
                         31             "SignatureVersion": "SigV4",
                         32             "CipherSuite": "TLS_AES_128_GCM_SHA256",
                         33             "bytesTransferredIn": 192,
                         34             "AuthenticationMethod": "AuthHeader",
                         35             "x-amz-id-2": "RAfIho4MSy9jHbks8nIT0y9mWjkwFodCKEixIWJFFZoy+c5f57s0XnFoGQuUfoq7g2q3zXJRDkvBe9DAff4ocqGjJopxyhM",
                         36             "bytesTransferredOut": 0
                     },
                     37     "requestID": "MSNVGH38PAP35ME",
                     38     "eventID": "2f38b656-ec93-40c6-b9fb-e42ba9e9f025",
                     39     "readOnly": false,
                     40     "eventType": "AwsApiCall",
                     41     "managementEvent": true,
                     42     "recipientAccountId": "546453746508",
                     43     "eventCategory": "Management",
                     44     "tlsDetails": {
                         45         "tlsVersion": "TLSv1.3",
                         46         "cipherSuite": "TLS_AES_128_GCM_SHA256",
                         47         "clientProvidedHostHeader": "cloudtrailaws2.s3.eu-north-1.amazonaws.com"
                     }
                 }
             }
         }
     }
 
```

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

THE ABOVE CODE:-

```
{
    "eventVersion": "1.11",
    "userIdentity": {
        "type": "Root",
        "principalId": "546453746508",
        "arn": "arn:aws:iam::546453746508:root",
        "accountId": "546453746508",
    }
}
```

```
"accessKeyId": "ASIA6OZOONGCV5J2MRH",
"sessionContext": {
    "attributes": {
        "creationDate": "2025-10-14T20:41:06Z",
        "mfaAuthenticated": "true"
    }
},
"eventTime": "2025-10-14T21:01:29Z",
"eventSource": "s3.amazonaws.com",
"eventName": "CreateBucket",
"awsRegion": "eu-north-1",
"sourceIPAddress": "223.237.184.58",
"userAgent": "[Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/140.0.0.0 Safari/537.36]",
"requestParameters": {
    "CreateBucketConfiguration": {
        "LocationConstraint": "eu-north-1",
        "xmlns": "http://s3.amazonaws.com/doc/2006-03-01/"
    },
    "bucketName": "cloudtrailaws2",
    "Host": "cloudtrailaws2.s3.eu-north-1.amazonaws.com"
},
"responseElements": null,
"additionalEventData": {
    "SignatureVersion": "SigV4",
    "CipherSuite": "TLS_AES_128_GCM_SHA256",
    "bytesTransferredIn": 192,
    "AuthenticationMethod": "AuthHeader",
    "x-amz-id-2": "rAf1ho4MSy9jHbks8nITOy9mMWjkwFodCKEixIWJFfZoy0+cf57s0XnFoGQ
uUfoq7g2q3zXJRDKvBe9DAff4ocqGjJopxyhM",
    "bytesTransferredOut": 0
},
"requestID": "MSNVGH38PAPE35ME",
"eventID": "2f38b656-ec93-40c6-b9fb-e42ba9e9f025",
"readOnly": false,
"eventType": "AwsApiCall",
"managementEvent": true,
"recipientAccountId": "546453746508",
"eventCategory": "Management",
```

```
"tlsDetails": {  
    "tlsVersion": "TLSv1.3",  
    "cipherSuite": "TLS_AES_128_GCM_SHA256",  
    "clientProvidedHostHeader": "cloudtrailaws2.s3.eu-north-  
1.amazonaws.com"  
}
```

Detail to Identify

Who performed the action Root user of AWS account 546453746508

Time of action 2025-10-14T21:01:29Z

Source IP address 223.237.184.58

Affected resource S3 bucket named **cloudtrailaws2**

What action was done CreateBucket (an S3 bucket was created)

Answer from the Event

This CloudTrail log records that the **root user** created an **S3 bucket** from IP address **223.237.184.58** in the AWS **eu-north-1 region** at a specific time. This level of detail helps in **security auditing and incident investigation**, because it clearly shows:

- Which user made the change
- What resource was affected
- When and from where the request was made

This helps detect **unauthorized access**, monitor **critical actions**, and maintain **accountability** in AWS environments.

DETAILS OF RUNNING INSTANCES

The screenshot shows the AWS CloudTrail Event history interface. The left sidebar is collapsed, and the main content area displays the details of a specific event.

Event Details:

- Event time:** October 15, 2025, 02:25:48 (UTC+05:30)
- User name:** AutoScaling
- Event name:** RunInstances
- Event source:** ec2.amazonaws.com
- AWS access key:** -
- Source IP address:** autoscaling.amazonaws.com
- Event ID:** eeb41a02-0695-4ced-9f6e-5c411465a92f
- Request ID:** f7e3873e-b190-4cf3-9228-0e17d0de7e3a
- AWS region:** eu-north-1
- Error code:** -
- Read-only:** false

Resources referenced (8) 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-0d33fd5d4c387e7ff	Enable AWS Config resource recording
AWS::EC2::Ami	ami-0c4fc5dcabc9df21d	Enable AWS Config resource recording
AWS::EC2::NetworkInterface	eni-01911ea314cdf2b83	Enable AWS Config resource recording

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

The screenshot shows the AWS CloudTrail Event history interface. The left sidebar is collapsed, and the main content area displays the details of a specific event.

Event Details:

- Event time:** October 15, 2025, 02:25:48 (UTC+05:30)
- User name:** AutoScaling
- Event name:** RunInstances
- Event source:** ec2.amazonaws.com
- AWS access key:** -
- Source IP address:** autoscaling.amazonaws.com
- Event ID:** eeb41a02-0695-4ced-9f6e-5c411465a92f
- Request ID:** f7e3873e-b190-4cf3-9228-0e17d0de7e3a
- AWS region:** eu-north-1
- Error code:** -
- Read-only:** false

Resources referenced (8) 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-0d33fd5d4c387e7ff	Enable AWS Config resource recording
AWS::EC2::Ami	ami-0c4fc5dcabc9df21d	Enable AWS Config resource recording
AWS::EC2::NetworkInterface	eni-01911ea314cdf2b83	Enable AWS Config resource recording
AWS::EC2::Instance	i-0e08f7fa9285f2a9	Enable AWS Config resource recording
AWS::EC2::KeyPair	static_website	Enable AWS Config resource recording
AWS::EC2::SecurityGroup	sg-04f7e384654e56eff	Enable AWS Config resource recording
AWS::EC2::SecurityGroup	launch-wizard-7	Enable AWS Config resource recording
AWS::EC2::Subnet	subnet-01e489d076097fbf2	Enable AWS Config resource recording

Event record Info

JSON view [Copy](#)

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

The screenshot shows the AWS CloudTrail console with the path: CloudTrail > Event history > RunInstances. The main area displays a JSON view of an event record. The event details include:

```
1  {
2      "eventVersion": "1.10",
3      "userIdentity": {
4          "type": "AssumedRole",
5          "principalId": "AROAX60Z0ONGB25L75Z2Y:AutoScaling",
6          "arn": "arn:aws:sts::546453746508:assumed-role/AWSServiceRoleForAutoScaling/AutoScaling",
7          "accountId": "546453746508",
8          "sessionContext": {
9              "sessionIssuer": {
10                  "type": "Role",
11                  "principalId": "AROAX60Z0ONGB25L75Z2Y",
12                  "arn": "arn:aws:iam::546453746508:role/aws-service-role/autoscaling.amazonaws.com/AWSServiceRoleForAutoScaling",
13                  "accountId": "546453746508",
14                  "userName": "AWSServiceRoleForAutoScaling"
15              },
16              "attributes": {
17                  "creationDate": "2025-10-14T20:55:47Z",
18                  "mfaAuthenticated": "false"
19              }
20          },
21          "invokedBy": "autoscaling.amazonaws.com"
22      },
23  }
```

At the bottom right of the JSON view, there is a blue "Copy" button.

The screenshot shows the AWS CloudTrail console with the path: CloudTrail > Event history > RunInstances. The main area displays a JSON view of an event record. The event details include:

```
23  {
24      "eventTime": "2025-10-14T20:55:48Z",
25      "eventSource": "ec2.amazonaws.com",
26      "eventName": "RunInstances",
27      "awsRegion": "eu-north-1",
28      "sourceIPAddress": "autoscaling.amazonaws.com",
29      "userAgent": "autoscaling.amazonaws.com",
30      "requestParameters": {
31          "instancesSet": {
32              "items": [
33                  {
34                      "minCount": 1,
35                      "maxCount": 1
36                  }
37              ]
38          },
39          "blockDeviceMapping": {},
40          "availabilityZone": "eu-north-1b",
41          "monitoring": {
42              "enabled": false
43          },
44          "disableApiTermination": false,
45          "disableApiStop": false,
46          "clientToken": "b9566792-07e4-e0cf-a64f-0055e036332e",
47          "networkInterfaceSet": {
48              "items": [
49  
```

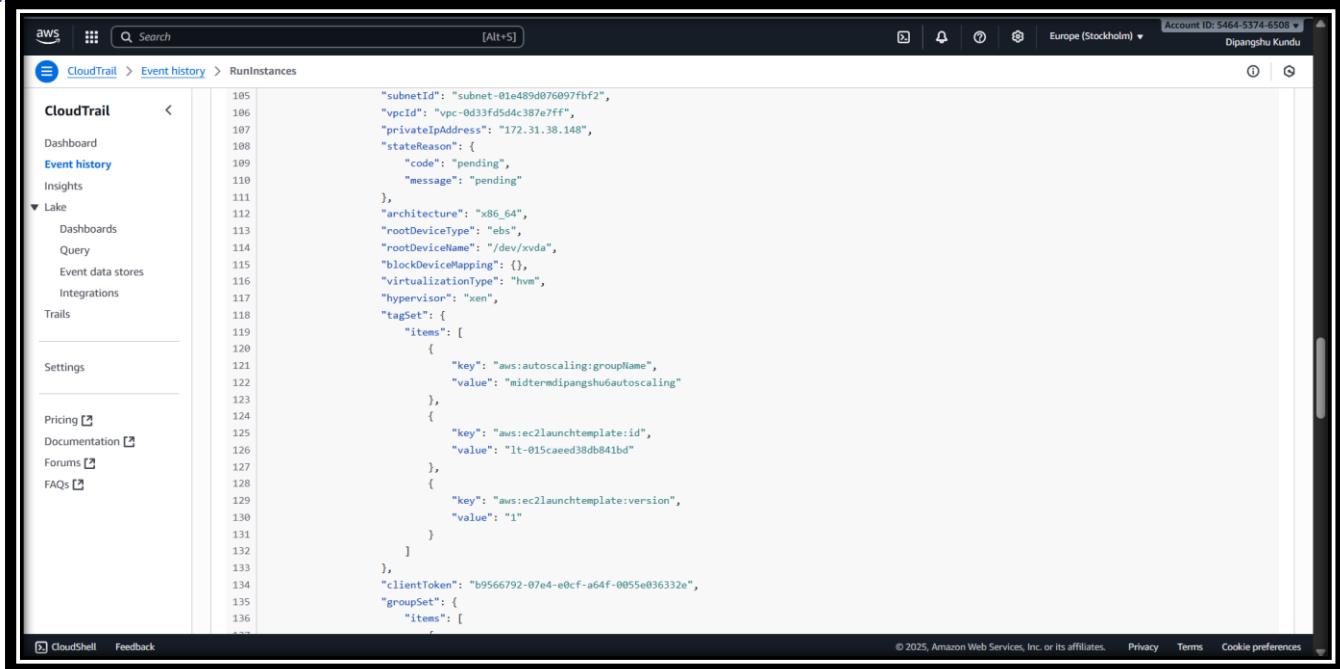
At the bottom right of the JSON view, there is a blue "Copy" button.

A screenshot of the AWS CloudTrail console. The left sidebar shows navigation links for CloudTrail, Dashboard, Event history, Insights, Lake (Dashboards, Query, Event data stores, Integrations), Trails, Settings, Pricing, Documentation, Forums, and FAQs. The main content area displays a JSON log entry for an event named 'RunInstances'. The log includes details such as deviceIndex, subnetId, tagSpecificationSet, resourceType, tags, launchTemplate, and responseElements. The responseElements section contains information like requestId, reservationId, ownerId, groupSet, instancesSet, instanceId, amiId, bootMode, currentInstanceBootMode, instanceState, code, name, privateDnsName, keyName, operator, managed, amiLaunchIndex, productCodes, instanceType, launchTime, placement, availabilityZone, availabilityZoneId, tenancy, monitoring, and state.

