

Lab 18

Configure Cloud Watch & SNS

Please configure VPC / use default vpc as per your requirement.

Click "EC2" service.

The screenshot shows the AWS Management Console interface. The top navigation bar includes the AWS logo, a 'Services' dropdown, 'Resource Groups', and user information ('siva1n82', 'Mumbai', 'Support'). Below the navigation bar is a search bar and two buttons: 'Group' and 'A-Z'. The main content area is titled 'History' and contains a list of services under various categories:

- Compute:** EC2, Lightsail, Elastic Container Service, Lambda, Batch, Elastic Beanstalk.
- Storage:** S3, EFS, Glacier, Storage Gateway.
- Database:** Relational Database Service, DynamoDB, ElastiCache, Amazon Redshift.
- Migration:** AWS Migration Hub, Application Discovery Service, Database Migration Service, Server Migration Service, Snowball.
- Developer Tools:** CodeStar, CodeCommit, CodeBuild, CodeDeploy, CodePipeline, Cloud9, X-Ray.
- Management Tools:** CloudWatch, AWS Auto Scaling, CloudFormation, CloudTrail, Config, OpsWorks, Service Catalog, Systems Manager, Trusted Advisor, Managed Services.
- Media Services:** Elastic Transcoder, Kinesis Video Streams, MediaConvert, MediaLive, MediaPackage, MediaStore.
- Machine Learning:** Amazon SageMaker, Amazon Comprehend, AWS DeepLens, Amazon Lex, Machine Learning, Amazon Polly, Rekognition, Amazon Transcribe, Amazon Translate.
- Analytics:** Athena, EMR, CloudSearch, Elasticsearch Service, Kinesis, QuickSight, Data Pipeline, AWS Glue.
- Security, Identity & Compliance:** IAM, Cognito, GuardDuty, Inspector, Amazon Macie, AWS Single Sign On.
- Customer Engagement:** Amazon Connect, Pinpoint, Simple Email Service.
- Business Productivity:** Alexa for Business, Amazon Chime, WorkDocs, WorkMail.
- Desktop & App Streaming:** WorkSpaces, AppStream 2.0.
- Internet Of Things:** (represented by a small icon).
- AR & VR:** Amazon Sumerian.
- Application Integration:** Step Functions, Amazon MQ, Simple Notification Service, Simple Queue Service, SWF.
- Customer Engagement:** Amazon Connect, Pinpoint, Simple Email Service.
- Business Productivity:** Alexa for Business, Amazon Chime, WorkDocs, WorkMail.
- Desktop & App Streaming:** WorkSpaces, AppStream 2.0.
- Internet Of Things:** (represented by a small icon).

At the bottom of the page, there are links for 'Feedback', 'English (US)', 'Privacy Policy', and 'Terms of Use'.

Launch instance → Select “Linux”.

Step 1: Choose an Amazon Machine Image (AMI)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

Quick Start	1 to 35 of 35 AMIs	
My AMIs		
AWS Marketplace		
Community AMIs		
<input type="checkbox"/> Free tier only ⓘ		
Amazon Linux Free tier eligible	Amazon Linux AMI 2017.09.1 (HVM), SSD Volume Type - ami-531a4c3c The Amazon Linux AMI is an EBS-backed, AWS-supported image. The default image includes AWS command line tools, Python, Ruby, Perl, and Java. The repositories include Docker, PHP, MySQL, PostgreSQL, and other packages. Root device type: ebs Virtualization type: hvm	Select
Amazon Linux Free tier eligible	Amazon Linux 2 LTS Candidate AMI 2017.12.0 (HVM), SSD Volume Type - ami-3b2f7954 Amazon Linux 2 is the next generation of Amazon Linux. It includes the latest LTS kernel (4.9) tuned for enhanced performance on Amazon EC2, systemd support, newer versions of glibc, gcc and binutils, and an additional set of core packages for performance and security improvements. Root device type: ebs Virtualization type: hvm	Select
SUSE Linux Free tier eligible	SUSE Linux Enterprise Server 12 SP3 (HVM), SSD Volume Type - ami-f7267298 SUSE Linux Enterprise Server 12 Service Pack 3 (HVM), EBS General Purpose (SSD) Volume Type. Public Cloud, Advanced Systems Management, Web and Scripting, and Legacy modules enabled. Root device type: ebs Virtualization type: hvm	Select
Red Hat Free tier eligible	Red Hat Enterprise Linux 7.4 (HVM), SSD Volume Type - ami-e60e5a89 Red Hat Enterprise Linux version 7.4 (HVM), EBS General Purpose (SSD) Volume Type Root device type: ebs Virtualization type: hvm	Select
Windows Free tier eligible	Microsoft Windows Server 2016 Base - ami-ad8addc2 Microsoft Windows 2016 Datacenter edition. [English] Root device type: ebs Virtualization type: hvm	Select

Select “General purpose – t2.micro”

Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. [Learn more](#) about instance types and how they can meet your computing needs.

Currently selected: t2.micro (Variable ECUs, 1 vCPUs, 2.5 GHz, Intel Xeon Family, 1 GiB memory, EBS only)								
	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
<input type="checkbox"/>	General purpose	t2.nano	1	0.5	EBS only	-	Low to Moderate	Yes
<input checked="" type="checkbox"/>	General purpose	t2.micro Free tier eligible	1	1	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.small	1	2	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.medium	2	4	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.large	2	8	EBS only	-	Low to Moderate	Yes
<input type="checkbox"/>	General purpose	t2.xlarge	4	16	EBS only	-	Moderate	Yes
<input type="checkbox"/>	General purpose	t2.2xlarge	8	32	EBS only	-	Moderate	Yes
<input type="checkbox"/>	General purpose	m5.large	2	8	EBS only	Yes	Up to 10 Gigabit	Yes
<input type="checkbox"/>	General purpose	m5.xlarge	4	16	EBS only	Yes	Up to 10 Gigabit	Yes
<input type="checkbox"/>	General purpose	m5.2xlarge	8	32	EBS only	Yes	Up to 10 Gigabit	Yes
<input type="checkbox"/>	General purpose	m5.4xlarge	16	64	EBS only	Yes	Up to 10 Gigabit	Yes

Cancel Previous Review and Launch Next: Configure Instance Details

Select Network "Sansbound_VPC_Chennai"

Subnet: "Sansbound Mumbai Public Subnet"

Auto-assign Public IP: Enable

Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances: 1

Purchasing option: Request Spot instances

Network: vpc-09fe2261 | Sansbound_VPC_Mumbai

Subnet: subnet-07d1c44a | Sansbound_Mumbai_Public_sub
251 IP Addresses available

Auto-assign Public IP: Enable

IAM role: None

Shutdown behavior: Stop

Enable termination protection: Protect against accidental termination

Monitoring: Enable CloudWatch detailed monitoring
Additional charges apply.

Tenancy: Shared - Run a shared hardware instance
Additional charges will apply for dedicated tenancy.

Network interfaces

Device	Network Interface	Subnet	Primary IP	Secondary IP addresses	IPv6 IPs
eth0	New network interface	subnet-07d1c44a	Auto-assign	Add IP	

[Feedback](#) [English \(US\)](#) © 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. [Privacy Policy](#) [Terms of Use](#)

Leave default and click “Next”.

The screenshot shows the AWS EC2 Management Console Launch Instance Wizard, specifically Step 4: Add Storage. The URL in the browser is <https://ap-south-1.console.aws.amazon.com/ec2/v2/home?region=ap-south-1#LaunchInstanceWizard>. The page title is "Step 4: Add Storage". The navigation bar includes tabs for 1. Choose AMI, 2. Choose Instance Type, 3. Configure Instance, 4. Add Storage (which is highlighted), 5. Add Tags, 6. Configure Security Group, and 7. Review. The main content area displays a table for adding storage volumes. A single row is present for the root volume:

Volume Type	Device	Snapshot	Size (GiB)	Volume Type	IOPS	Throughput (MB/s)	Delete on Termination	Encrypted
Root	/dev/xvda	snap-0fbaf6369a5a7ca56	8	General Purpose SSD (GP2)	100 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypted

Below the table, there is a note: "Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage. [Learn more](#) about free usage tier eligibility and usage restrictions." At the bottom of the page are buttons for Cancel, Previous, Review and Launch (which is highlighted in blue), and Next: Add Tags.

Type name as Linux Server.

EC2 Management Console X

Secure | https://ap-south-1.console.aws.amazon.com/ec2/v2/home?region=ap-south-1#LaunchInstanceWizard:

aws Services Resource Groups

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

Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver.
A copy of a tag can be applied to volumes, instances or both.
Tags will be applied to all instances and volumes. [Learn more](#) about tagging your Amazon EC2 resources.

Key	(127 characters maximum)	Value	(255 characters maximum)	Instances	Volumes
Name		Linux Server		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Add another tag (Up to 50 tags maximum)

Cancel Previous Review and Launch Next: Configure Security Group

Feedback English (US) © 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Create a new security group as Linux-Sec-Group

The screenshot shows the AWS EC2 Management Console interface. The top navigation bar includes the AWS logo, Services dropdown, Resource Groups dropdown, and user information (siva1n82, Mumbai, Support). Below the navigation is a breadcrumb trail: 1. Choose AMI, 2. Choose Instance Type, 3. Configure Instance, 4. Add Storage, 5. Add Tags, 6. Configure Security Group (which is highlighted), and 7. Review.

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow Internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group: Create a new security group Select an existing security group

Security group name:

Description:

Type	Protocol	Port Range	Source	Description
SSH	TCP	22	Custom 0.0.0.0/0	e.g. SSH for Admin Desktop

Add Rule

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

At the bottom right are buttons for **Cancel**, **Previous**, and **Review and Launch**.

At the very bottom of the page are links for **Feedback**, **English (US)**, **© 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.**, **Privacy Policy**, and **Terms of Use**.

Leave default and click “Next”.

The screenshot shows the AWS EC2 Management Console Launch Instance Wizard at Step 7: Review Instance Launch. The browser address bar shows the URL: https://ap-south-1.console.aws.amazon.com/ec2/v2/home?region=ap-south-1#LaunchInstanceWizard. The navigation bar includes Services, Resource Groups, and a user profile (sivaIn82, Mumbai, Support). Below the navigation is a progress bar with steps 1 through 7, where step 7 is highlighted.

Step 7: Review Instance Launch

Please review your instance launch details. You can go back to edit changes for each section. Click **Launch** to assign a key pair to your instance and complete the launch process.

AMI Details

Amazon Linux AMI 2017.09.1 (HVM), SSD Volume Type - ami-531a4c3c

Free tier eligible The Amazon Linux AMI is an EBS-backed, AWS-supported image. The default image includes AWS command line tools, Python, Ruby, Perl, and Java. The repositories include Docker, PHP, MySQL, PostgreSQL, and other packages.

