

Create an instance with an ubuntu image

The screenshot shows the AWS EC2 Management Console with the 'Launch an instance' wizard open. The 'Name and tags' section has 'Name' set to 'ubuntuser'. The 'Virtual server type (instance type)' is set to 't2.micro'. The 'Software Image (AMI)' is set to 'Canonical, Ubuntu, 22.04 LTS'. The 'Firewall (security group)' is set to 'New security group'. The 'Storage (volumes)' section is collapsed. A large orange 'Launch instance' button is visible at the bottom right. The browser address bar shows 'us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#LaunchInstances'. The AWS navigation bar includes 'Services' and a search bar.

The screenshot shows the AWS EC2 Management Console with the 'Application and OS Images (Amazon Machine Image)' search interface. A search bar at the top contains the placeholder 'Search our full catalog including 1000s of application and OS images'. Below it, a 'Quick Start' section shows icons for Amazon Linux, macOS, Ubuntu, Windows, and Red Hat. A 'Browse more AMIs' link is also present. The 'Ubuntu' icon is highlighted. The 'Software Image (AMI)' section shows 'Canonical, Ubuntu, 22.04 LTS' selected. The 'Virtual server type (instance type)' is set to 't2.micro'. The 'Firewall (security group)' is set to 'New security group'. The 'Storage (volumes)' section is collapsed. A large orange 'Launch instance' button is visible at the bottom right. The browser address bar shows 'us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#LaunchInstances'. The AWS navigation bar includes 'Services' and a search bar.

The screenshot shows the AWS EC2 Management Console interface for launching a new instance. The top navigation bar includes links for Case History, EC2 Management Console, Subnets, and VPC Management Console. The main content area is titled "Launch instances" and contains several configuration sections:

- Instance type**: Set to t2.micro, which is free tier eligible. It lists family details, On-Demand Windows pricing, On-Demand SUSE pricing, On-Demand RHEL pricing, and On-Demand Linux pricing.
- Key pair (login)**: A dropdown menu shows "new" selected, with a "Create new key pair" button.
- Summary**: Shows 1 instance, uses Canonical, Ubuntu 22.04 LTS AMI (ami-0557a15b87f6559cf), and a t2.micro instance type. It also includes a "New security group" and "Storage (volumes)" section.

At the bottom right is a large orange "Launch instance" button.

This screenshot shows the same AWS EC2 Management Console interface, but with two security group rules defined under the "Security group rule 1 (TCP, 22, 0.0.0.0/0)" and "Security group rule 2 (TCP, 80, 0.0.0.0/0)" sections. The rules allow traffic from anywhere on port 22 (SSH) and port 80 (HTTP).

The "Summary" section remains identical to the first screenshot, showing 1 instance, Canonical, Ubuntu 22.04 LTS AMI, t2.micro instance type, and a new security group.

At the bottom right is a large orange "Launch instance" button.

The screenshot shows the AWS EC2 Management Console interface. On the left, there are three tabs: 'Case History | AWS Support Console', 'EC2 Management Console' (which is active), and 'Subnets | VPC Management Con...'. The main content area displays two security group rules for a new instance:

- Security group rule 3 (TCP, 443, 0.0.0.0/0)**:
 - Type: HTTPS
 - Protocol: TCP
 - Port range: 443
 - Source type: Anywhere
 - Description: e.g. SSH for admin desktop
- Security group rule 4 (All, All, 0.0.0.0/0)**:
 - Type: All traffic
 - Protocol: All
 - Port range: All
 - Source type: Anywhere
 - Description: e.g. SSH for admin desktop

To the right, a summary panel shows the following details:

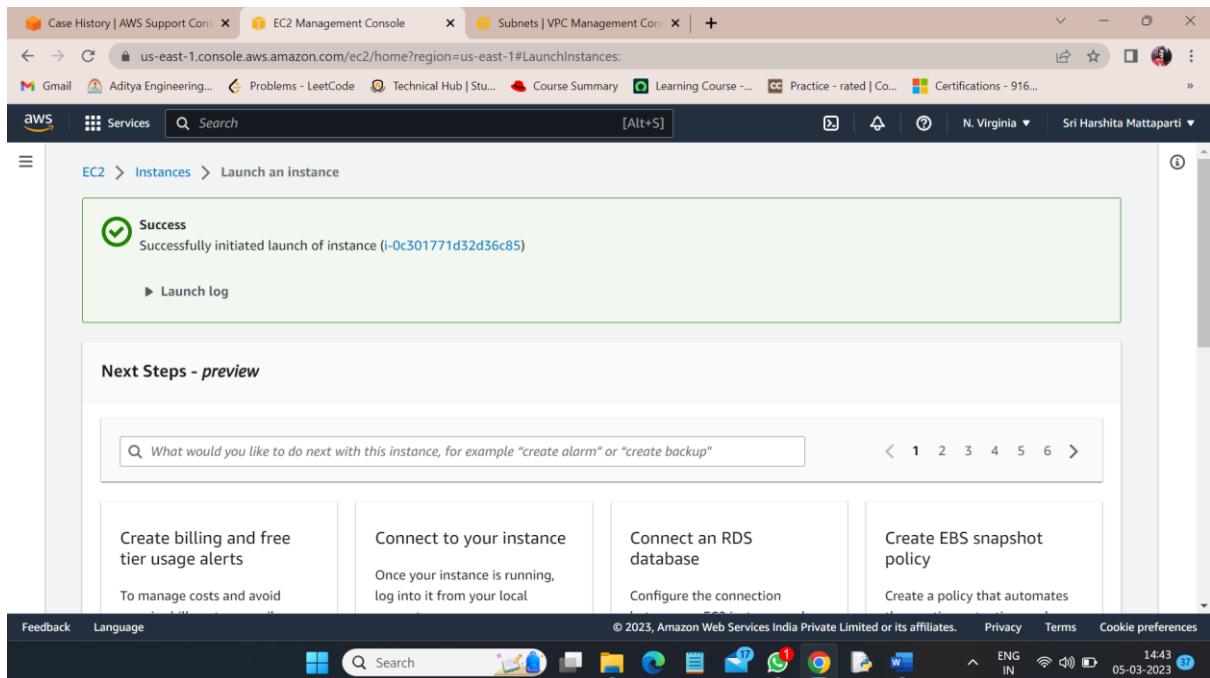
- Number of instances**: 1
- Software Image (AMI)**: Canonical, Ubuntu, 22.04 LTS, ami-0557a15b87f6559cf
- Virtual server type (instance type)**: t2.micro
- Firewall (security group)**: New security group
- Storage (volumes)**: (No volumes listed)

At the bottom right of the summary panel is a large orange button labeled "Launch instance".

This screenshot shows the continuation of the AWS EC2 Management Console setup. The left pane now includes a "Configure storage" section with the following settings:

- Root volume: 1x 8 GiB gp2 (Root volume (Not encrypted))
- A note: "Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage" (with a close button X).
- An "Add new volume" button.
- A note: "The selected AMI contains more instance store volumes than the instance allows. Only the first 0 instance store volumes from the AMI will be accessible from the instance".
- File systems: 0 x File systems (with an "Edit" link).

The right side of the screen remains identical to the previous screenshot, showing the summary panel with one instance, the specified AMI, instance type, security group, and a "Launch instance" button.