```
48     {
49         "deviceIndex": 0,
50         "subnetId": "subnet-01e489d076097fbf2"
51     }
52 ],
53 },
54 "tagSpecificationSet": {
55     "items": [
56         {
57             "resourceType": "instance",
58             "tags": [
59                 {
60                     "key": "aws:autoscaling:groupName",
61                     "value": "midterm-dipangshu6-autoscaling"
62                 }
63             ]
64         }
65     ]
66 },
67 "launchTemplate": {
68     "launchTemplateId": "lt-015caeef38db841bd",
69     "version": "1"
70 },
71 },
72 "responseElements": {
```

A screenshot of the AWS CloudTrail console, identical to the one above but showing a more detailed log entry for the 'RunInstances' event. This log entry provides extensive details about the instance creation, including its configuration, placement, and monitoring settings.

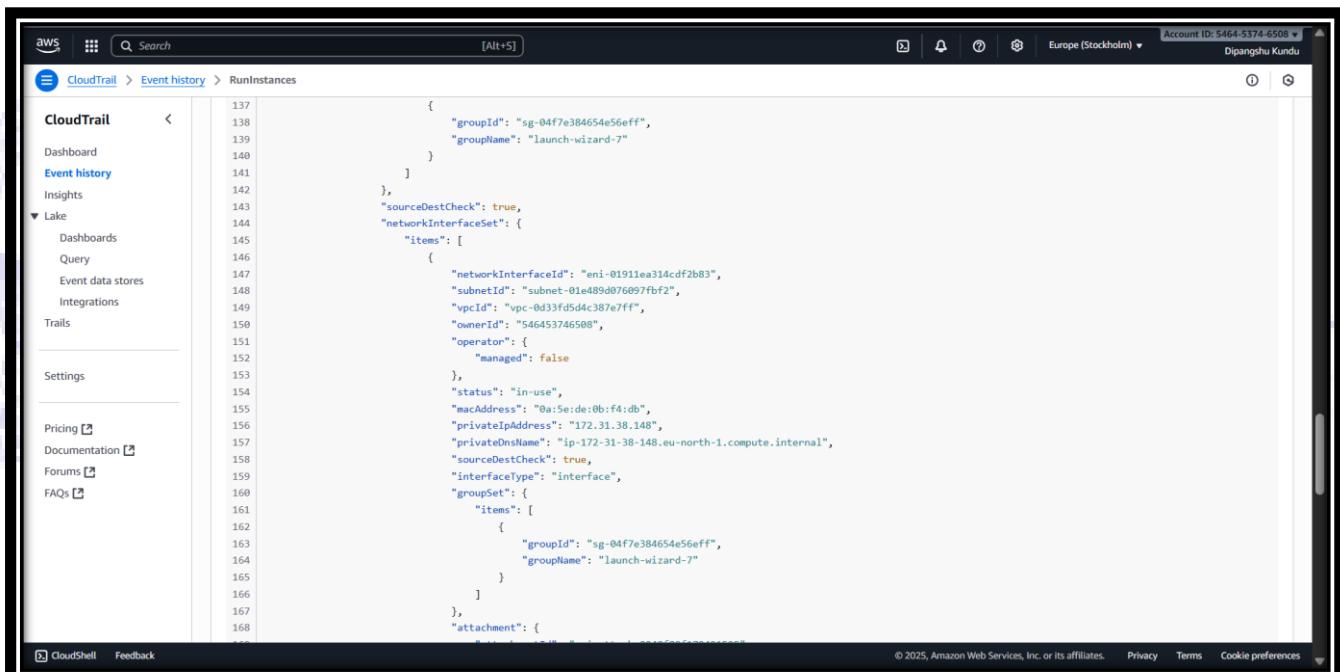
```
72 "responseElements": {
73     "requestId": "f7e3873e-b190-4cf3-9228-0e17d0de7e3a",
74     "reservationId": "-0be/b7143b4f0b120",
75     "ownerId": "546453746508",
76     "groupSet": {},
77     "instancesSet": {
78         "items": [
79             {
80                 "instanceId": "i-0e08f7f4a9285f2a0",
81                 "amiId": "ami-0c4fc5dcabc9df21d",
82                 "bootMode": "uefi-preferred",
83                 "currentInstanceBootMode": "uefi",
84                 "instanceState": {
85                     "code": 0,
86                     "name": "pending"
87                 },
88                 "privateDnsName": "ip-172-31-38-148.eu-north-1.compute.internal",
89                 "keyName": "static_website",
90                 "operator": {
91                     "managed": false
92                 },
93                 "amiLaunchIndex": 0,
94                 "productCodes": {},
95                 "instanceType": "t3.micro",
96                 "launchTime": 1760475348000,
97                 "placement": {
98                     "availabilityZone": "eu-north-1b",
99                     "availabilityZoneId": "euni-az2",
100                    "tenancy": "default"
101                },
102                "monitoring": {
103                    "state": "disabled"
104                }
105            }
106        ]
107    }
108 }
```



A screenshot of the AWS CloudTrail console showing the Event history section for the RunInstances API. The event details are displayed in a JSON-like format with line numbers. The event occurred at line 105 and is associated with a specific VPC and subnet.

```
CloudTrail < 105
  "subnetId": "subnet-01e489d076097fbf2",
  "vpcId": "vpc-0d3fd5d54c387e7ff",
  "privateIpAddress": "172.31.38.148",
  "stateReason": {
    "code": "pending",
    "message": "pending"
  },
  "architecture": "x86_64",
  "rootDeviceType": "ebs",
  "rootDeviceName": "/dev/xvda",
  "blockDeviceMapping": {},
  "virtualizationType": "hvm",
  "hypervisor": "xen",
  "tagSet": [
    "items": [
      {
        "key": "aws:autoscaling:groupName",
        "value": "midterm-dipangshu6-autoscaling"
      },
      {
        "key": "aws:ec2launchtemplate:id",
        "value": "lt-015cae038db841bd"
      },
      {
        "key": "aws:ec2launchtemplate:version",
        "value": "1"
      }
    ]
  },
  "clientToken": "b9566792-07e4-e0cf-a64f-0055e036332e",
  "groupSet": {
    "items": [
      ...
    ]
  }
}

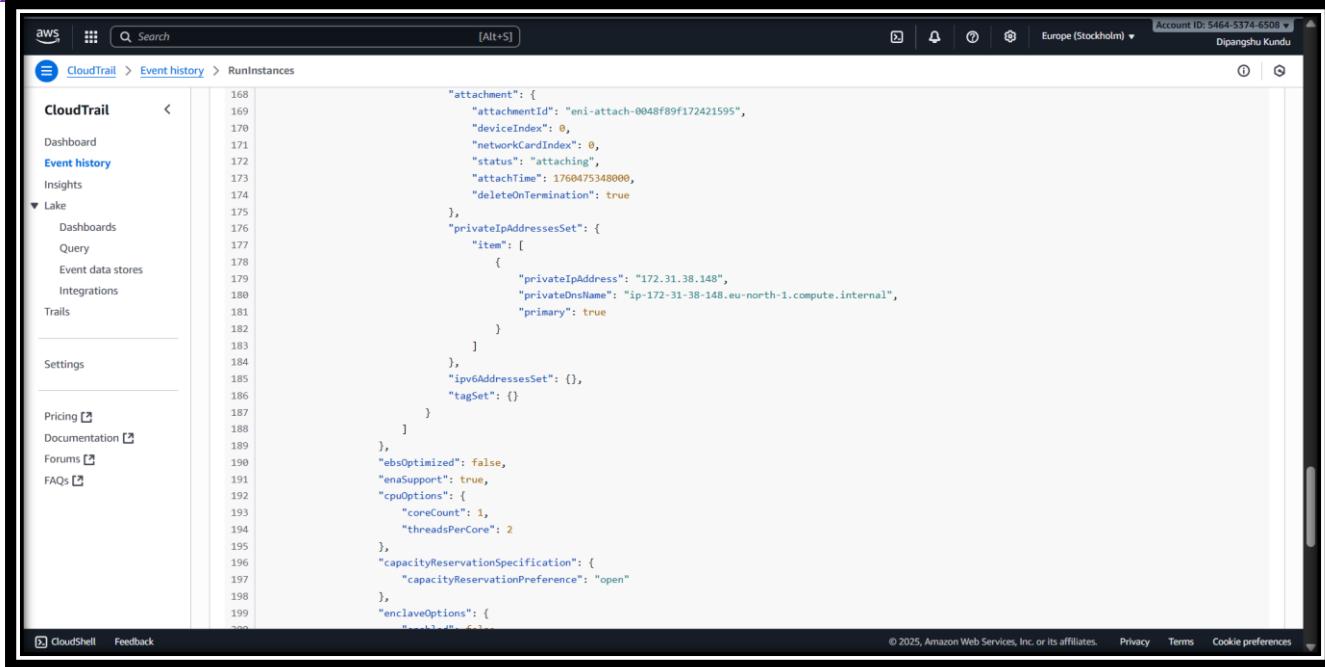
© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences
```



A screenshot of the AWS CloudTrail console showing the Event history section for the RunInstances API. The event details are displayed in a JSON-like format with line numbers. This event is similar to the one above but includes more detailed information about the network interface created.

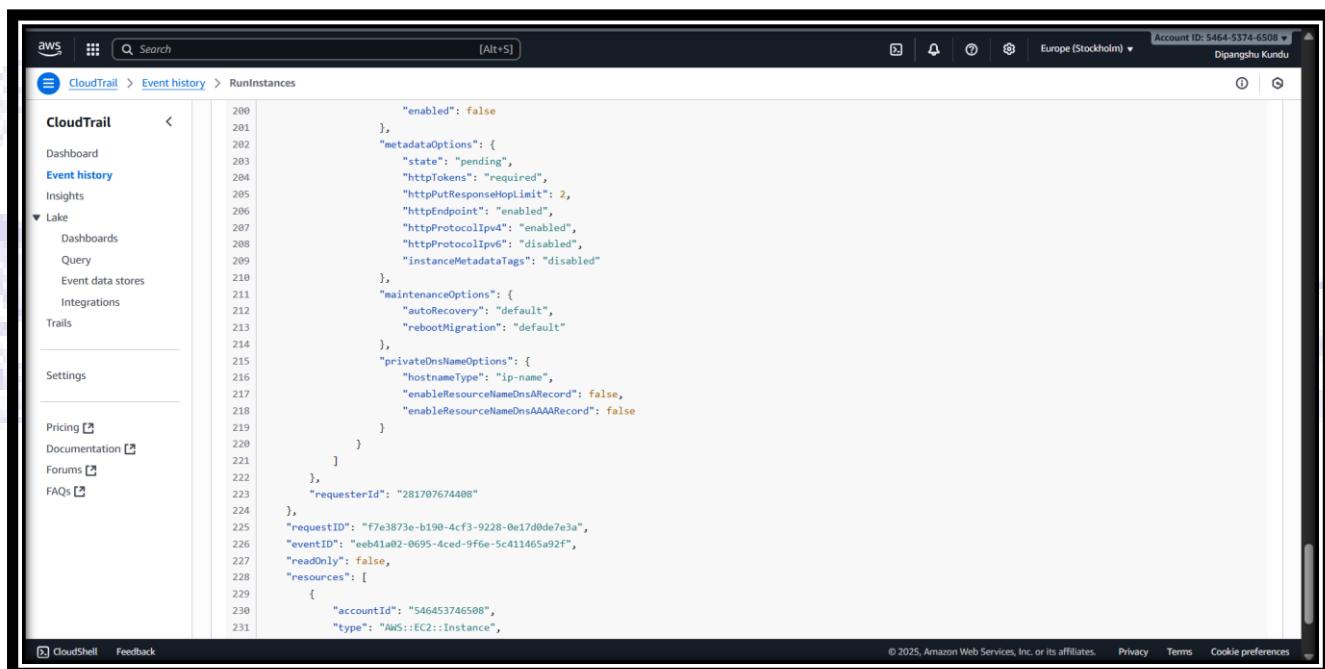
```
CloudTrail < 137
  "groupId": "sg-04f7e384654e56eff",
  "groupName": "launch-wizard-7"
}
],
"sourceDestCheck": true,
"networkInterfaceSet": [
  "items": [
    {
      "networkInterfaceId": "eni-01911ea314cdf2b83",
      "subnetId": "subnet-01e489d076097fbf2",
      "vpcId": "vpc-0d3fd5d54c387e7ff",
      "ownerId": "546453746508",
      "operator": {
        "managed": false
      },
      "status": "in-use",
      "macAddress": "0a:5e:de:0b:f4:db",
      "privateIpAddress": "172.31.38.148",
      "privateDnsName": "ip-172-31-38-148.eu-north-1.compute.internal",
      "sourceDestCheck": true,
      "interfaceType": "interface",
      "groupSet": {
        "items": [
          {
            "groupId": "sg-04f7e384654e56eff",
            "groupName": "launch-wizard-7"
          }
        ]
      },
      "attachment": {
        "deviceIndex": 0
      }
    }
  ]
}