Root Device Type: ebs Virtualization type: hvm

Instance Type

Instance Type	ECUs	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance
t2.micro	Variable	1	1	EBS only	-	Low to Moderate

Security Groups

Security group name: Linux-Sec-Group
Description: Linux-Sec-Group

Type (i)	Protocol (i)	Port Range (i)	Source (i)	Description (i)
SSH	TCP	22	0.0.0.0/0	

Instance Details

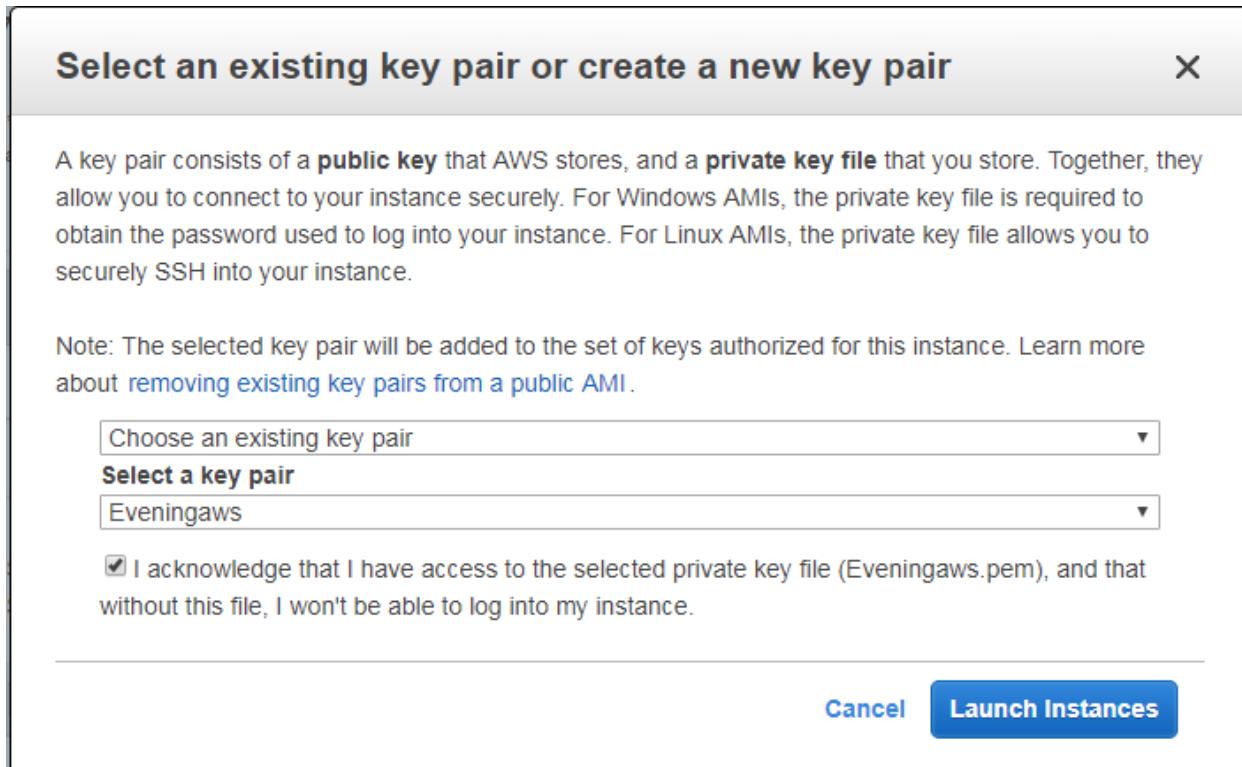
Click **Launch** to start the instance.

Buttons: Cancel, Previous, Launch.

Footer: Feedback, English (US), © 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved. Privacy Policy, Terms of Use.

Click “Launch”.

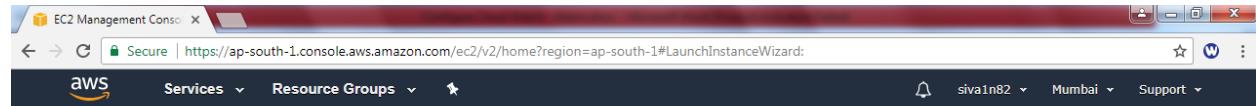
Click "Choose existing key pair".



Click "I acknowledge".

Then click "Launch instance"

Click "View instances"



Launch Status

Your instances are now launching

The following instance launches have been initiated: i-0b597ed1a7f39d0ad [View launch log](#)

Get notified of estimated charges

Create billing alerts to get an email notification when estimated charges on your AWS bill exceed an amount you define (for example, if you exceed the free usage tier).

How to connect to your instances

Your instances are launching, and it may take a few minutes until they are in the **running** state, when they will be ready for you to use. Usage hours on your new instances will start immediately and continue to accrue until you stop or terminate your instances.

Click [View Instances](#) to monitor your instances' status. Once your instances are in the **running** state, you can **connect** to them from the Instances screen. [Find out](#) how to connect to your instances.

Here are some helpful resources to get you started

- [How to connect to your Linux instance](#)
- [Amazon EC2: User Guide](#)
- [Learn about AWS Free Usage Tier](#)
- [Amazon EC2: Discussion Forum](#)

While your instances are launching you can also

[Create status check alarms](#) to be notified when these instances fail status checks. (Additional charges may apply)

[Create and attach additional EBS volumes](#) (Additional charges may apply)

[Manage security groups](#)

[View Instances](#)

[Feedback](#) [English \(US\)](#)

© 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.

[Privacy Policy](#) [Terms of Use](#)

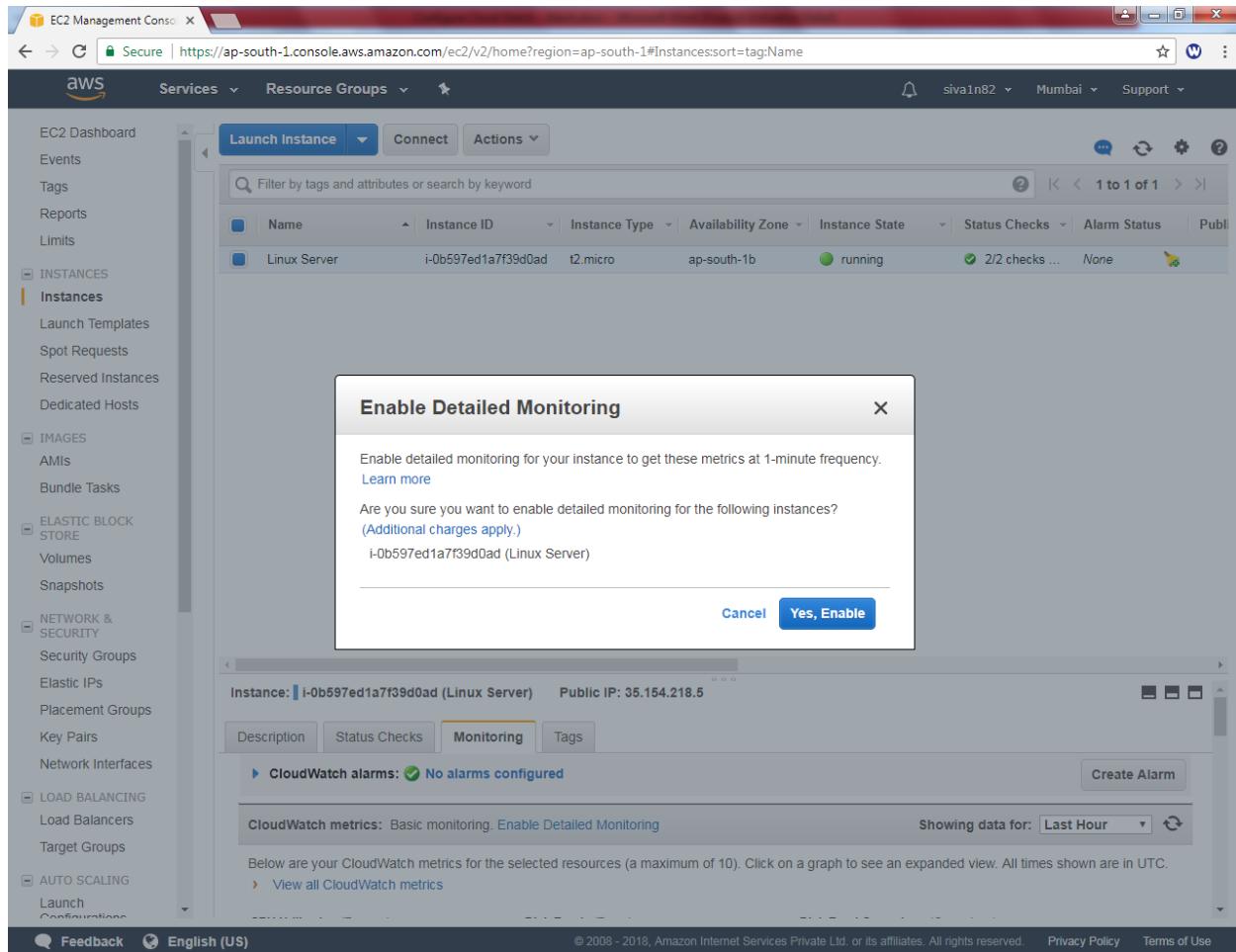
Go to EC2 instances

The screenshot shows the AWS EC2 Management Console interface. The left sidebar navigation includes: EC2 Dashboard, Events, Tags, Reports, Limits, INSTANCES (selected), Instances, Launch Templates, Spot Requests, Reserved Instances, Dedicated Hosts, IMAGES (AMIs, Bundle Tasks), ELASTIC BLOCK STORE (Volumes, Snapshots), NETWORK & SECURITY (Security Groups, Elastic IPs, Placement Groups, Key Pairs, Network Interfaces), LOAD BALANCING (Load Balancers, Target Groups), and AUTO SCALING (Launch Configurations). The main content area displays a table of instances with a single row selected: Name (Linux Server), Instance ID (i-0b597ed1a7f39d0ad), Instance Type (t2.micro), Availability Zone (ap-south-1b), Instance State (running), Status Checks (2/2 checks), and Alarm Status (None). Below this, a detailed view for the selected instance (i-0b597ed1a7f39d0ad) is shown, including fields for Description, Status Checks, Monitoring, and Tags. The detailed view table includes columns for Instance ID, Instance state, Instance type, Elastic IPs, Availability zone, Security groups, Public DNS (IPv4), IPv4 Public IP, IPv6 IPs, Private DNS, Private IPs, and Secondary private IPs.

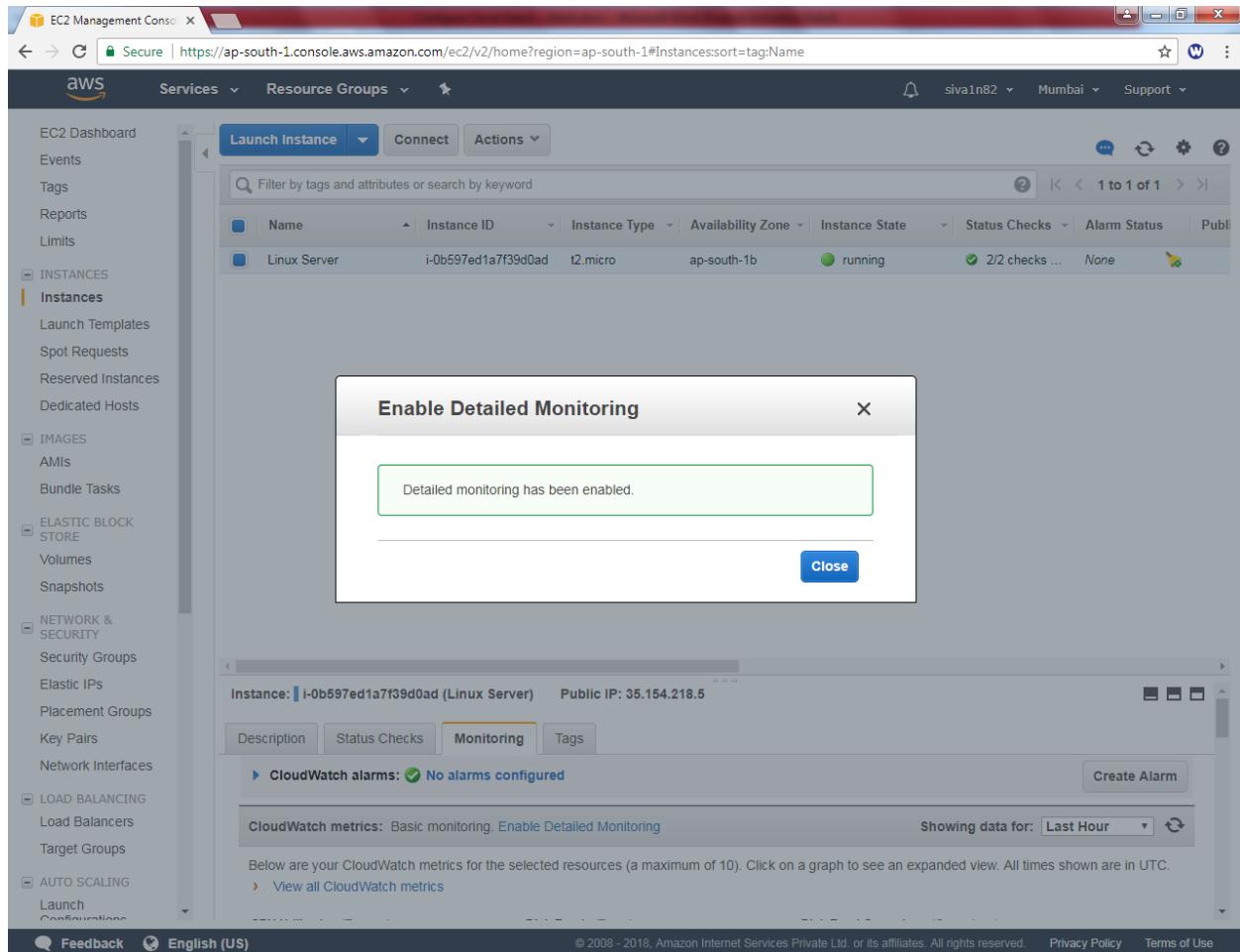
Click “Enable detailed monitoring”.

The screenshot shows the AWS EC2 Management Console interface. The left sidebar navigation menu includes: EC2 Dashboard, Events, Tags, Reports, Limits, INSTANCES (selected), Instances, Launch Templates, Spot Requests, Reserved Instances, Dedicated Hosts, IMAGES, AMIs, Bundle Tasks, ELASTIC BLOCK STORE, Volumes, Snapshots, NETWORK & SECURITY, Security Groups, Elastic IPs, Placement Groups, Key Pairs, Network Interfaces, LOAD BALANCING, Load Balancers, Target Groups, and AUTO SCALING, Launch Configurations. The main content area displays a table of instances. A single instance is selected: Name: Linux Server, Instance ID: i-0b597ed1a7f39d0ad, Instance Type: t2.micro, Availability Zone: ap-south-1b, Instance State: running, Status Checks: 2/2 checks ... (green), Alarm Status: None. Below the table, a detailed view for the selected instance (i-0b597ed1a7f39d0ad) is shown. The Public IP is 35.154.218.5. The 'Monitoring' tab is active, showing CloudWatch alarms (No alarms configured) and CloudWatch metrics (Basic monitoring, Enable Detailed Monitoring). The metrics section indicates data is being shown for the last hour. At the bottom of the page, there are links for Feedback, English (US), and footer links for Privacy Policy and Terms of Use.

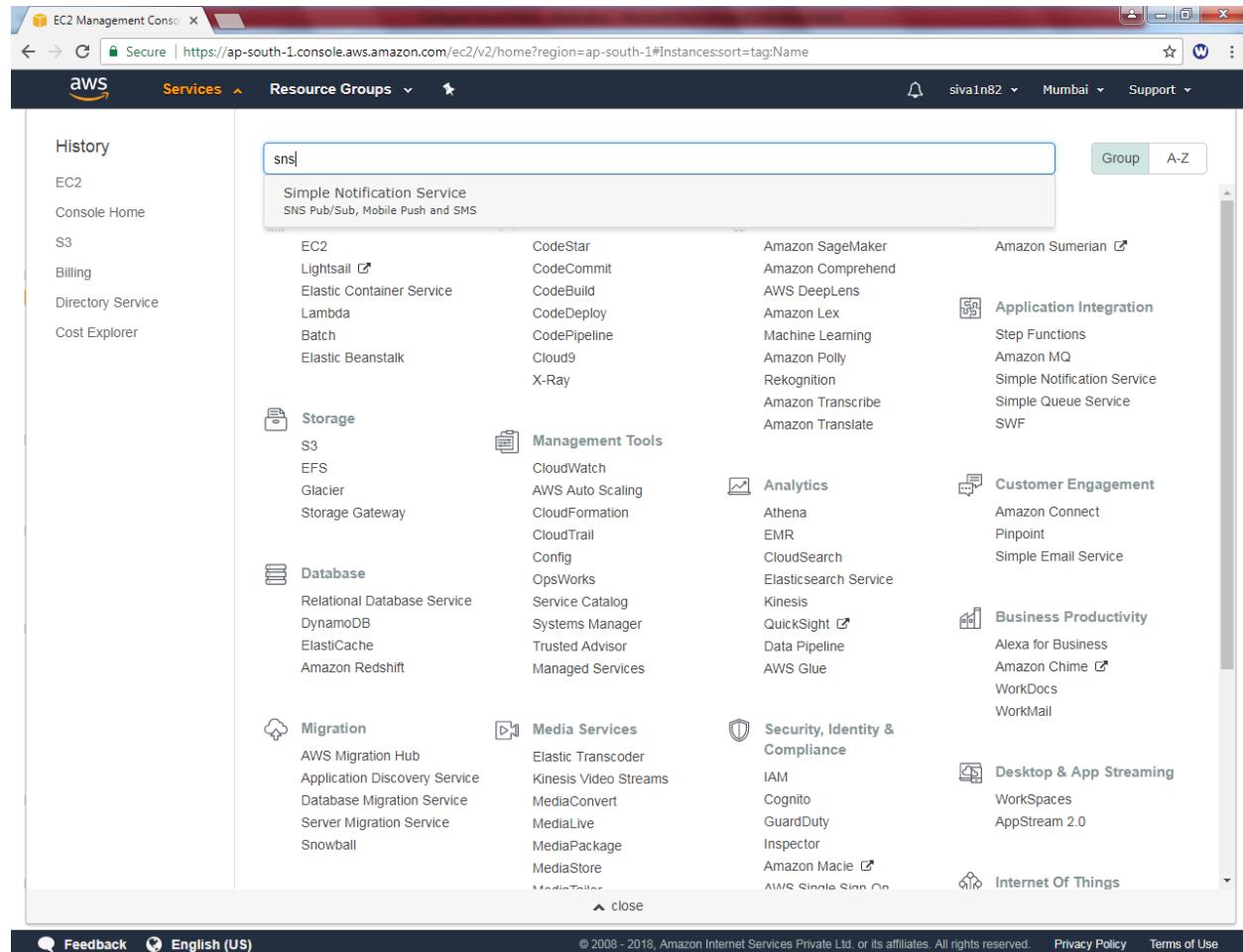
Click “Yes, enable”.



Click “Close”.



Type “SNS”.



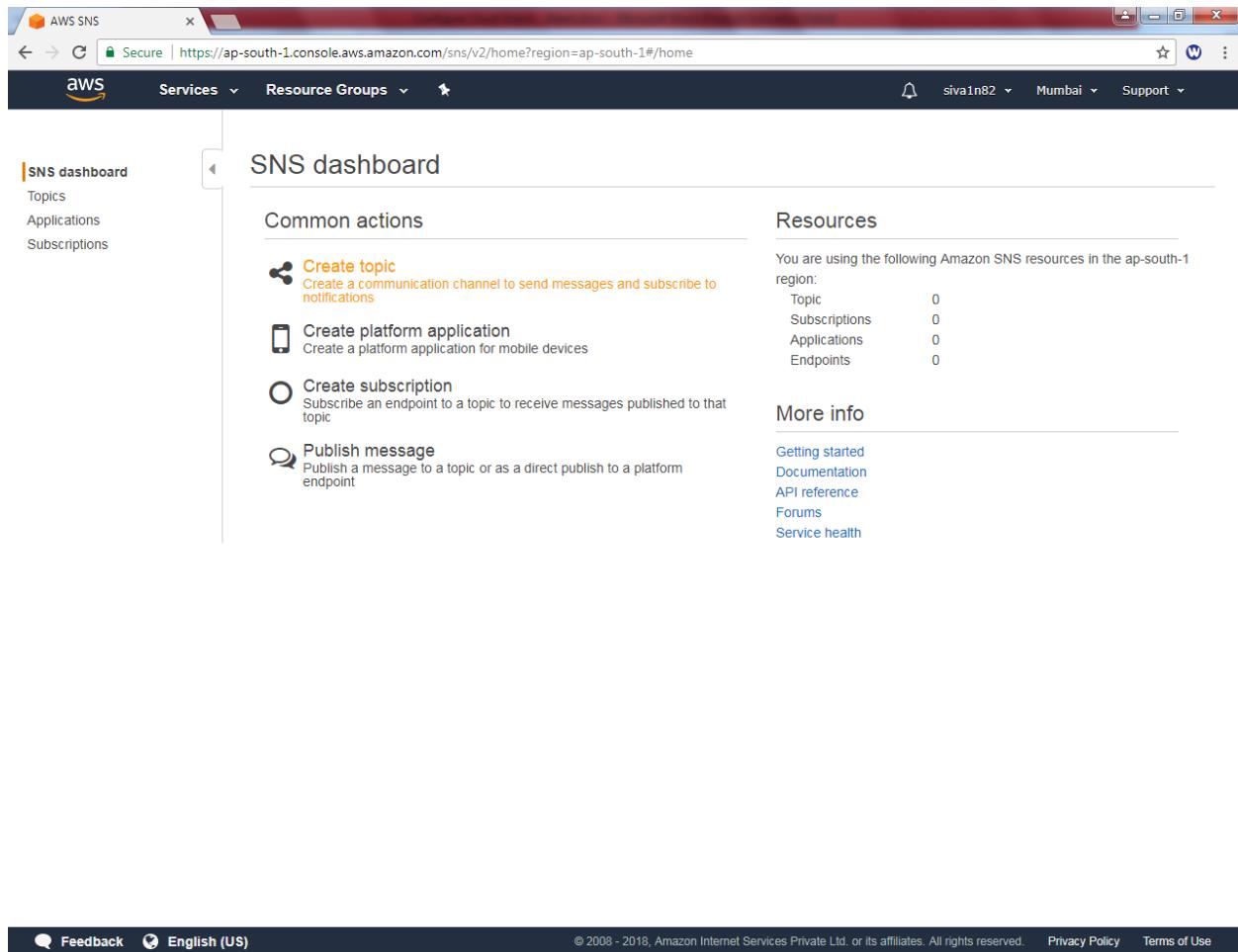
Click “Get started”.

The screenshot shows the AWS Simple Notification Service (SNS) console home page. At the top, there's a navigation bar with the AWS logo, a search bar, and user information (siva1n82, Mumbai, Support). Below the header is a large circular icon containing a purple bell-like shape. The main title "Simple Notification Service" is centered above a brief description: "Amazon Simple Notification Service (SNS) is a fast, flexible, fully managed push messaging service." A blue "Get started" button is positioned below the description. The page then features three main sections with icons and text:

- Broadcast notifications to any destination**: An icon showing a smartphone, a laptop, and a tablet connected by arrows. Text: "Amazon SNS lets you send notifications to multiple destinations in a single broadcast. Destinations can be mobile devices that are iOS, Android, Windows, or FireOS based. You can also use Amazon SNS to broadcast messages to destinations that are AWS Lambda, Amazon SQS, HTTP, Email or SMS based."
- Global & fast at massive scale**: An icon showing two globes (one blue, one orange) with arrows indicating global reach. Text: "With Amazon SNS, you can send billions of notifications across the world. Amazon SNS is available in all regions of AWS and is designed to handle your most stringent latency needs."
- Use any language or platform**: An icon showing a smartphone with a cursor pointing at it, and a box listing supported languages: Java, Python, PHP, .NET, Node.js. Text: "You can choose from a variety of programming languages or platforms to send notifications via Amazon SNS such as Java, .NET, Node.js, PHP, Python, or Ruby."

At the bottom of the page, there's a footer with the text "Amazon SNS documentation and support" and a link to the URL "https://ap-south-1.console.aws.amazon.com/sns/v2/home?region=ap-south-1#/home".

Click “Create topic”.