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



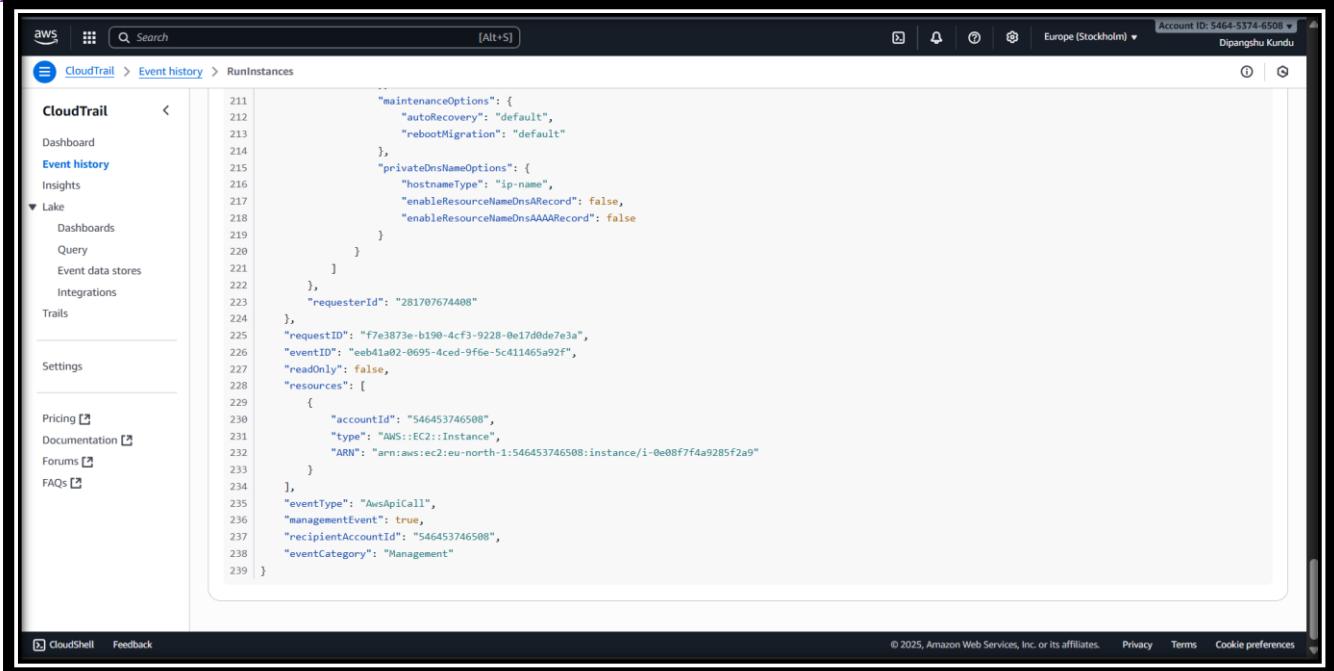
A screenshot of the AWS CloudTrail Event history interface. The left sidebar shows navigation links for CloudTrail, Dashboard, Event history, Insights, Lake, Settings, Pricing, Documentation, Forums, and FAQs. The main content area displays a JSON log entry for an EC2 instance creation. The log includes fields like attachment, privateIpAddressesSet, ipv6AddressesSet, tagSet, ebsOptimized, enaSupport, cpuOptions, capacityReservationSpecification, and enclaveOptions. The log ID is 1706475348000.

```
    "attachment": {
        "attachmentId": "eni-attach-0048f89f172421595",
        "deviceIndex": 0,
        "networkCardIndex": 0,
        "status": "attaching",
        "attachTime": 1706475348000,
        "deleteOnTermination": true
    },
    "privateIpAddressesSet": {
        "item": [
            {
                "privateIpAddress": "172.31.38.148",
                "privateDnsName": "ip-172-31-38-148.eu-north-1.compute.internal",
                "primary": true
            }
        ]
    },
    "ipv6AddressesSet": {},
    "tagSet": {}
},
],
"ebsOptimized": false,
"enaSupport": true,
"cpuOptions": {
    "coreCount": 1,
    "threadsPerCore": 2
},
"capacityReservationSpecification": {
    "capacityReservationPreference": "open"
},
"enclaveOptions": {
    "enclaveType": "aws-grl"
}
```



A screenshot of the AWS CloudTrail Event history interface. The left sidebar shows navigation links for CloudTrail, Dashboard, Event history, Insights, Lake, Settings, Pricing, Documentation, Forums, and FAQs. The main content area displays a JSON log entry for an EC2 instance modification. The log includes fields like enabled, metadataOptions, maintenanceOptions, privateDnsNameOptions, requesterId, requestID, eventID, readOnly, and resources. The log ID is 281707674408.

```
    "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": false,
    "enableResourceNameDnsAAAARecord": false
}
},
"requesterId": "281707674408"
},
"requestID": "f7e3873e-b190-4cf3-9228-0e17d0de7e3a",
"eventID": "eeb41ad2-0695-4ced-9f6e-5c411465a92f",
"readOnly": false,
"resources": [
{
    "accountId": "546453746508",
    "type": "AWS::EC2::Instance"
}
```



The screenshot shows the AWS CloudTrail Event history interface. The left sidebar shows navigation options like Dashboard, Event history, Insights, Lake, Dashboards, Query, Event data stores, Integrations, Trails, Settings, Pricing, Documentation, Forums, and FAQs. The main content area displays a JSON log entry with line numbers from 211 to 239. The log details an event where an Auto Scaling instance was created. Key fields include:

```

  "eventVersion": "1.10",
  "userIdentity": {
    "type": "AssumedRole",
    "principalId": "AROAX6OZOONGB25L75Z2Y:AutoScaling",
    "arn": "arn:aws:sts::546453746508:assumed-role/AWSServiceRoleForAutoScaling/AutoScaling",
    "accountId": "546453746508",
    "sessionContext": {
      "sessionIssuer": {
        "type": "Role",
        "principalId": "AROAX6OZOONGB25L75Z2Y",
        "arn": "arn:aws:iam::546453746508:role/aws-service-role/autoscaling.amazonaws.com/AWSServiceRoleForAutoScaling",
        "accountId": "546453746508",
        "userName": "AWSServiceRoleForAutoScaling"
      },
      "attributes": {
        "creationDate": "2025-10-14T20:55:47Z",
        "mfaAuthenticated": "false"
      }
    },
    "invokedBy": "autoscaling.amazonaws.com"
  },
  "requestId": "f7e3873e-b190-4cf3-9228-0e17d0de7e3a",
  "eventID": "eeb41a02-0695-4ced-9f6e-5c411465a92f",
  "readOnly": false,
  "resources": [
    {
      "accountId": "546453746508",
      "type": "AWS::EC2::Instance",
      "ARN": "arn:aws:ec2:eu-north-1:546453746508:instance/i-0e08ff4a9285f2a9"
    }
  ],
  "eventType": "AwsApiCall",
  "managementEvent": true,
  "recipientAccountId": "546453746508",
  "eventCategory": "Management"
}