The screenshot shows the AWS SNS dashboard. On the left, there's a sidebar with links for 'Topics', 'Applications', and 'Subscriptions'. The main area has a header 'SNS dashboard'. Under 'Common actions', there are four items: 'Create topic' (highlighted in orange), 'Create platform application', 'Create subscription', and 'Publish message'. To the right, under 'Resources', it says 'You are using the following Amazon SNS resources in the ap-south-1 region:' followed by a table with four rows: Topic (0), Subscriptions (0), Applications (0), and Endpoints (0). Below that is a 'More info' section with links to 'Getting started', 'Documentation', 'API reference', 'Forums', and 'Service health'. At the bottom, there are links for 'Feedback', 'English (US)', and copyright information: '© 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.' followed by 'Privacy Policy' and 'Terms of Use'.

Type “Topic Name” Linux_SNS

Type “Display Name” Linux_SNS

Create new topic

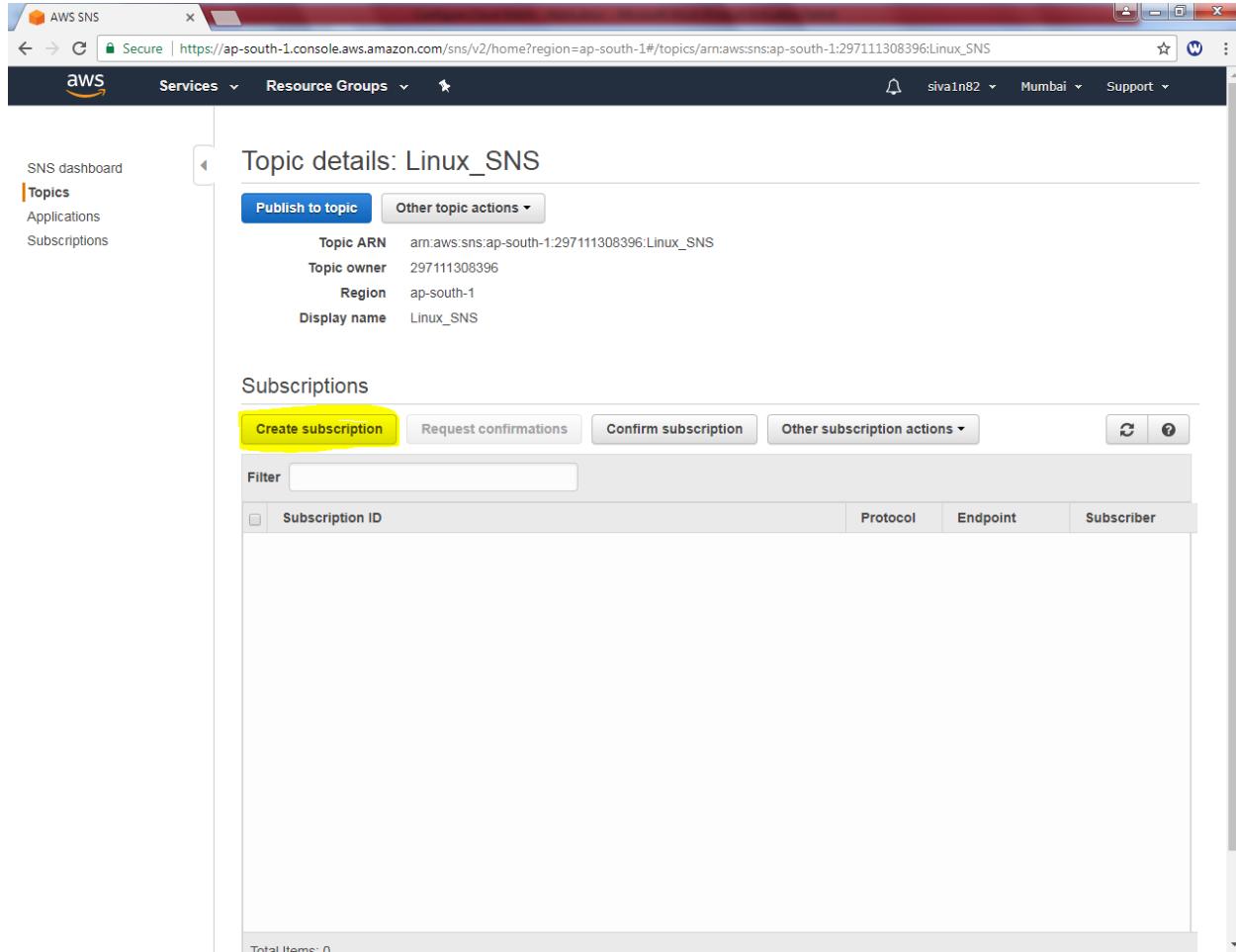
A topic name will be used to create a permanent unique identifier called an Amazon Resource Name (ARN).

Topic name	Linux_SNS	i
Display name	Linux_SNS	i

Cancel Create topic

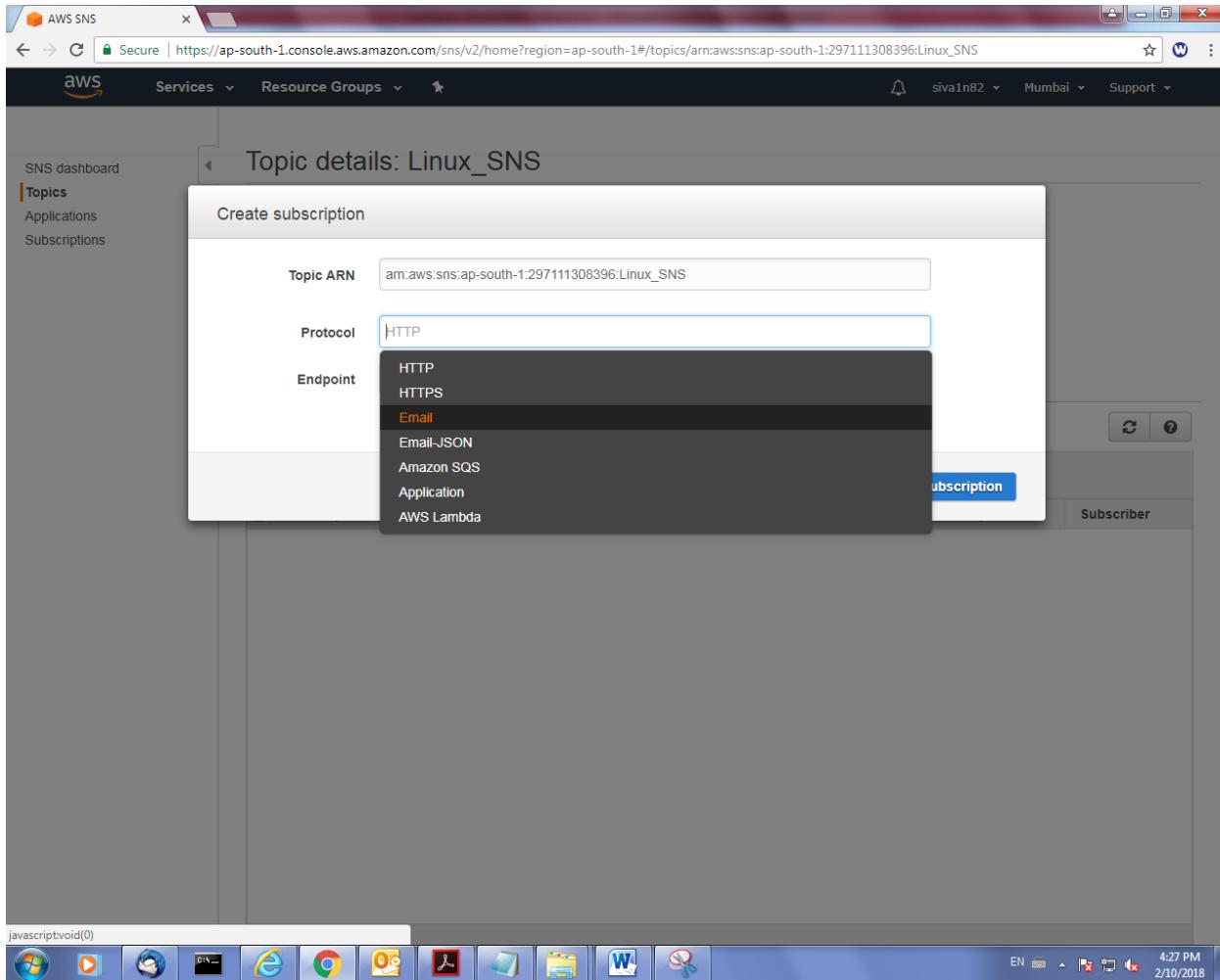
Click “Create topic”.

Click “Create subscription”.

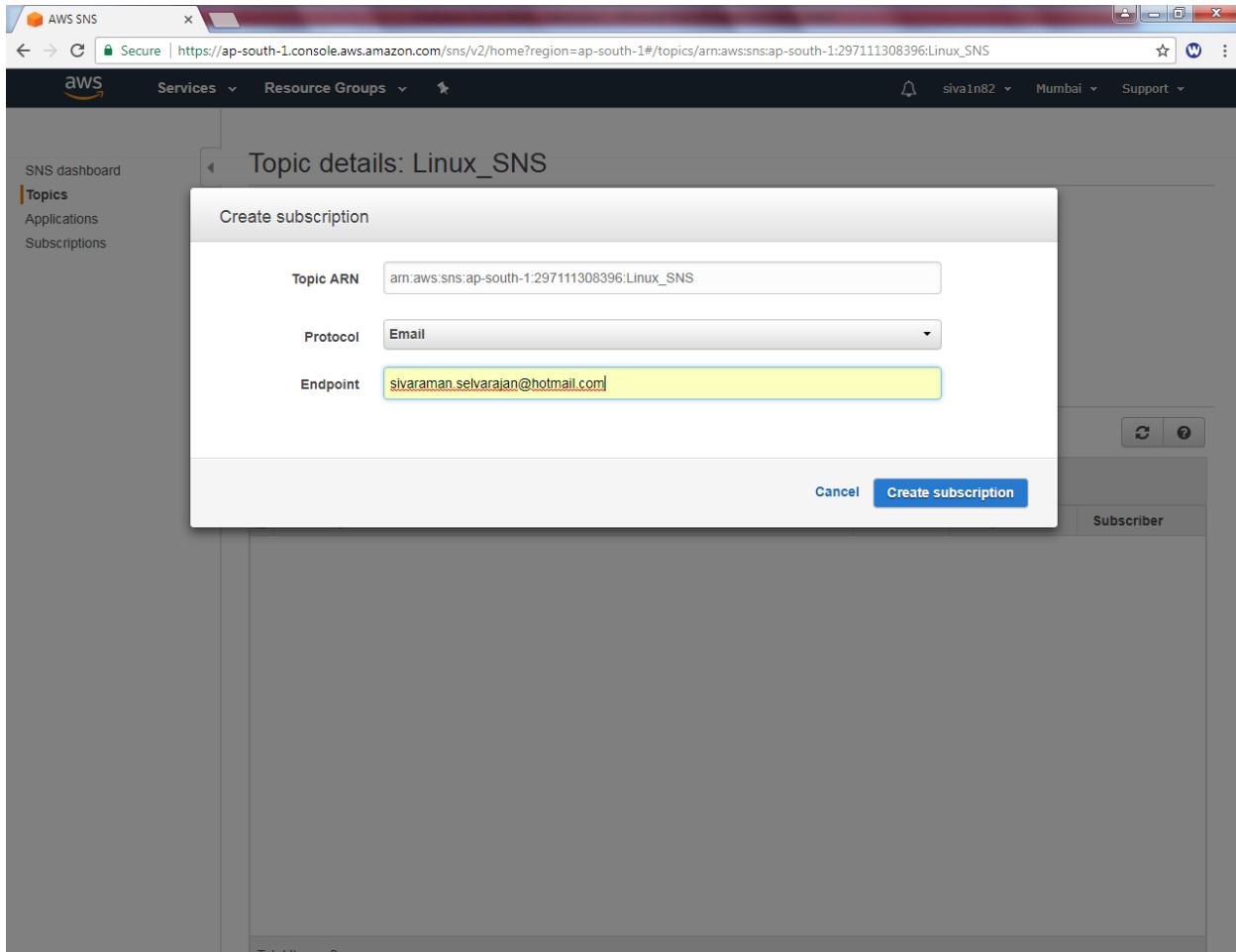


The screenshot shows the AWS SNS Topic details page for a topic named "Linux_SNS". The top navigation bar includes links for "Services", "Resource Groups", and "Support". On the left, there's a sidebar with "Topics" selected, along with links for "Applications" and "Subscriptions". The main content area displays "Topic details: Linux_SNS" with fields for "Topic ARN" (arn:aws:sns:ap-south-1:297111308396:Linux_SNS), "Topic owner" (297111308396), "Region" (ap-south-1), and "Display name" (Linux_SNS). Below this is a "Subscriptions" section with a table header containing columns for "Subscription ID", "Protocol", "Endpoint", and "Subscriber". At the top of this section, there are four buttons: "Create subscription" (highlighted with a yellow box), "Request confirmations", "Confirm subscription", and "Other subscription actions". A "Filter" input field is also present above the table.

In Protocol, select “Email”.



Type your name email id in endpoint.



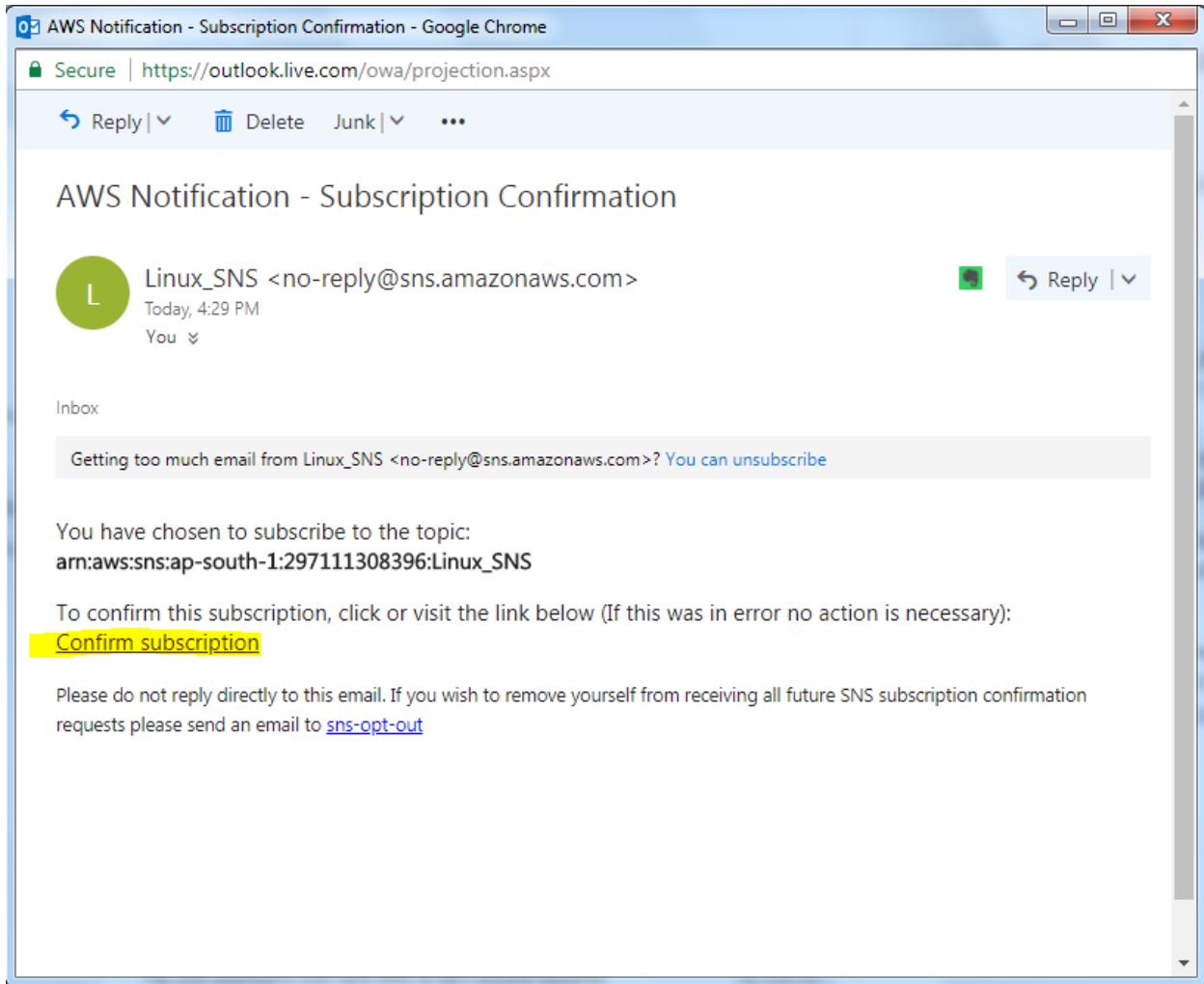
Click “Create subscription”.

Now it's in pending confirmation, we need to confirm. Go to your email id entered in endpoint.

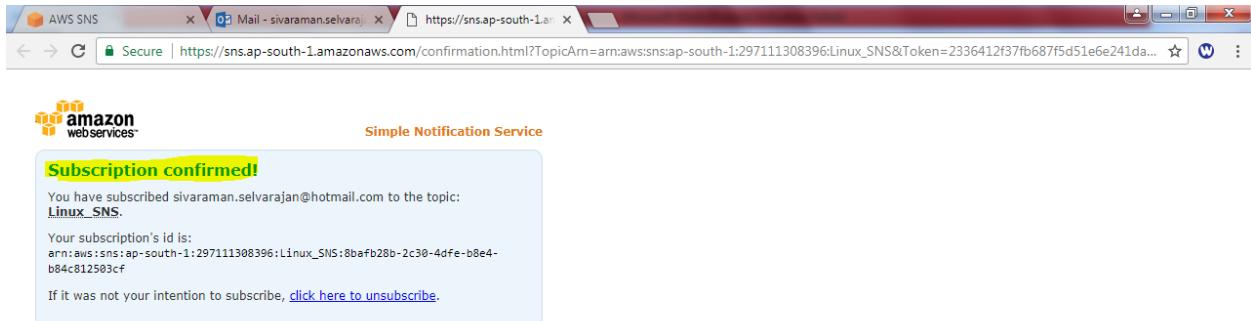
The screenshot shows the AWS SNS Topic details page for a topic named "Linux_SNS". The topic ARN is "arn:aws:sns:ap-south-1:297111308396:Linux_SNS". The topic owner is "297111308396" and the region is "ap-south-1". The display name is "Linux_SNS". In the "Subscriptions" section, there is one entry: "PendingConfirmation" with "Protocol" set to "email" and "Endpoint" set to "sivaraman.selv...".

Subscription ID	Protocol	Endpoint	Subscriber
PendingConfirmation	email	sivaraman.selv...	

Login to email id and Click “Confirm subscription”.



Your subscription has been confirmed.



Click “refresh”.

The screenshot shows the AWS SNS Topic details page for a topic named "Linux_SNS". The top navigation bar includes links for "Services", "Resource Groups", and "Support". The left sidebar has links for "SNS dashboard", "Topics" (which is selected), "Applications", and "Subscriptions". The main content area displays the topic's ARN, owner, region, and display name. Below this is a "Subscriptions" section with a table showing one email subscription.

Subscription ID	Protocol	Endpoint	Subscriber
arn:aws:sns:ap-south-1:297111308396:Linux_SNS:8bafb28b-2c30-4dfe-b8e4-b84c812503cf	email	sivaraman.selv...	297111308396

Go to EC2 instance (Linux)

The screenshot shows the AWS EC2 Management Console interface. The left sidebar navigation includes: EC2 Dashboard, Events, Tags, Reports, Limits, INSTANCES (selected), Instances, Launch Templates, Spot Requests, Reserved Instances, Dedicated Hosts, IMAGES (AMIs, Bundle Tasks), ELASTIC BLOCK STORE (Volumes, Snapshots), NETWORK & SECURITY (Security Groups, Elastic IPs, Placement Groups, Key Pairs, Network Interfaces), LOAD BALANCING (Load Balancers, Target Groups), and AUTO SCALING (Launch Configurations). The main content area displays a table of instances. A single instance is selected: "Linux Server" (i-0b597ed1a7f39d0ad, t2.micro, ap-south-1b, running). Below the table, a detailed view for this instance is shown, including its Public IP (35.154.218.5) and various network and security details.

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS
Linux Server	i-0b597ed1a7f39d0ad	t2.micro	ap-south-1b	running	2/2 checks ...	None	-

Instance: i-0b597ed1a7f39d0ad (Linux Server) Public IP: 35.154.218.5

Description		Status Checks	Monitoring	Tags
Instance ID	i-0b597ed1a7f39d0ad	Public DNS (IPv4)	-	
Instance state	running	IPv4 Public IP	35.154.218.5	
Instance type	t2.micro	IPv6 IPs	-	
Elastic IPs		Private DNS	ip-10-0-2-110.ap-south-1.compute.internal	
Availability zone	ap-south-1b	Private IPs	10.0.2.110	
Security groups	Linux-Sec-Group, view inbound rules	Secondary private IPs		

In Monitoring tab, Click “Create Alarm”.

The screenshot shows the AWS EC2 Management Console interface. On the left, there's a navigation sidebar with various service links like EC2 Dashboard, Events, Tags, Reports, Limits, Instances, Images, Elastic Block Store, Network & Security, Load Balancing, and Auto Scaling. The 'Instances' link is currently selected. The main content area displays a table of instances, with one row selected for a 'Linux Server' (instance ID: i-0b597ed1a7f39d0ad). Below the table, the 'Monitoring' tab is active, showing CloudWatch metrics for the selected instance. The 'CloudWatch alarms' section indicates 'No alarms configured' and has a 'Create Alarm' button highlighted with a yellow box. The 'CloudWatch metrics' section shows detailed monitoring for CPU Utilization, Disk Reads, Disk Read Operations, Disk Writes, Disk Write Operations, Network In, and Network Out over the last hour. The CPU Utilization chart shows a significant dip from approximately 0.201% at 10:30 to 0.051% at 11:00. The Network In chart shows a peak around 11:00.

Click "Create Alarm"

Create Alarm

You can use CloudWatch alarms to be notified automatically whenever metric data reaches a level you define.

To edit an alarm, first choose whom to notify and then define when the notification should be sent.

Send a notification to: Linux_SNS (sivaraman.selvarajan@hotm ▾ [create topic](#)

Take the action: Recover this instance ⓘ
 Stop this instance ⓘ
 Terminate this instance ⓘ
 Reboot this instance ⓘ

AWS will create the following IAM role in your account so that AWS can perform this action. [Learn more.](#)

Create IAM role: **EC2ActionsAccess** ([show IAM policy document](#))

Whenever: **Minimum** of **CPU Utilization**
Is: **<= 10** Percent

For at least: **1** consecutive period(s) of **1 Minute**

CPU Utilization Percent

Create Alarm

Please see the requirements as below.

Create Alarm

You can use CloudWatch alarms to be notified automatically whenever metric data reaches a level you define.

To edit an alarm, first choose whom to notify and then define when the notification should be sent.