```

THE ABOVE CODE :-

{
 "eventVersion": "1.10",
 "userIdentity": {
 "type": "AssumedRole",
 "principalId": "AROAX6OZOONGB25L75Z2Y:AutoScaling",
 "arn": "arn:aws:sts::546453746508:assumed-role/AWSServiceRoleForAutoScaling/AutoScaling",
 "accountId": "546453746508",
 "sessionContext": {
 "sessionIssuer": {
 "type": "Role",
 "principalId": "AROAX6OZOONGB25L75Z2Y",
 "arn": "arn:aws:iam::546453746508:role/aws-service-role/autoscaling.amazonaws.com/AWSServiceRoleForAutoScaling",
 "accountId": "546453746508",
 "userName": "AWSServiceRoleForAutoScaling"
 },
 "attributes": {
 "creationDate": "2025-10-14T20:55:47Z",
 "mfaAuthenticated": "false"
 }
 },
 "invokedBy": "autoscaling.amazonaws.com"
},

```
"eventTime": "2025-10-14T20:55:48Z",
"eventSource": "ec2.amazonaws.com",
"eventName": "RunInstances",
"awsRegion": "eu-north-1",
"sourceIPAddress": "autoscaling.amazonaws.com",
"userAgent": "autoscaling.amazonaws.com",
"requestParameters": {
    "instancesSet": {
        "items": [
            {
                "minCount": 1,
                "maxCount": 1
            }
        ]
    },
    "blockDeviceMapping": {},
    "availabilityZone": "eu-north-1b",
    "monitoring": {
        "enabled": false
    },
    "disableApiTermination": false,
    "disableApiStop": false,
    "clientToken": "b9566792-07e4-e0cf-a64f-0055e036332e",
    "networkInterfaceSet": {
        "items": [
            {
                "deviceIndex": 0,
                "subnetId": "subnet-01e489d076097fbf2"
            }
        ]
    },
    "tagSpecificationSet": {
        "items": [
            {
                "resourceType": "instance",
                "tags": [
                    {
                        "key": "aws:autoscaling:groupName",
                        "value": "midterm-dipangshu6-autoscaling"
                    }
                ]
            }
        ]
    }
}
```

```
        }
    ],
},
"launchTemplate": {
    "launchTemplateId": "lt-015cae038db841bd",
    "version": "1"
},
"responseElements": {
    "requestId": "f7e3873e-b190-4cf3-9228-0e17d0de7e3a",
    "reservationId": "r-0be7b7143b9f0b120",
    "ownerId": "546453746508",
    "groupSet": {},
    "instancesSet": {
        "items": [
            {
                "instanceId": "i-0e08f7f4a9285f2a9",
                "imageId": "ami-0c4fc5dcabc9df21d",
                "bootMode": "uefi-preferred",
                "currentInstanceBootMode": "uefi",
                "instanceState": {
                    "code": 0,
                    "name": "pending"
                },
                "privateDnsName": "ip-172-31-38-148.eu-north-1.compute.internal",
                "keyName": "static_website",
                "operator": {
                    "managed": false
                },
                "amiLaunchIndex": 0,
                "productCodes": {},
                "instanceType": "t3.micro",
                "launchTime": 1760475348000,
                "placement": {
                    "availabilityZone": "eu-north-1b",
                    "availabilityZoneId": "eun1-az2",
                    "tenancy": "default"
                },
                "monitoring": {
                    "state": "disabled"
                }
            }
        ]
    }
}
```

```
        },
        "subnetId": "subnet-01e489d076097fbf2",
        "vpcId": "vpc-0d33fd5d4c387e7ff",
        "privateIpAddress": "172.31.38.148",
        "stateReason": {
            "code": "pending",
            "message": "pending"
        },
        "architecture": "x86_64",
        "rootDeviceType": "ebs",
        "rootDeviceName": "/dev/xvda",
        "blockDeviceMapping": {},
        "virtualizationType": "hvm",
        "hypervisor": "xen",
        "tagSet": {
            "items": [
                {
                    "key": "aws:autoscaling:groupName",
                    "value": "midtermdipangshu6autoscaling"
                },
                {
                    "key": "aws:ec2launchtemplate:id",
                    "value": "lt-015caeед38db841bd"
                },
                {
                    "key": "aws:ec2launchtemplate:version",
                    "value": "1"
                }
            ]
        },
        "clientToken": "b9566792-07e4-e0cf-a64f-0055e036332e",
        "groupSet": {
            "items": [
                {
                    "groupId": "sg-04f7e384654e56eff",
                    "groupName": "launch-wizard-7"
                }
            ]
        },
        "sourceDestCheck": true,
        "networkInterfaceSet": {
```

```
"items": [
  {
    "networkInterfaceId": "eni-01911ea314cdf2b83",
    "subnetId": "subnet-01e489d076097fbf2",
    "vpcId": "vpc-0d33fd5d4c387e7ff",
    "ownerId": "546453746508",
    "operator": {
      "managed": false
    },
    "status": "in-use",
    "macAddress": "0a:5e:de:0b:f4:db",
    "privateIpAddress": "172.31.38.148",
    "privateDnsName": "ip-172-31-38-148.eu-north-
1.compute.internal",
      "sourceDestCheck": true,
      "interfaceType": "interface",
      "groupSet": {
        "items": [
          {
            "groupId": "sg-04f7e384654e56eff",
            "groupName": "launch-wizard-7"
          }
        ]
      },
      "attachment": {
        "attachmentId": "eni-attach-0048f89f172421595",
        "deviceIndex": 0,
        "networkCardIndex": 0,
        "status": "attaching",
        "attachTime": 1760475348000,
        "deleteOnTermination": true
      },
      "privateIpAddressesSet": {
        "item": [
          {
            "privateIpAddress": "172.31.38.148",
            "privateDnsName": "ip-172-31-38-148.eu-north-
1.compute.internal",
              "primary": true
            }
          ]
        ]
      }
    }
  ]
}
```

```
        },
        "ipv6AddressesSet": {},
        "tagSet": {}
    }
],
},
"ebsOptimized": false,
"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": false,
    "enableResourceNameDnsAAAARecord": false
}
}
],
},
"requesterId": "281707674408"
},
```

```

    "requestID": "f7e3873e-b190-4cf3-9228-0e17d0de7e3a",
    "eventID": "eeb41a02-0695-4ced-9f6e-5c411465a92f",
    "readOnly": false,
    "resources": [
        {
            "accountId": "546453746508",
            "type": "AWS::EC2::Instance",
            "ARN": "arn:aws:ec2:eu-north-1:546453746508:instance/i-
0e08f7f4a9285f2a9"
        }
    ],
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "546453746508",
    "eventCategory": "Management"
}

```

Detail to Identify

Who performed the action

Type of user

Time of action

Source IP address

Event name (what action happened)

AWS Region

Affected resource

Triggered by

This CloudTrail log shows that the **Auto Scaling service** automatically launched a new **EC2 instance** using the **RunInstances** API call. The action was performed by the IAM service role **AWSServiceRoleForAutoScaling** on behalf of Auto Scaling, not by a human user. It happened in the **eu-north-1 region** at the time **2025-10-14T20:55:48Z**. The request came from **autoscaling.amazonaws.com**, which means it was triggered automatically by AWS to scale the system based on demand.

CloudTrail captured **who triggered the action, when it occurred, and which EC2 instance was affected**, which helps with auditing and understanding system behavior.

Answer from the Event

AWSServiceRoleForAutoScaling (Assumed IAM Role)

AWS Service Role (Auto Scaling)

2025-10-14T20:55:48Z

autoscaling.amazonaws.com

RunInstances (EC2 instance launched)

eu-north-1

EC2 Instance ID: i-0e08f7f4a9285f2a9

AWS Auto Scaling service

QUESTION:

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.

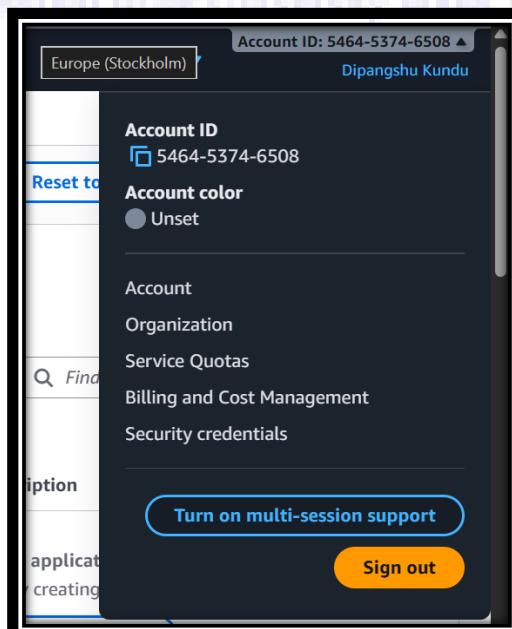
6. Create a **CloudWatch Alarm**:

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

Expected Output:

- CloudWatch dashboard showing metrics (CPU, Memory).
- Alarm configuration screenshot.
- Email alert showing triggered event.

SOLUTION:-



Step 1: Launch an EC2 Instance

- Open AWS Console → EC2 → Launch Instance
- Name: CloudWatchTestInstance
- AMI: Amazon Linux 2
- Instance type: t2.micro (Free Tier eligible)
- Key pair: Select or create one
- Security group: Allow SSH (port 22), and optionally HTTP (port 80)
- Click Launch Instance

Name and tags

Name
CloudWatchTestInstance

Application and OS Images (Amazon Machine Image)

An AMI contains the operating system, application server, and applications for your instance. If you don't see a suitable AMI below, use the search field or choose [Browse more AMIs](#).

Search our full catalog including 1000s of application and OS images

Recents | My AMIs | **Quick Start**

Summary

Number of instances | Info
1

Software Image (AMI)
Amazon Linux 2023 AMI 2023.9.2... [read more](#)
ami-04c08fd8aa14af291

Virtual server type (instance type)
t3.micro

Firewall (security group)
New security group

Storage (volumes)
1 volume(s) - 8 GiB

Free tier: In your first year of opening an AWS account, you get 700 hours per month.

Success
Successfully initiated launch of instance (i-079a616ae52c65abf)

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](#)

Step 2: Install and Configure CloudWatch Agent

What to do:

Connect to the EC2 instance using SSH, then run:

```
sudo yum install amazon-cloudwatch-agent -y
```

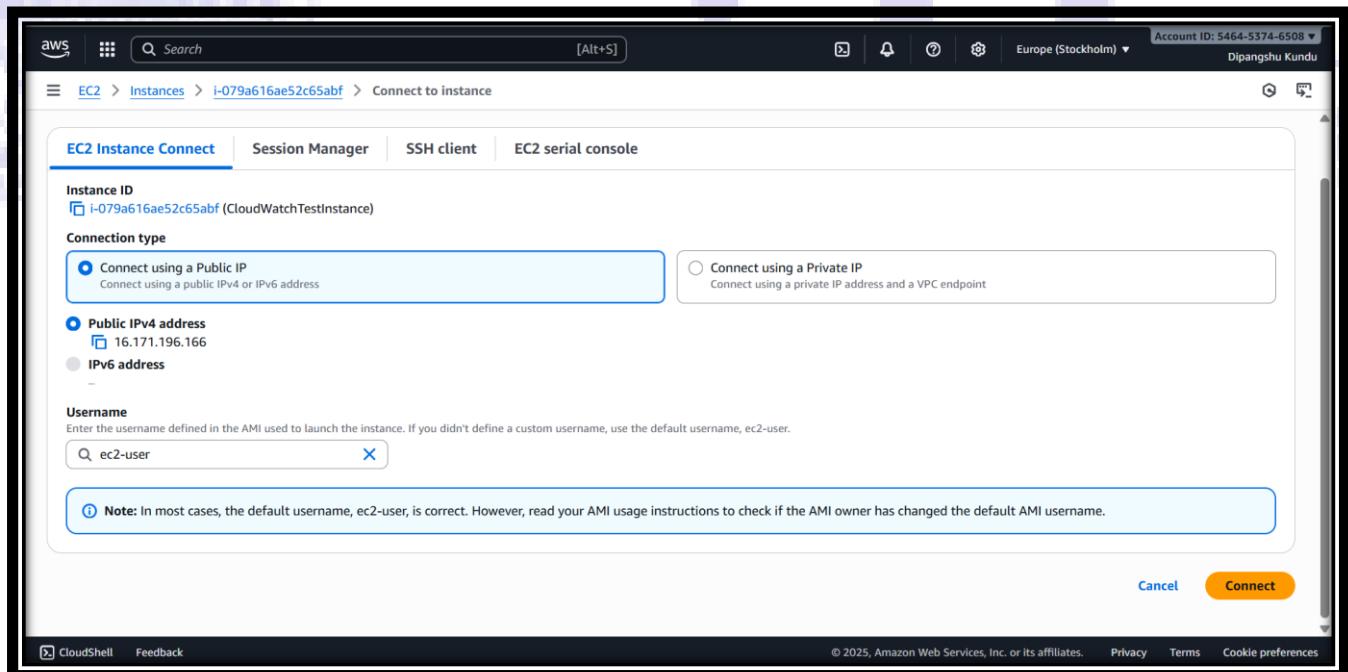
This installs the agent.