Send a notification to: [create topic](#)

Take the action: Recover this instance [i](#)
 Stop this instance [i](#)
 Terminate this instance [i](#)
 Reboot this instance [i](#)

Whenever: of

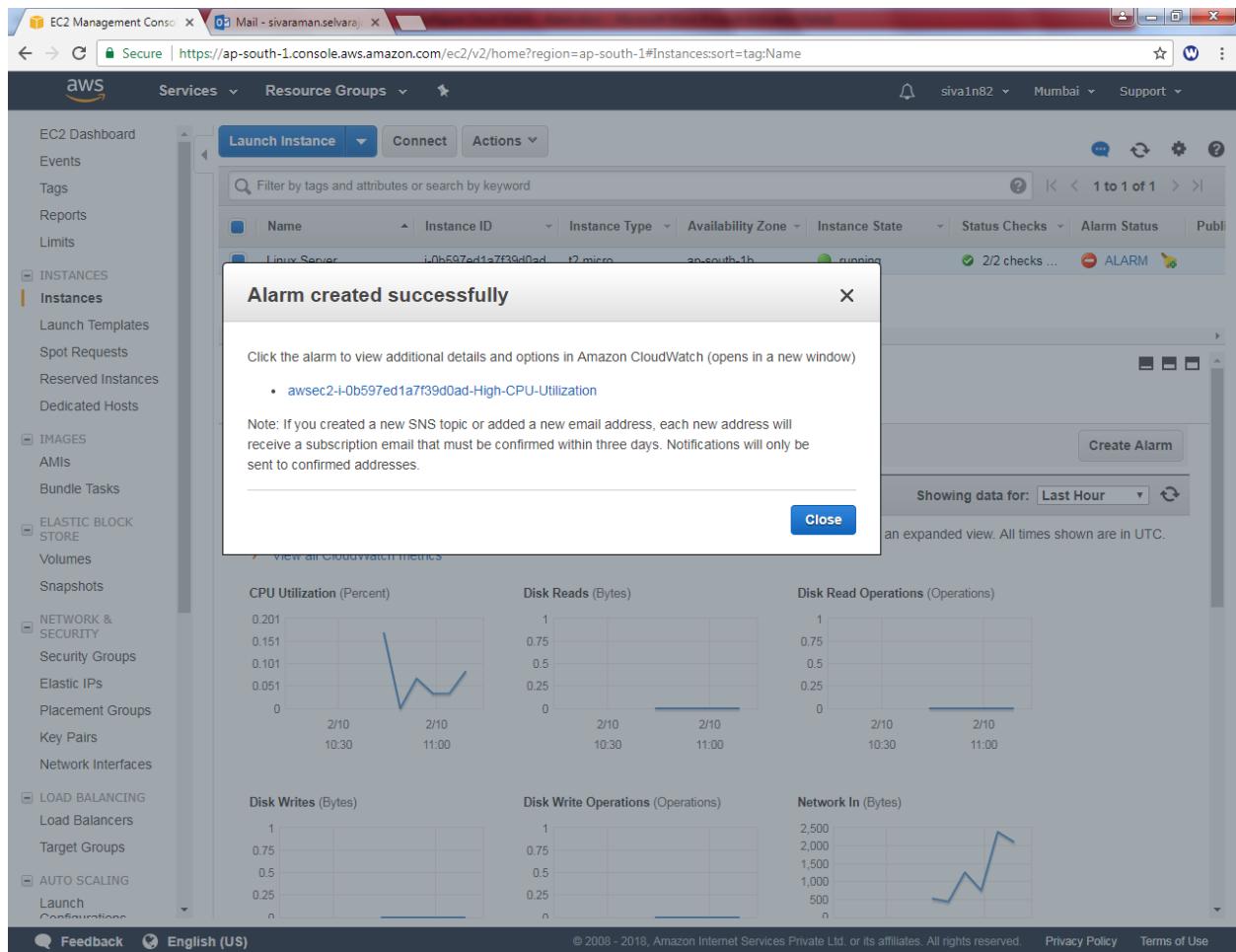
Is: Percent

For at least: consecutive period(s) of

Name of alarm:

CPU Utilization Percent

Cancel **Create Alarm**



Click “Refresh”.

You can able to see that instance is getting stop.

The screenshot shows the AWS EC2 Management Console interface. On the left, a sidebar lists various services: EC2 Dashboard, Events, Tags, Reports, Limits, Instances (selected), Launch Templates, Spot Requests, Reserved Instances, Dedicated Hosts, Images (AMIs), Bundle Tasks, Elastic Block Store (Volumes, Snapshots), Network & Security (Security Groups, Elastic IPs, Placement Groups, Key Pairs, Network Interfaces), Load Balancing (Load Balancers, Target Groups), and Auto Scaling (Launch Configurations). The main content area displays the monitoring details for an instance named "Linux Server" (i-0b597ed1a7f39d0ad). The instance is listed as "stopping". A CloudWatch alarm is triggered, indicated by a red "ALARM" status. Below the instance details, there are five line graphs showing CloudWatch metrics over the last hour:

- CPU Utilization (Percent): Values range from 0 to 0.201, with a sharp dip around 10:30.
- Disk Reads (Bytes): Values range from 0 to 1, with a small peak at 10:30.
- Disk Read Operations (Operations): Values range from 0 to 1, with a small peak at 10:30.
- Disk Writes (Bytes): Values range from 0 to 1, with a small peak at 10:30.
- Disk Write Operations (Operations): Values range from 0 to 1, with a small peak at 10:30.
- Network In (Bytes): Values range from 0 to 2,500, with a steady increase starting around 10:30.

At the bottom, there are links for Feedback, English (US), and footer information: © 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved., Privacy Policy, and Terms of Use.

Now the instance is stopped.

The screenshot shows the AWS EC2 Management Console interface. The left sidebar navigation includes:

- EC2 Dashboard
- Events
- Tags
- Reports
- Limits
- INSTANCES
 - Instances** (selected)
 - Launch Templates
 - Spot Requests
 - Reserved Instances
 - Dedicated Hosts
- IMAGES
 - AMIs
 - Bundle Tasks
- ELASTIC BLOCK STORE
 - Volumes
 - Snapshots
- NETWORK & SECURITY
 - Security Groups
 - Elastic IPs
 - Placement Groups
 - Key Pairs
 - Network Interfaces
- LOAD BALANCING
 - Load Balancers
 - Target Groups
- AUTO SCALING
 - Launch Configurations

The main content area displays the following information:

- Launch Instance** button
- Actions** dropdown
- Filter by tags and attributes or search by keyword** search bar
- Instances Table**:

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public IP
Linux Server	i-0b597ed1a7f39d0ad	t2.micro	ap-south-1b	stopped	OK	ALARM	10.0.2.110
- Instance Details**:

Instance: i-0b597ed1a7f39d0ad (Linux Server) Private IP: 10.0.2.110

Description Status Checks Monitoring Tags

CloudWatch alarms: 1 of 1 in ALARM [Create Alarm](#)

CloudWatch metrics: Detailed monitoring. [Disable Detailed Monitoring](#) Showing data for: Last Hour

Below are your CloudWatch metrics for the selected resources (a maximum of 10). Click on a graph to see an expanded view. All times shown are in UTC.

[View all CloudWatch metrics](#)

Metrics displayed:
 - CPU Utilization (Percent)
 - Disk Reads (Bytes)
 - Disk Read Operations (Operations)
 - Disk Writes (Bytes)
 - Disk Write Operations (Operations)
 - Network In (Bytes)

Graphs for CPU Utilization, Disk Reads, Disk Read Operations, Disk Writes, Disk Write Operations, and Network In over the last hour.

The screenshot shows an email from "Linux_SNS <no-reply@sns.amazonaws.com>" with the subject "ALARM: "awsec2-i-0b597ed1a7f39d0ad-High-CPU-Utilization" in Asia Pacific (Mumbai) - Google Chrome". The email content details an alarm state change:

You are receiving this email because your Amazon CloudWatch Alarm "awsec2-i-0b597ed1a7f39d0ad-High-CPU-Utilization" in the Asia Pacific (Mumbai) region has entered the ALARM state, because "Threshold Crossed: 1 datapoint [0.169491525423728 (10/02/18 11:15:00)] was less than or equal to the threshold (10.0)." at "Saturday 10 February, 2018 11:17:18 UTC".

View this alarm in the AWS Management Console:
<https://console.aws.amazon.com/cloudwatch/home?region=ap-south-1#s=Alarms&alarm=awsec2-i-0b597ed1a7f39d0ad-High-CPU-Utilization>

Alarm Details:

- Name: awsec2-i-0b597ed1a7f39d0ad-High-CPU-Utilization
- Description: Created from EC2 Console
- State Change: INSUFFICIENT_DATA -> ALARM
- Reason for State Change: Threshold Crossed: 1 datapoint [0.169491525423728 (10/02/18 11:15:00)] was less than or equal to the threshold (10.0).
- Timestamp: Saturday 10 February, 2018 11:17:18 UTC
- AWS Account: 297111308396

Threshold:

- The alarm is in the ALARM state when the metric is LessThanOrEqualToThreshold 10.0 for 60 seconds.

Monitored Metric:

- MetricNamespace: AWS/EC2
- MetricName: CPUUtilization
- Dimensions: [InstanceId = i-0b597ed1a7f39d0ad]
- Period: 60 seconds
- Statistic: Minimum
- Unit: not specified

State Change Actions:

- OK:
- ALARM: [arn:aws:sns:ap-south-1:297111308396:Linux_SNS]
- INSUFFICIENT_DATA:

--
If you wish to stop receiving notifications from this topic, please click or visit the link below to unsubscribe:
https://sns.ap-south-1.amazonaws.com/unsubscribe.html?SubscriptionArn=arn:aws:sns:ap-south-1:297111308396:Linux_SNS:8bafb28b-2c30-4dfe-b8e4-b84c812503cf&Endpoint=sivaraman.selvarajan@hotmail.com

Please do not reply directly to this email. If you have any questions or comments regarding this email, please contact us at <https://aws.amazon.com/support>

You have successfully configured and tested Cloudwatch.

We need to delete the alarm.

Type SNS in aws console.

The screenshot shows the AWS SNS service page. At the top, there is a search bar with the text "sns". Below the search bar, a list of services is displayed, grouped into categories. The services listed include:

- Simple Notification Service** (highlighted in blue)
- EC2**
- CloudWatch**
- S3**
- Billing**
- Storage**: S3, EFS, Glacier, Storage Gateway
- Management Tools**: CloudWatch, AWS Auto Scaling, CloudFormation, CloudTrail, Config, OpsWorks, Service Catalog, Systems Manager, Trusted Advisor, Managed Services
- Database**: Relational Database Service, DynamoDB, ElastiCache, Amazon Redshift
- Migration**: AWS Migration Hub, Application Discovery Service, Database Migration Service, Server Migration Service, Snowball
- Media Services**: Elastic Transcoder, Kinesis Video Streams, MediaConvert, MediaLive, MediaPackage, MediaStore
- Analytics**: Athena, EMR, CloudSearch, Elasticsearch Service, Kinesis, QuickSight
- Customer Engagement**: Amazon Connect, Pinpoint, Simple Email Service
- Business Productivity**: Alexa for Business, Amazon Chime, WorkDocs, WorkMail
- Security, Identity & Compliance**: IAM, Cognito, GuardDuty, Inspector, Amazon Macie
- Desktop & App Streaming**: WorkSpaces, AppStream 2.0

At the bottom of the page, there are links for Feedback, English (US), Copyright notice (© 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.), Privacy Policy, and Terms of Use.

Click "Simple notification service".