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

This wizard asks simple questions to generate a config file. It will ask:

- Install agent as root? → yes
- Format: json
- Collect CPU stats? → yes
- Collect memory metrics? → yes
- Collect disk metrics? → yes
- Log file collection? → no (optional)

By default, CloudWatch only monitors basic EC2 metrics like CPU and network. To monitor memory and disk usage, you must install the CloudWatchAgent.



The screenshot shows a terminal window on an Amazon Linux 2023 instance. The user is installing the Amazon CloudWatch Agent via yum. The terminal output includes:

```

/m/'
[ec2-user@ip-172-31-36-206 ~]$ 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
=====
Total
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
Preparing :
  Running scriptlet: amazon-cloudwatch-agent-1.300057.2-1.amzn2023.x86_64
create group cwagent, result: 0
=====
1/1
1/1
=====
i-079a616ae52c65abf (CloudWatchTestInstance)
Public IPs: 16.171.196.166  Private IPs: 172.31.36.206

```

At the bottom, a modal window displays the instance ID and its public and private IP addresses.

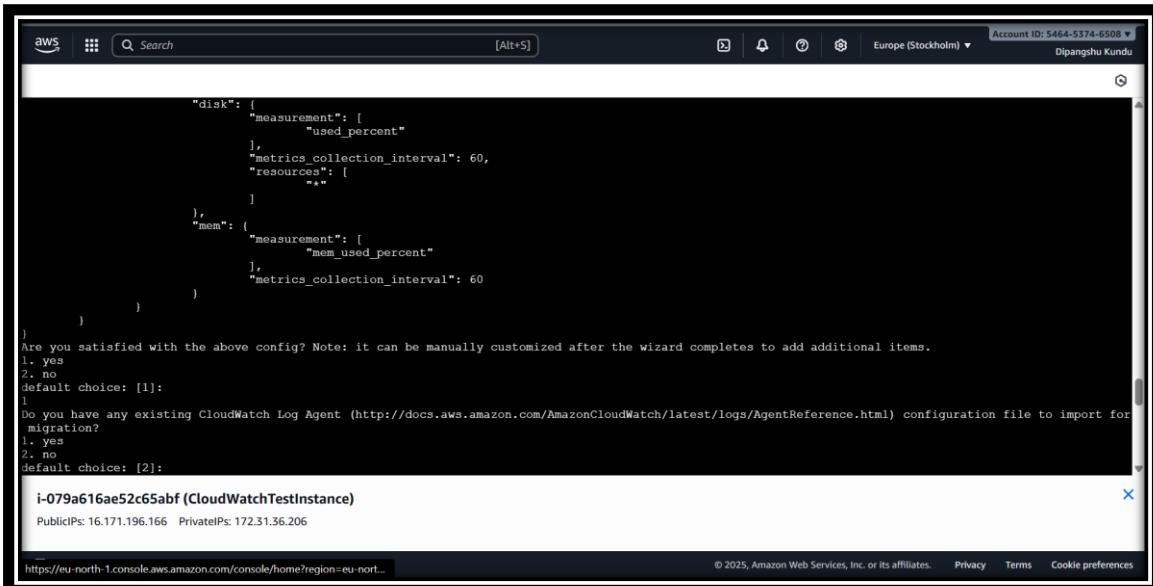
The screenshot shows a terminal window running the Amazon CloudWatch Agent Configuration Manager. The user is prompted through a series of questions:

- On which OS are you planning to use the agent? (Choices: 1. linux, 2. windows, 3. darwin)
- Are you using EC2 or On-Premises hosts? (Choices: 1. EC2, 2. On-Premises)
- Which user are you planning to run the agent? (Choices: 1. cwagent, 2. root, 3. others)
- Do you want to turn on StatsD daemon? (Choices: 1. yes, 2.)

After the configuration is completed, a modal window shows the instance ID and its public and private IP addresses.

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
Do you want to monitor any host metrics? e.g. CPU, memory, etc.
1. yes
2. no
default choice: [1]:
1
Do you want to monitor cpu metrics per core?
1. yes
2. no
default choice: [1]:
1
Do you want to add ec2 dimensions (ImageId, InstanceId, InstanceType, AutoScalingGroupName) into all of your metrics if the info is available?
1. yes
2. no
default choice: [1]:
2
Do you want to aggregate ec2 dimensions (InstanceId)?
1. yes
2. no
default choice: [1]:
1
i-079a616ae52c65abf (CloudWatchTestInstance)
PublicIPs: 16.171.196.166 PrivateIPs: 172.31.36.206

Do you want to aggregate ec2 dimensions (InstanceId)?
1. yes
2. no
default choice: [1]:
2
Would you like to collect your metrics at high resolution (sub-minute resolution)? This enables sub-minute resolution for all metrics, but you can customize for specific metrics in the output json file.
1. 1s
2. 10s
3. 30s
4. 60s
default choice: [4]:
4
Which default metrics config do you want?
1. Basic
2. Standard
3. Advanced
4. None
default choice: [1]:
1
Current config as follows:
{
 "agent": {
 "metrics_collection_interval": 60,
 "run_as_user": "root"
 },
 "metrics": {
 "metrics_collected": {
 "cpu": {}
 }
 }
}
i-079a616ae52c65abf (CloudWatchTestInstance)
PublicIPs: 16.171.196.166 PrivateIPs: 172.31.36.206



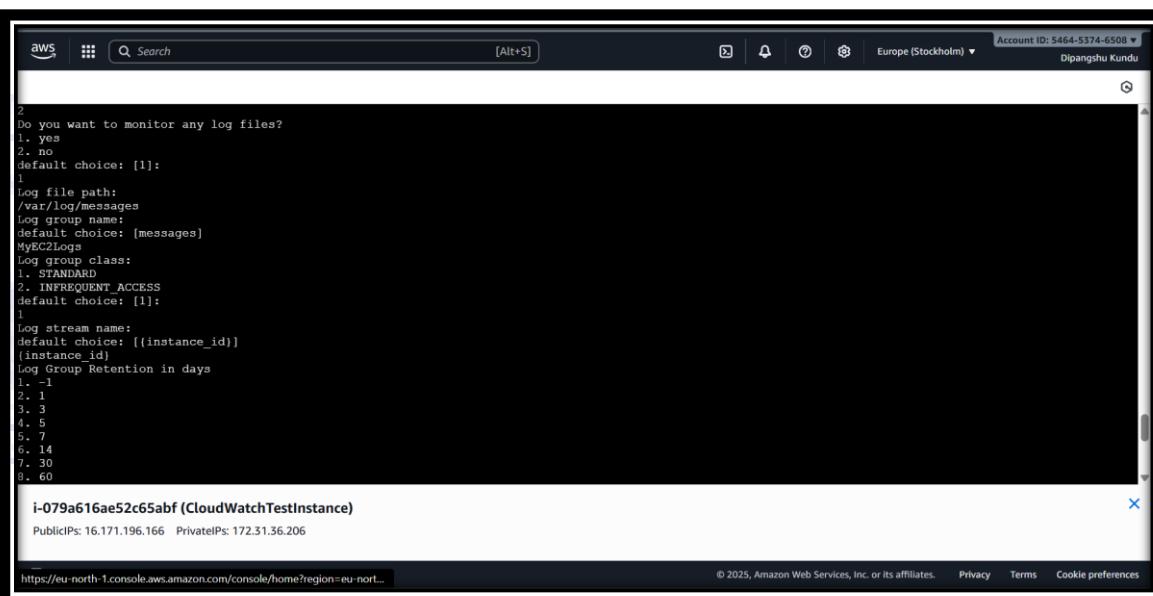
```

"disk": [
    "measurement": [
        "used_percent"
    ],
    "metrics_collection_interval": 60,
    "resources": [
        "*"
    ]
},
"mem": [
    "measurement": [
        "mem_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]:
i-079a616ae52c65abf (CloudWatchTestInstance)
PublicIPs: 16.171.196.166 PrivateIPs: 172.31.36.206

```

https://eu-north-1.console.aws.amazon.com/console/home?region=eu-nort... © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

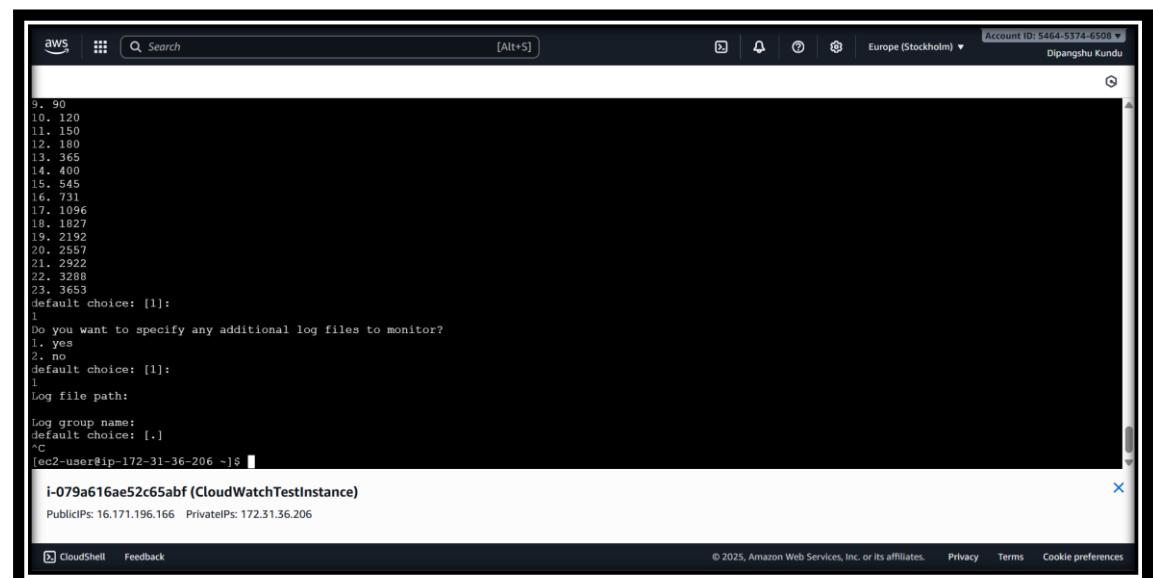


```

2
Do you want to monitor any log files?
1. yes
2. no
default choice: [1]:
1
Log file path:
/var/log/messages
Log group name:
default choice: [messages]
MyEC2Logs
Log group class:
1. STANDARD
2. INFREQUENT_ACCESS
default choice: [1]:
1
Log stream name:
default choice: [{{instance_id}}]
{{instance_id}}
Log Group Retention in days
1. -1
2. 1
3. 3
4. 5
5. 7
6. 14
7. 30
8. 60
i-079a616ae52c65abf (CloudWatchTestInstance)
PublicIPs: 16.171.196.166 PrivateIPs: 172.31.36.206

```

https://eu-north-1.console.aws.amazon.com/console/home?region=eu-nort... © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences



```

9. 90
10. 120
11. 150
12. 180
13. 365
14. 400
15. 545
16. 731
17. 1096
18. 1827
19. 2192
20. 2557
21. 2922
22. 3288
23. 3653
default choice: [1]:
1
Do you want to specify any additional log files to monitor?
1. yes
2. no
default choice: [1]:
1
Log file path:
Log group name:
default choice: [..]
^C
[ec2-user@ip-172-31-36-206 ~]$ 
i-079a616ae52c65abf (CloudWatchTestInstance)
PublicIPs: 16.171.196.166 PrivateIPs: 172.31.36.206