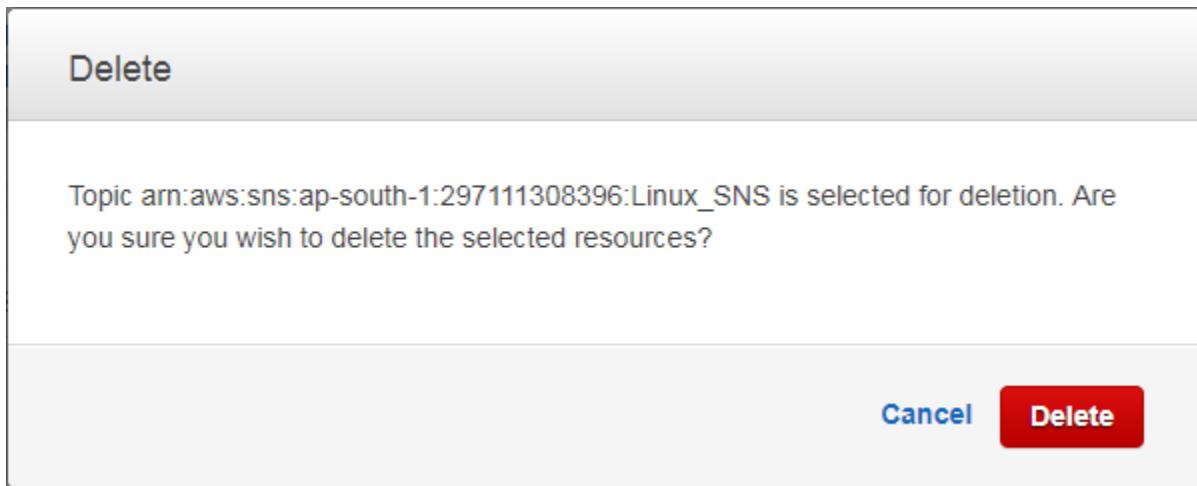
Click Topics and then "Linux_SNS"

The screenshot shows the AWS SNS Topics page. At the top, there's a navigation bar with links for 'Services', 'Resource Groups', and user information ('sivaIn82', 'Mumbai', 'Support'). Below the navigation is a search bar and a 'Topics' link. The main content area is titled 'Topics' and contains a table with one row. The table has columns for 'Name' and 'ARN'. The single entry is 'Linux_SNS' with ARN 'arn:aws:sns:ap-south-1:297111308396:Linux_SNS'. At the bottom of the table, it says 'Total Items: 1' and 'Selected Items: 1'. The footer of the page includes links for 'Feedback', 'English (US)', and copyright information: '© 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.' followed by 'Privacy Policy' and 'Terms of Use'.

Actions → Delete topics

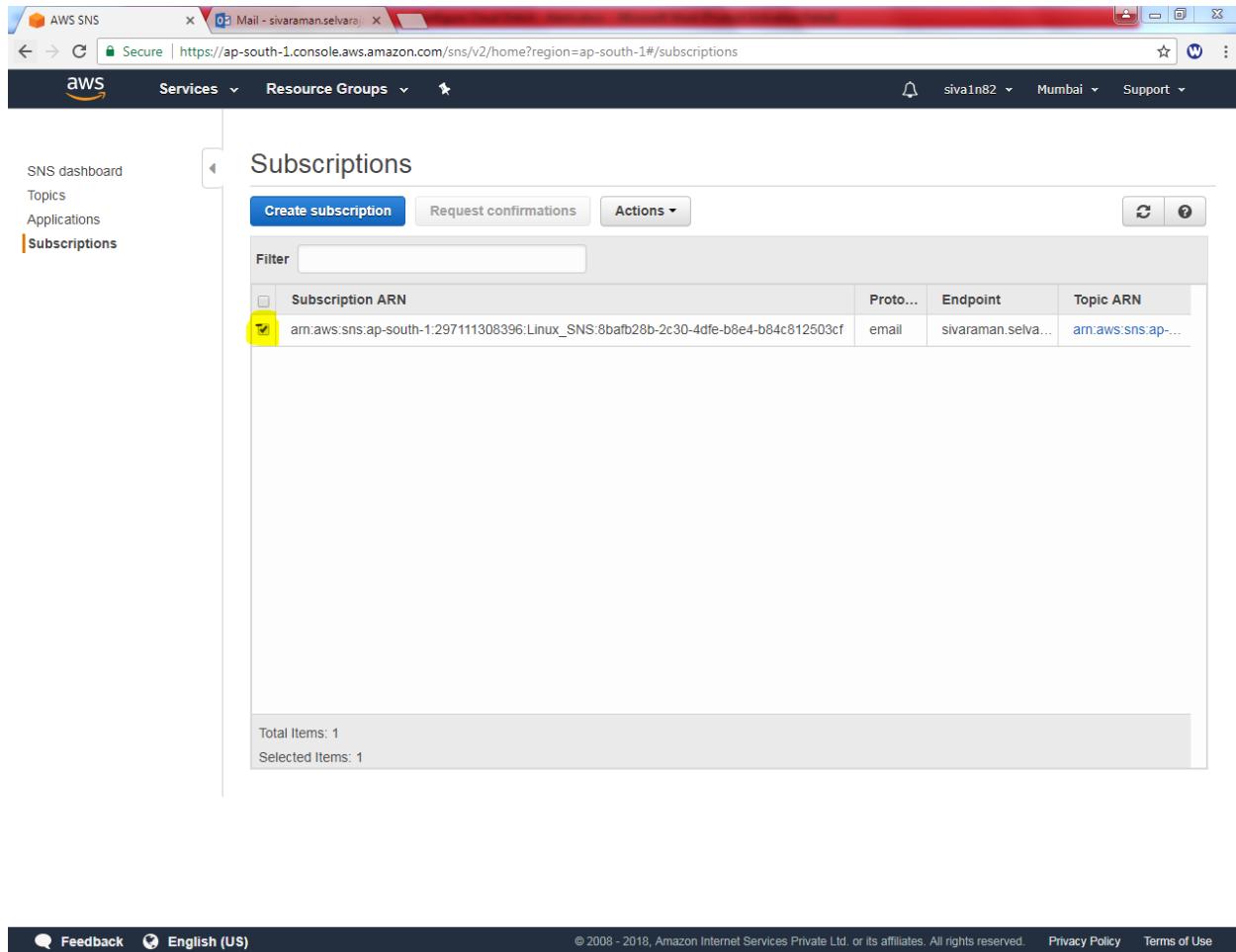
The screenshot shows the AWS SNS Topics page. On the left, there's a navigation sidebar with links for 'Topics' (which is selected and highlighted in orange), 'Applications', and 'Subscriptions'. The main area is titled 'Topics' and contains a table with one row. The table has columns for 'Name' and 'ARN'. The single entry is 'Linux_SNS' with ARN 'arn:aws:sns:ap-south-1:123456789012:Linux_SNS'. Below the table, there's a 'Actions' dropdown menu with options: 'Edit topic display name', 'Subscribe to topic', 'Confirm a subscription', 'Edit topic policy', 'Edit topic delivery policy', 'Delivery status', and 'Delete topics'. The 'Delete topics' option is highlighted with a yellow background. At the bottom of the page, there are footer links for 'Feedback', 'English (US)', and copyright information: '© 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.' followed by 'Privacy Policy' and 'Terms of Use'.

Click "Delete".



Click “Subscriptions”

Click “Checkbox”



The screenshot shows the AWS SNS Subscriptions page. The URL is https://ap-south-1.console.aws.amazon.com/sns/v2/home?region=ap-south-1#/subscriptions. The page title is "Subscriptions". On the left, there's a sidebar with links: SNS dashboard, Topics, Applications, and Subscriptions (which is selected). The main content area has a "Create subscription" button, a "Request confirmations" button, and an "Actions" dropdown. A "Filter" input field is present. A table lists one subscription:

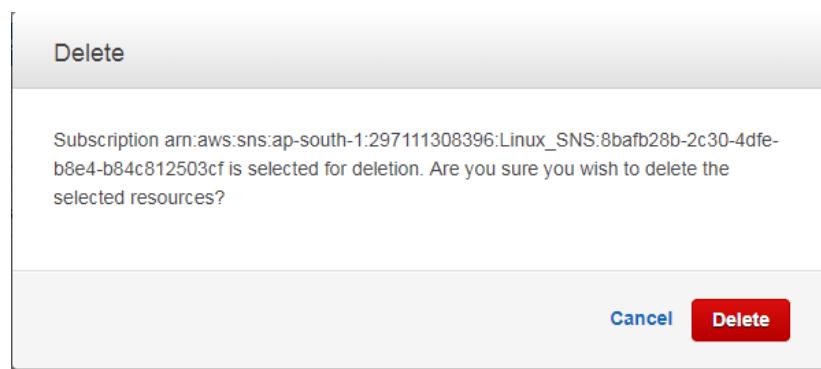
Subscription ARN	Protocol	Endpoint	Topic ARN
arn:aws:sns:ap-south-1:297111308396:Linux_SNS:8bafb28b-2c30-4dfe-b8e4-b84c812503cf	email	sivaraman.selva...	arn:aws:sns:ap...

At the bottom, it says "Total Items: 1" and "Selected Items: 1".

Click Actions → “Delete subscription”

The screenshot shows the AWS SNS Subscriptions page. On the left, there's a navigation sidebar with links like SNS dashboard, Topics, Applications, and Subscriptions (which is currently selected). The main area is titled "Subscriptions". It has tabs for "Create subscription", "Request confirmations", and "Actions". A context menu is open over a selected row, with options: "Edit subscription filter policy", "Edit subscription delivery policy", "Edit subscription attributes", and "Delete subscriptions". The "Delete subscriptions" option is highlighted in orange. Below the table, it says "Total Items: 1" and "Selected Items: 1". At the bottom of the page, there are links for Feedback, English (US), Privacy Policy, and Terms of Use.

Click “Delete”.



Click “Cloudwatch”

The screenshot shows the AWS Services Catalog interface. On the left, there's a sidebar with a 'History' section containing links like Simple Notification Service, CloudWatch, EC2, Console Home, S3, and Billing. The main area is divided into several sections: Storage (S3, EFS, Glacier, Storage Gateway), Database (Relational Database Service, DynamoDB, ElastiCache, Amazon Redshift), Migration (AWS Migration Hub, Application Discovery Service, Database Migration Service, Server Migration Service, Snowball), Networking & Content Delivery (VPC, CloudFront, Route 53, API Gateway, Direct Connect), Management Tools (CloudWatch, AWS Auto Scaling, CloudFormation, CloudTrail, Config, OpsWorks, Service Catalog, Systems Manager, Trusted Advisor, Managed Services), Analytics (Athena, EMR, CloudSearch, Elasticsearch Service, Kinesis, QuickSight, Data Pipeline, AWS Glue), Customer Engagement (Amazon Connect, Pinpoint, Simple Email Service), Business Productivity (Alexa for Business, Amazon Chime, WorkDocs, WorkMail), Security, Identity & Compliance (IAM, Cognito, GuardDuty, Inspector, Amazon Macie, AWS Single Sign-On, Certificate Manager, CloudHSM, Directory Service, WAF & Shield, Artifact), Desktop & App Streaming (WorkSpaces, AppStream 2.0), Internet Of Things (AWS IoT, IoT Analytics, IoT Device Management, Amazon FreeRTOS, AWS Greengrass), Mobile Services, and Game Development. A search bar at the top says 'Find a service by name or feature (for example, EC2, S3 or VM, storage)'. At the bottom, there are links for Feedback, English (US), Copyright notice (© 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.), Privacy Policy, and Terms of Use.