```

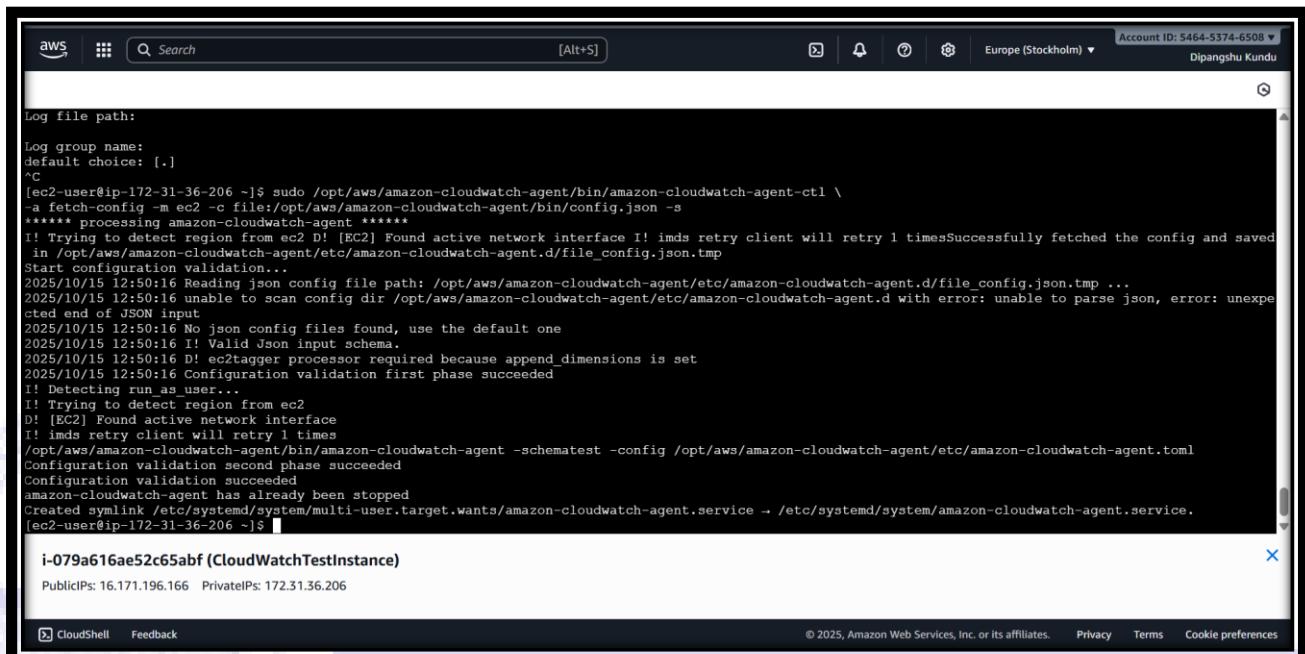
CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Step 3: Start the CloudWatch Agent

Once configuration is done, start the agent with:

```
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
```

This fetches our monitoring configuration and starts sending metrics from our EC2 instance to CloudWatch.



```
aws Log file path: Log group name: default choice: [.] ^C [ec2-user@ip-172-31-36-206 ~]$ 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 *****
! Trying to detect region from ec2 D! [EC2] Found active network interface !! 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 12:50:16 Reading json config file path: /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.d/file_config.json.tmp ...
2025/10/15 12:50:16 unable to scan config dir /opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.d with error: unable to parse json, error: unexpected end of JSON input
2025/10/15 12:50:16 No json config files found, use the default one
2025/10/15 12:50:16 ! Valid Json input schema.
2025/10/15 12:50:16 D! ec2tagger processor required because append dimensions is set
2025/10/15 12:50:16 Configuration validation first phase succeeded
! Detecting run_as_user...
! Trying to detect region from ec2
D! [EC2] Found active network interface
! 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-172-31-36-206 ~]$
```

i-079a616ae52c65abf (CloudWatchTestInstance)

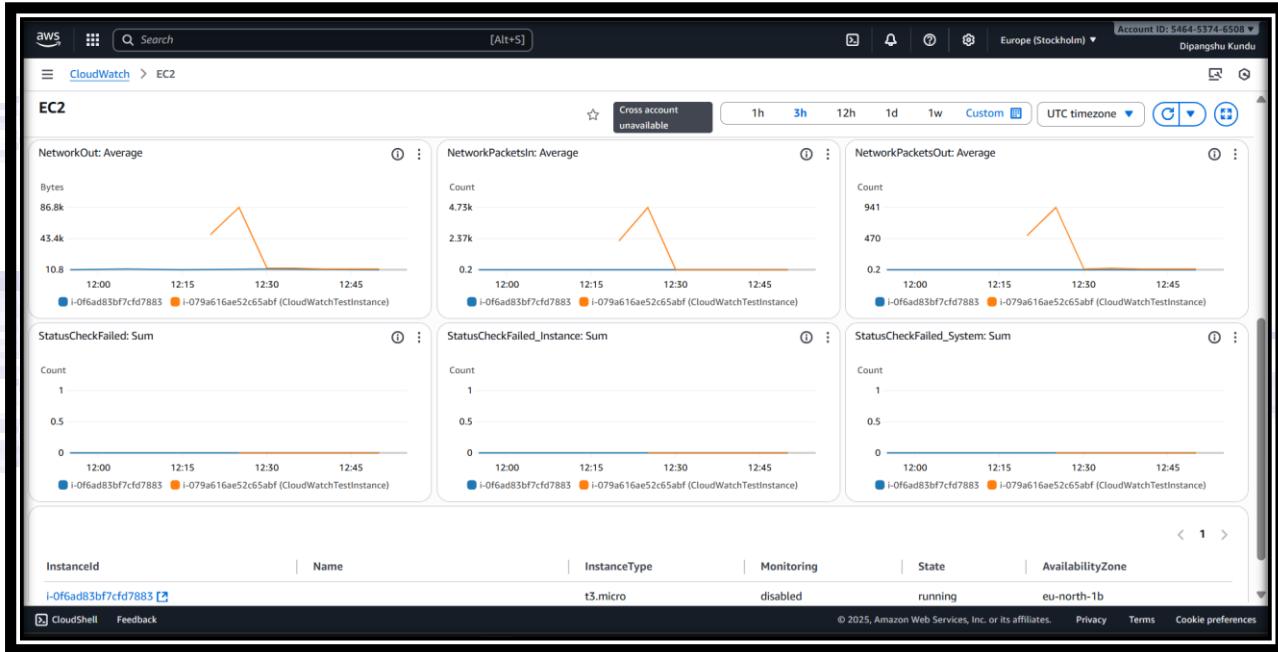
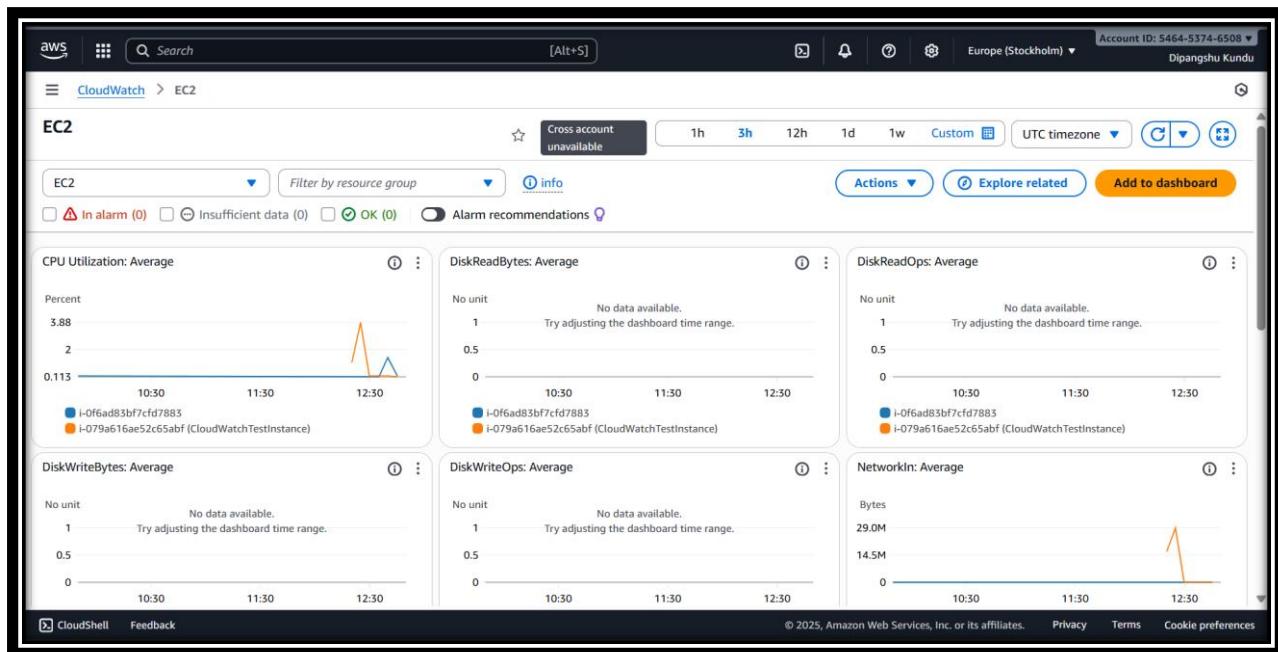
Public IPs: 16.171.196.166 Private IPs: 172.31.36.206

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

Step 4: Verify Metrics in CloudWatch

- Go to AWS Console → CloudWatch → Metrics
- Click EC2 metrics
- We should see:
 - CPU Utilization
 - mem_used_percent (Memory)
 - disk_used_percent (Disk)

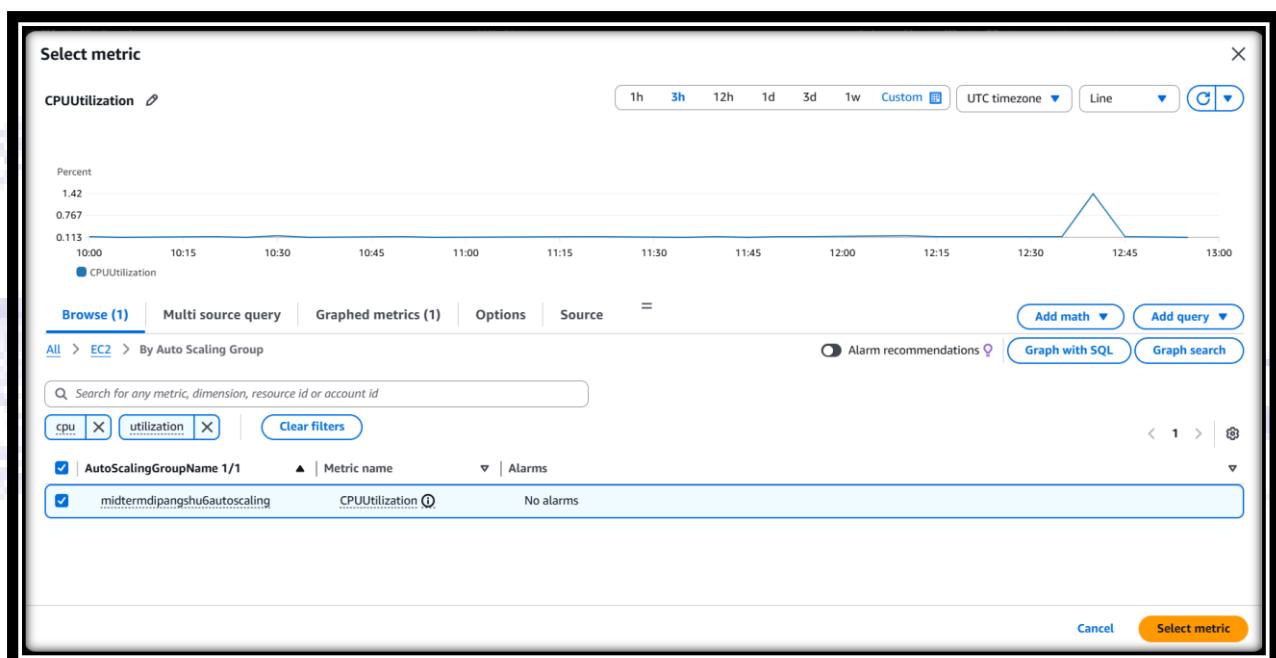
This confirms that our CloudWatch Agent is correctly sending data from your EC2 instance.



Step 5: Create a CloudWatch Alarm

- Go to **CloudWatch Console** → **Alarms** → **Create Alarm**
- Select metric: **CPU Utilization**
- Set condition:
 - **Greater than 70%**
 - For **2 consecutive 5-minute periods**
- Notification:
 - Create or select **SNS Topic**
 - Add our **email** to receive alerts
- Click **Create alarm**

A **CloudWatch Alarm** notifies you when something goes wrong. Here, if CPU usage goes too high, you'll get an **email alert**—this is proactive monitoring.



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
70
35.1
0.113
10:30 11:00 11:30 12:00 12:30 13:00
CPUUtilization

Namespace: AWS/EC2
Metric name: CPUUtilization
AutoScalingGroupName: midtermdipangshu6autoscaling
Statistic: Average
Period: 5 minutes

Conditions

Threshold type

[https://eu-north-1.console.aws.amazon.com/cloudwatch/home?region=eu-north-1...](https://eu-north-1.console.aws.amazon.com/cloudwatch/home?region=eu-north-1#)

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

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.
70
Must be a number.

Additional configuration

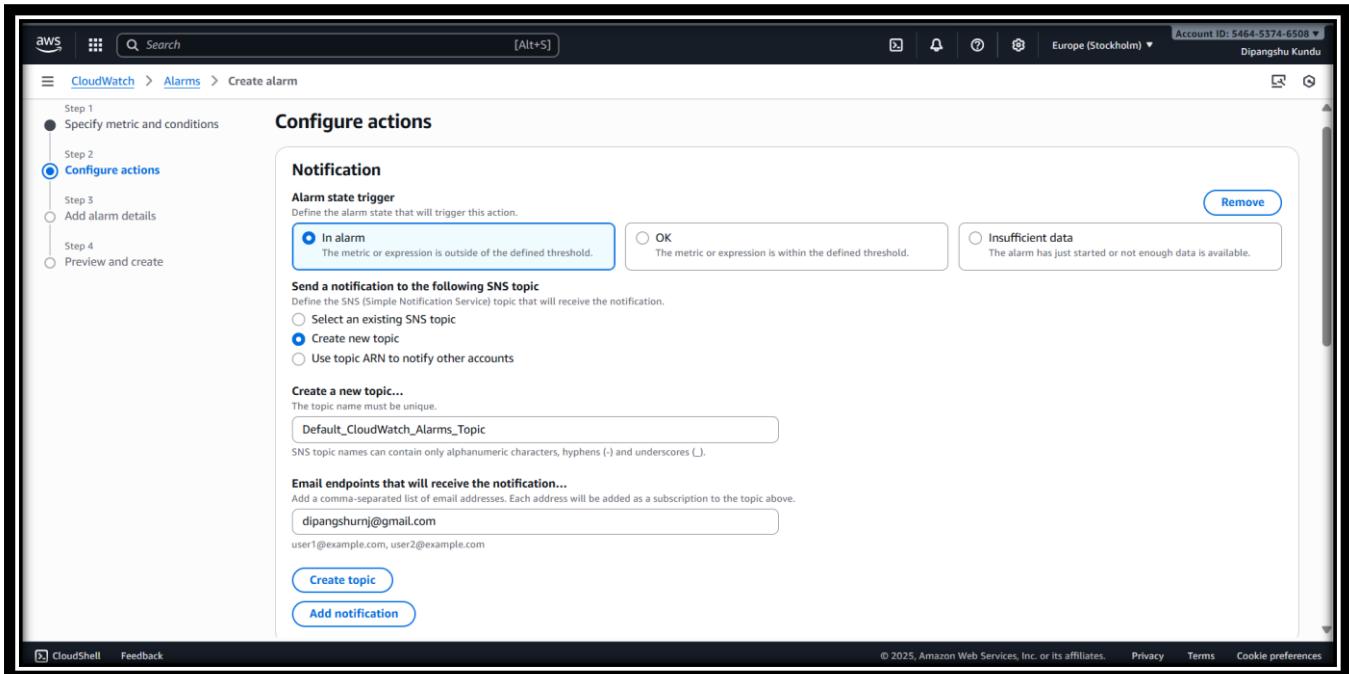
Datapoints to alarm
Define the number of datapoints within the evaluation period that must be breaching to cause the alarm to go to ALARM state.
1 out of 1

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

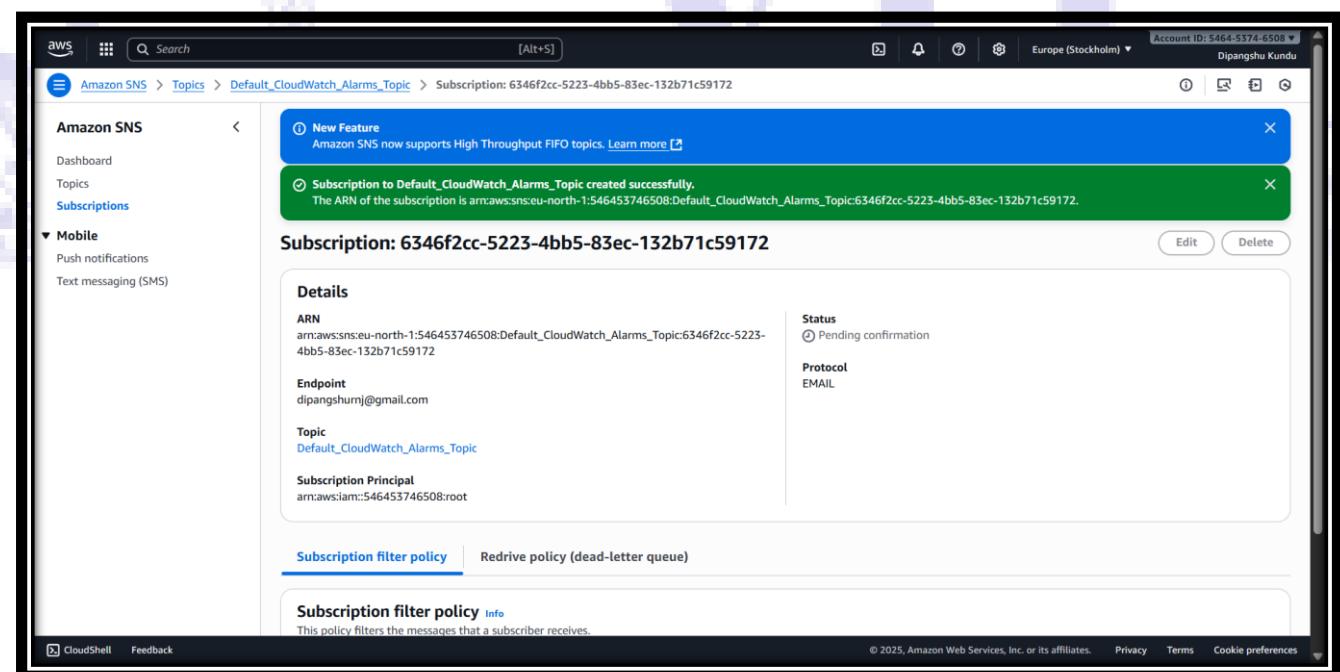
<https://eu-north-1.console.aws.amazon.com/console/home?region=eu-north-1...>

Cancel Next

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



The screenshot shows the 'Configure actions' step of creating a CloudWatch alarm. The left sidebar lists steps: Step 1 (Specify metric and conditions), Step 2 (Configure actions, which is selected), Step 3 (Add alarm details), and Step 4 (Preview and create). The main area is titled 'Notification' and contains the 'Alarm state trigger' section. It shows three options: 'In alarm' (selected), 'OK', and 'Insufficient data'. Below this is the 'Send a notification to the following SNS topic' section, which includes options to 'Select an existing SNS topic', 'Create new topic' (which is selected), and 'Use topic ARN to notify other accounts'. A text input field contains 'Default_CloudWatch_Alarms_Topic'. The 'Email endpoints that will receive the notification...' section shows an email address 'dipangshurnj@gmail.com' entered into a text input field. At the bottom are 'Create topic' and 'Add notification' buttons.



The screenshot shows the 'Subscription' details for a specific subscription. The left sidebar shows 'Amazon SNS' with 'Topics' selected. The main area shows a success message: 'Subscription to Default_CloudWatch_Alarms_Topic created successfully.' The ARN of the subscription is listed as 'arn:aws:sns:eu-north-1:546453746508:Default_CloudWatch_Alarms_Topic:6346f2cc-5223-4bb5-83ec-132b71c59172'. Below this, the 'Subscription: 6346f2cc-5223-4bb5-83ec-132b71c59172' section displays the following details:

- ARN:** arn:aws:sns:eu-north-1:546453746508:Default_CloudWatch_Alarms_Topic:6346f2cc-5223-4bb5-83ec-132b71c59172
- Endpoint:** dipangshurnj@gmail.com
- Topic:** Default_CloudWatch_Alarms_Topic
- Subscription Principal:** arn:aws:iam::546453746508:root
- Status:** Pending confirmation
- Protocol:** EMAIL

At the bottom, there are tabs for 'Subscription filter policy' (selected) and 'Redrive policy (dead-letter queue)'. A note below the policy tab states: 'This policy filters the messages that a subscriber receives.'

Add alarm details

Name and description

Alarm name
HighCPU_CloudWatchTestInstance

Alarm description - optional View formatting guidelines

Edit **Preview**

This is an H1
double asterisks will produce strong character
This is [an example](https://example.com/) inline link.

Up to 1024 characters (0/1024)

Markdown formatting is only applied when viewing your alarm in the console. The description will remain in plain text in the alarm notifications.

Tags - optional Info

No tags associated with the resource.

Add new tag

You can add up to 50 tags.

Preview and create

Step 1: 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

70

35.1

0.113

10:30 11:00 11:30 12:00 12:30 13:00

CPUUtilization

Namespace
AWS/EC2

Metric name
CPUutilization

AutoScalingGroupName
midtermdipangshu6autoscaling

Statistic
Average

Period
5 minutes

Conditions

Threshold type

The screenshot shows the 'Create alarm' wizard on the 'Step 1: Set conditions' page. The 'Conditions' section is active, showing a static threshold configuration where CPUUtilization is greater than or equal to 70. There is a link to 'Additional configuration'.