Click "INSUFFICIENT" then click checkbox

The screenshot shows the AWS CloudWatch Metrics & Alarms console. The left sidebar has 'Alarms' selected, showing 1 INSUFFICIENT alarm. The main pane displays a table of alarms with one row highlighted:

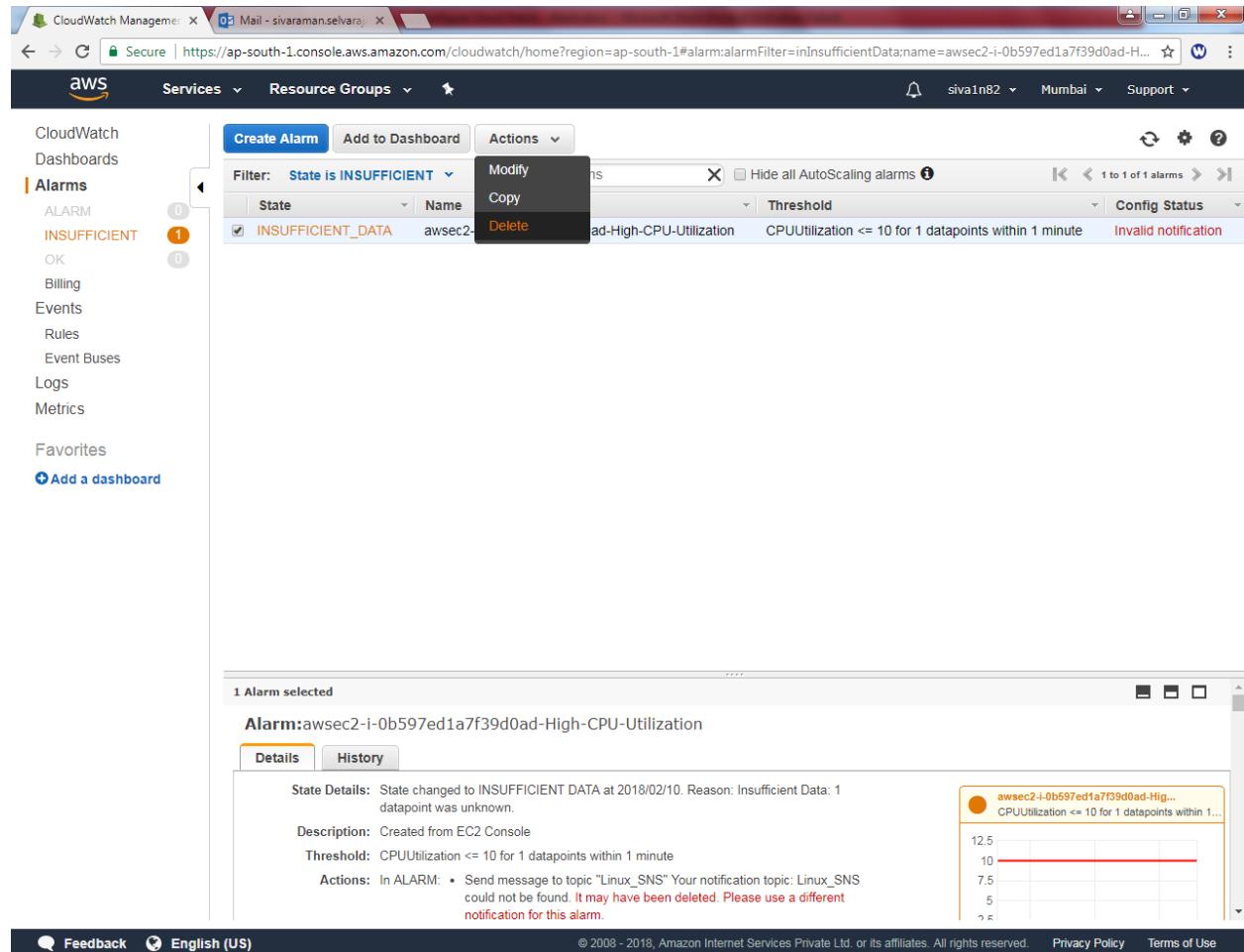
State	Name	Threshold	Config	Status
INSUFFICIENT	awsec2-i-0b597ed1a7f39d0ad-High-CPU-Utilization	CPUUtilization <= 10 for 1 datapoints within 1 minute		Invalid notification

A modal window titled '1 Alarm selected' is open for the 'awsec2-i-0b597ed1a7f39d0ad-High-CPU-Utilization' alarm. It contains the following details:

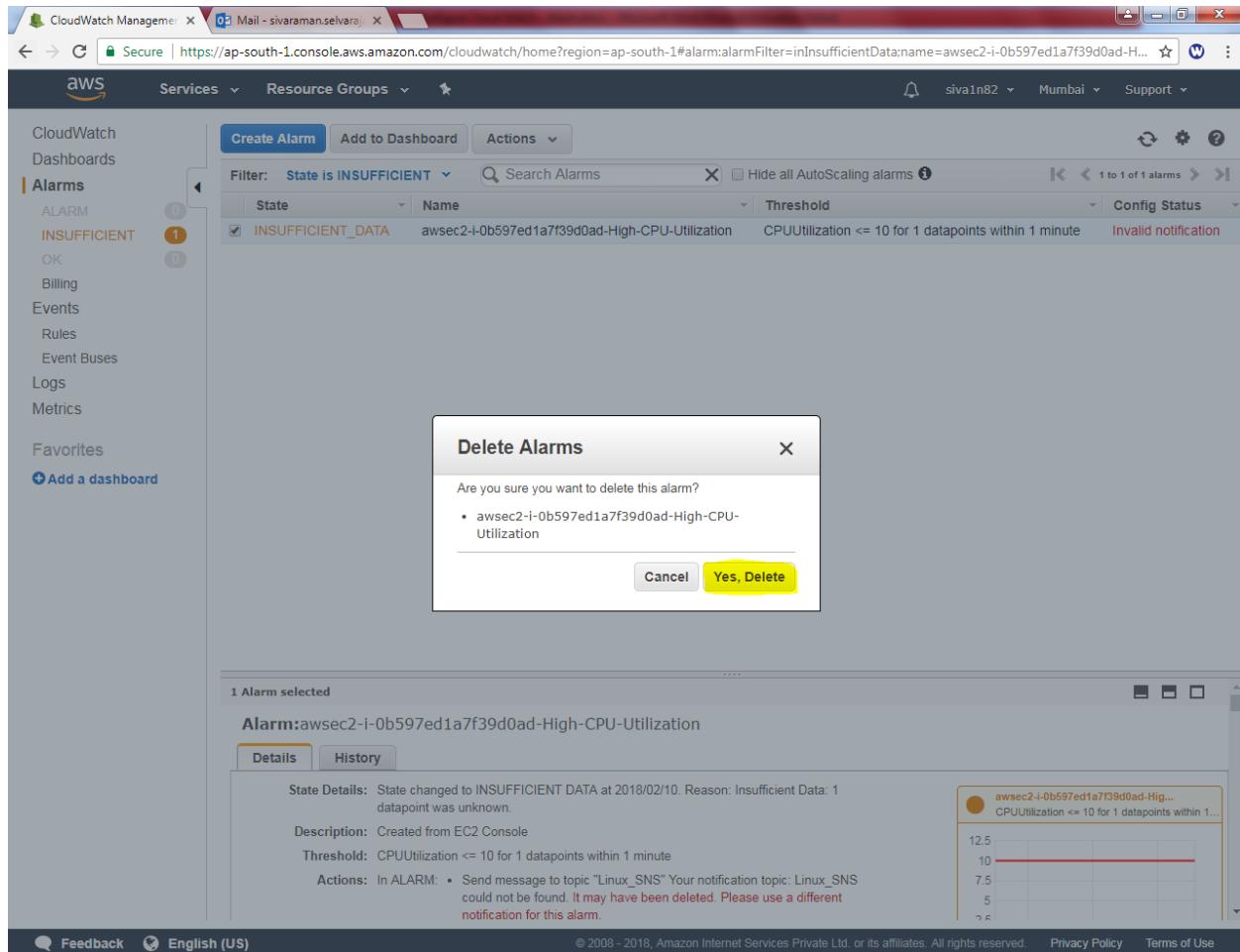
- State Details:** State changed to INSUFFICIENT DATA at 2018/02/10. Reason: Insufficient Data: 1 datapoint was unknown.
- Description:** Created from EC2 Console
- Threshold:** CPUUtilization <= 10 for 1 datapoints within 1 minute
- Actions:** In ALARM:
 - Action action/actions/AWS_EC2.InstanceId.Stop/1.0 (i-0b597ed1a7f39d0ad)
 - Send message to topic "Linux_SNS" Your notification topic: Linux_SNS

On the right side of the modal, there is a line chart titled 'awsec2-i-0b597ed1a7f39d0ad-High-CPU-Utilization' showing CPUUtilization over time. The Y-axis ranges from 5 to 12.5. A red horizontal line is drawn at the 10 mark, indicating the threshold level.

Click “Actions” → Delete



Click "Yes, Delete"



You have no cloudwatch.

The screenshot shows the AWS CloudWatch Management Console interface. The top navigation bar includes the AWS logo, a search bar, and links for Services, Resource Groups, Notifications (bell icon), User (siva1n82), Region (Mumbai), and Support. The main left sidebar has a 'CloudWatch' heading and a 'Dashboards' section which is currently selected, indicated by a blue border. Under 'Dashboards', there are links for Alarms (0), Events (0), Metrics (0), Logs (0), Rules (0), Event Buses (0), and Favorites. A sub-section 'Add a dashboard' is also present. The central content area is titled 'Dashboards' and features a 'Create dashboard' button. Below it is a table with columns 'Name', 'Favorite', and 'Last updated (UTC)'. A message states 'You have no CloudWatch dashboards. Please [create a dashboard](#)'. On the right side, there is an 'Additional Information' section with links to 'Getting Started Guide', 'Documentation', 'Forums', and 'Report an Issue'. At the bottom of the page, there are links for 'Feedback', 'English (US)', and copyright information: '© 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.' followed by 'Privacy Policy' and 'Terms of Use'.

Click EC2 to terminate the instance.

The screenshot shows the AWS EC2 Management Console interface. The left sidebar navigation menu includes: EC2 Dashboard, Events, Tags, Reports, Limits, INSTANCES (selected), Instances, Launch Templates, Spot Requests, Reserved Instances, Dedicated Hosts, IMAGES (AMIs, Bundle Tasks), ELASTIC BLOCK STORE (Volumes, Snapshots), NETWORK & SECURITY (Security Groups, Elastic IPs, Placement Groups, Key Pairs, Network Interfaces), LOAD BALANCING (Load Balancers, Target Groups), and AUTO SCALING (Launch Configurations). The main content area displays the 'Instances' page with a table showing one instance: Name (Linux Server), Instance ID (i-0b597ed1a7f39d0ad), Instance Type (t2.micro), Availability Zone (ap-south-1b), Instance State (terminated), Status Checks (None), and Alarm Status (None). Below the table, the instance details for i-0b597ed1a7f39d0ad (Linux Server) are shown, including Public DNS (-). The 'Monitoring' tab is selected, showing CloudWatch alarms (No alarms configured) and CloudWatch metrics (Detailed monitoring, Disable Detailed Monitoring). Six line graphs are displayed: CPU Utilization (Percent), Disk Reads (Bytes), Disk Read Operations (Operations), Disk Writes (Bytes), Disk Write Operations (Operations), and Network In (Bytes). The graphs show data for the last hour. The bottom of the page includes a footer with copyright information (© 2008 - 2018, Amazon Internet Services Private Ltd. or its affiliates. All rights reserved.), privacy policy, and terms of use links.

Click “Disable detailed monitoring”

The screenshot shows the AWS EC2 Management Console interface. On the left, there's a navigation sidebar with various service links like EC2 Dashboard, Events, Tags, Reports, Limits, Instances, Images, AMIs, Bundle Tasks, Elastic Block Store, Volumes, Snapshots, Network & Security, Security Groups, Elastic IPs, Placement Groups, Key Pairs, Network Interfaces, Load Balancing, and Auto Scaling. The 'Instances' link is currently selected. The main content area displays a table of instances. One instance, named 'Linux Server' with ID i-0b597ed1a7f39d0ad, is listed as 'terminated'. Below the table, under the 'Monitoring' tab, there's a section titled 'CloudWatch metrics: Detailed monitoring. Disable Detailed Monitoring'. A yellow box highlights the 'Disable Detailed Monitoring' link. There are also tabs for 'Description', 'Status Checks', and 'Monitoring'. Below this, there are six line graphs showing CPU Utilization (Percent), Disk Reads (Bytes), Disk Read Operations (Operations), Disk Writes (Bytes), Disk Write Operations (Operations), and Network In (Bytes) over a one-hour period. The 'Network In' graph shows a significant peak around 11:15. At the bottom of the page, there are links for Feedback, English (US), and footer information including copyright notice and links to Privacy Policy and Terms of Use.