Conditions

Threshold type
Static

Whenever **CPUUtilization** is
Greater/Equal (\geq)

than...
70

Additional configuration

Step 2: Configure actions

Actions

Notification
When In alarm, send a notification to "Default_CloudWatch_Alarms_Topic"

Step 3: Add alarm details

Alarm details

Name
HighCPU_CloudWatchTestInstance

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

The screenshot shows the 'Create alarm' wizard on the 'Step 2: Configure actions' page. The 'Actions' section is active, showing a notification rule to the Default_CloudWatch_Alarms_Topic. There is a link to 'Additional configuration'.

Additional configuration

Step 2: Configure actions

Actions

Notification
When In alarm, send a notification to "Default_CloudWatch_Alarms_Topic"

Step 3: Add alarm details

Alarm details

Name
HighCPU_CloudWatchTestInstance

Description
-

Tags (0)

Cancel Previous Create alarm

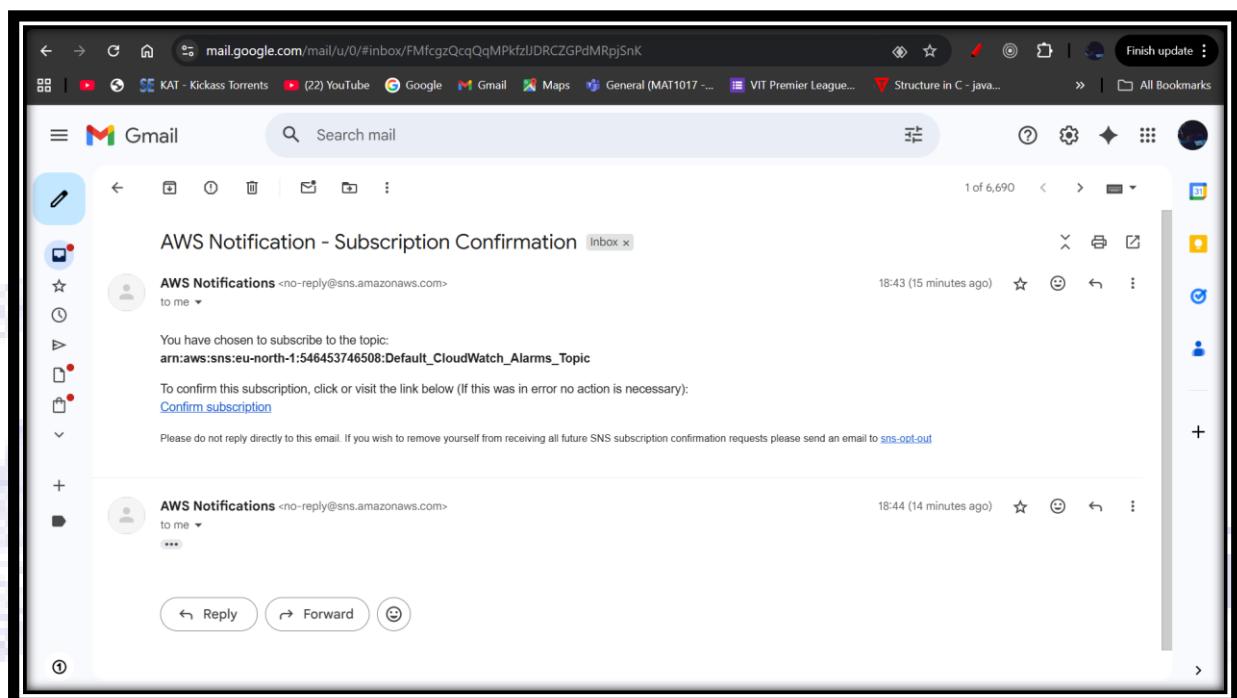
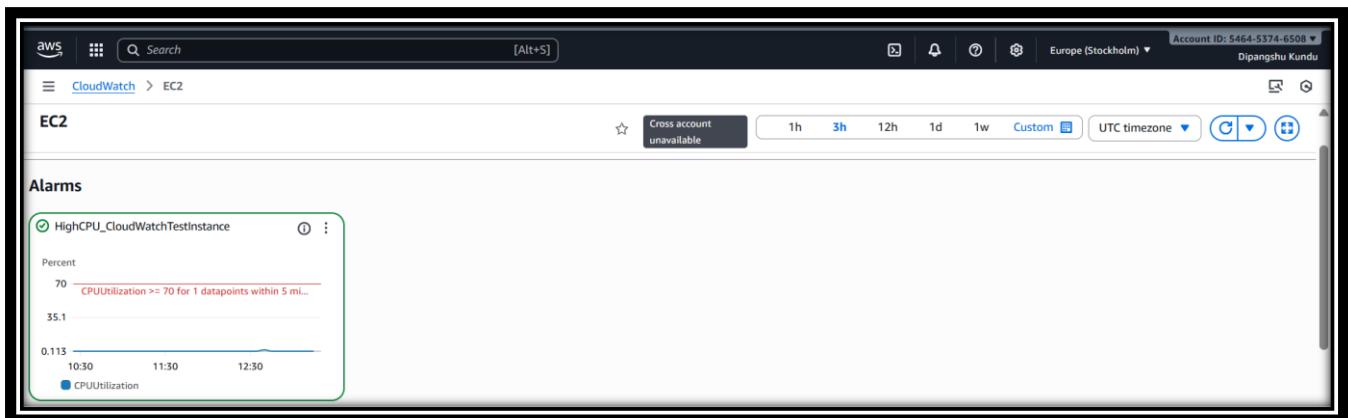
CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

The screenshot shows the AWS CloudWatch Metrics Alarms console. On the left, there's a navigation sidebar with options like AI Operations, Alarms, Logs, Metrics, Application Signals, Network Monitoring, and Insights. The main area displays a green success message: "Successfully created alarm HighCPU_CloudWatchTestInstance." Below it, a blue info message says "Some subscriptions are pending confirmation" and "Amazon SNS doesn't send messages to an endpoint until the subscription is confirmed." A "View SNS Subscriptions" button is available. The central part of the screen shows a table titled "Alarms (1)" with one row for "HighCPU_CloudWatchTestInstance". The table includes columns for Name, State, Last state update (UTC), Conditions, and Actions. The Conditions column shows "CPUUtilization >= 70 for 1 datapoints within 5 minutes". The Actions column has a "Actions e..." button. At the bottom, the URL is https://eu-north-1.console.aws.amazon.com/console/home?region=eu-nort... and the footer includes links for Privacy, Terms, and Cookie preferences.

SENDING ALARM NOTIFICATION PROCESS

The screenshot shows the AWS CloudShell terminal interface. The user is running a sudo yum install stress command. The output shows the package being installed from the amazonlinux repository. It includes transaction details, download speeds, and a warning about a newer Amazon Linux release. The terminal also shows the user's AWS account ID and IP information. The URL at the bottom is https://eu-north-1.console.aws.amazon.com/console/home?region=eu-nort... and the footer includes links for Privacy, Terms, and Cookie preferences.

The screenshot shows the AWS CloudShell terminal interface. The user runs a stress --cpu 1 --timeout 60 command. The output indicates a successful run completed in 60 seconds. The terminal shows the user's AWS account ID and IP information. The URL at the bottom is https://eu-north-1.console.aws.amazon.com/console/home?region=eu-nort... and the footer includes links for CloudShell, Feedback, Privacy, Terms, and Cookie preferences.



New Feature
Amazon SNS now supports High Throughput FIFO topics. Learn more

Message published to topic Default_CloudWatch_Alarms_Topic successfully.
Message ID: 95f12e76-0f11-5670-bc39-4f1fab9fdb66
Request ID: 044bccee-d6d4-516d-9e49-afa7725a7c7b

Default_CloudWatch_Alarms_Topic

Details

Name: Default_CloudWatch_Alarms_Topic

Display name:

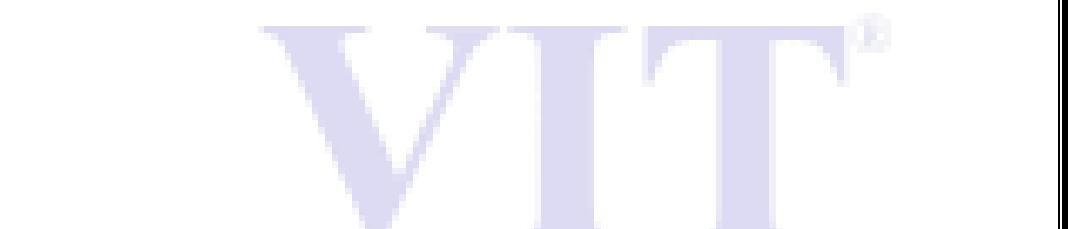
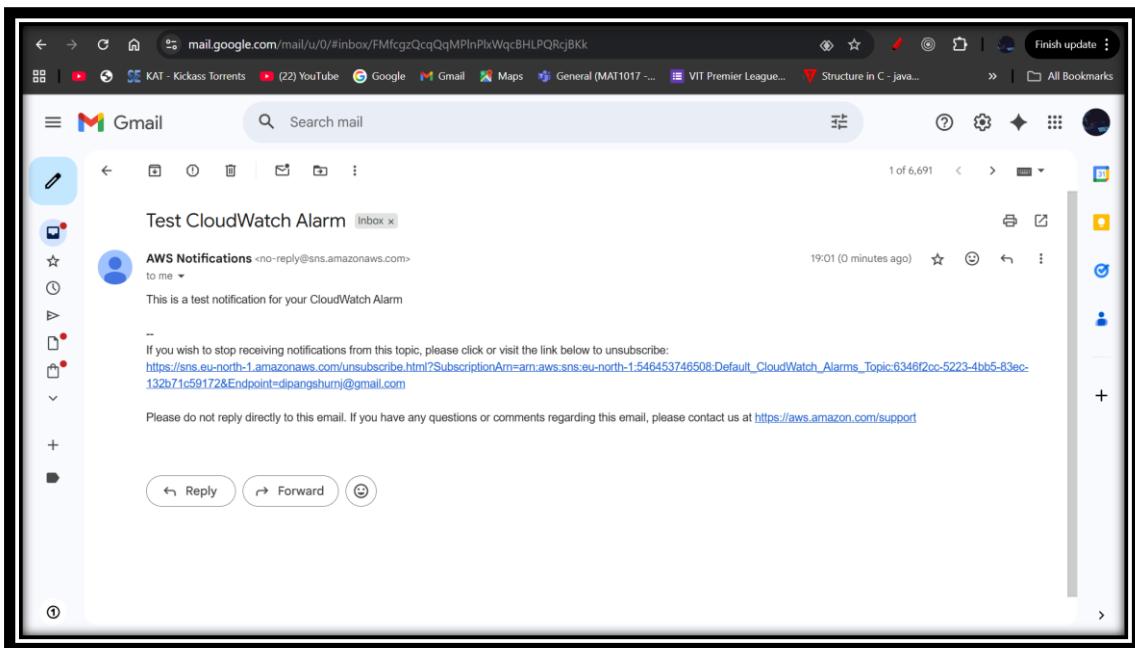
ARN: arn:aws:sns:eu-north-1:546453746508:Default_CloudWatch_Alarms_Topic

Topic owner: 546453746508

Type: Standard

Subscriptions (1)

Subscriptions (1) Edit Delete Request confirmation Confirm subscription Create subscription



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