Copy and paste the ssh command

```
ubuntu@ip-172-31-63-31: ~ + 
C:\Users\HARSHITA>cd downloads

C:\Users\HARSHITA\Downloads>ssh -i "new.pem" ubuntu@ec2-54-210-195-6.compute-1.amazonaws.com
The authenticity of host 'ec2-54-210-195-6.compute-1.amazonaws.com (54.210.195.6)' can't be established.
ED25519 key fingerprint is SHA256:gBqlp0aaXfb0fNX/dY2AR/pAdZIQ8TINs9gU99iKc.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ec2-54-210-195-6.compute-1.amazonaws.com' (ED25519) to the list of known hosts.
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-1028-aws x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/advantage

 System information as of Sun Mar  5 09:17:53 UTC 2023

 System load: 0.0419921875   Processes:          101
 Usage of /: 19.8% of 7.57GB  Users logged in:    0
 Memory usage: 19%           IPv4 address for eth0: 172.31.63.31
 Swap usage:  0%

 Expanded Security Maintenance for Applications is not enabled.

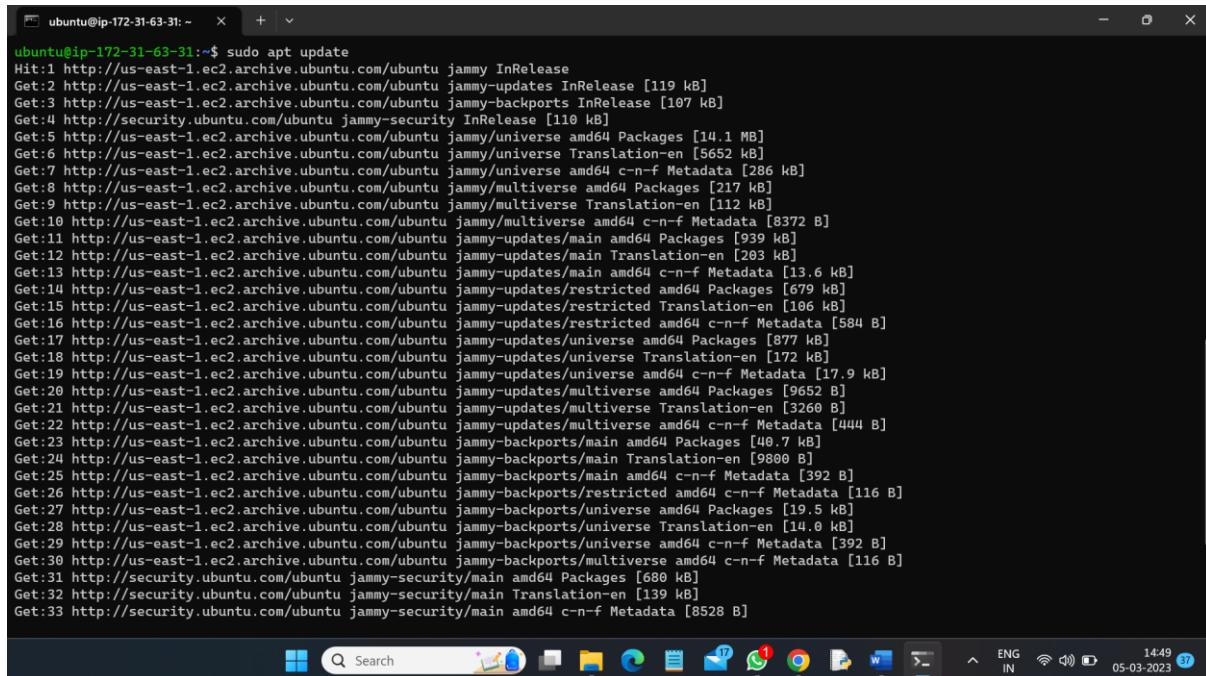
 0 updates can be applied immediately.

 Enable ESM Apps to receive additional future security updates.
 See https://ubuntu.com/esm or run: sudo pro status

 The list of available updates is more than a week old.
 To check for new updates run: sudo apt update

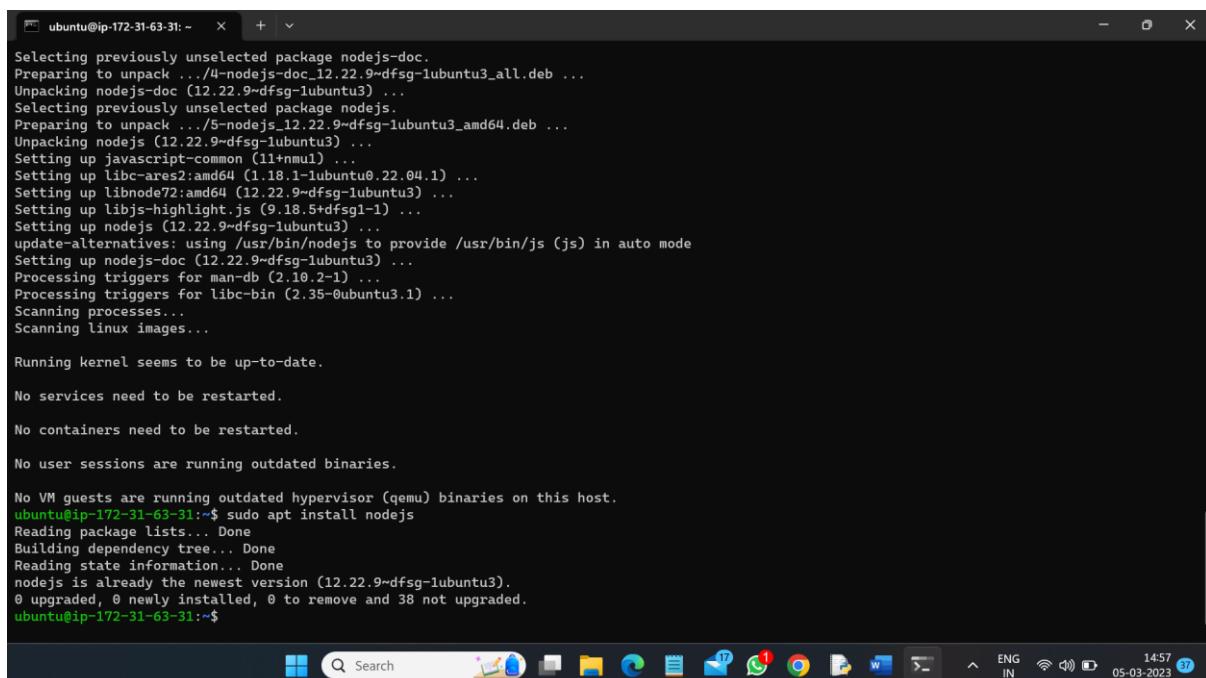

```

Give sudo apt update



```
ubuntu@ip-172-31-63-31:~$ sudo apt update
Hit:1 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy InRelease
Get:2 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates InRelease [119 kB]
Get:3 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports InRelease [107 kB]
Get:4 http://security.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
Get:5 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/universe amd64 Packages [14.1 MB]
Get:6 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/universe Translation-en [5652 kB]
Get:7 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/universe amd64 c-n-f Metadata [286 kB]
Get:8 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/multiverse amd64 Packages [217 kB]
Get:9 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/multiverse Translation-en [112 kB]
Get:10 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy/multiverse amd64 c-n-f Metadata [8372 B]
Get:11 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main amd64 Packages [939 kB]
Get:12 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main Translation-en [203 kB]
Get:13 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/main amd64 c-n-f Metadata [13.6 kB]
Get:14 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/restricted amd64 Packages [679 kB]
Get:15 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/restricted Translation-en [106 kB]
Get:16 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/restricted amd64 c-n-f Metadata [584 kB]
Get:17 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 Packages [877 kB]
Get:18 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/universe Translation-en [172 kB]
Get:19 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 c-n-f Metadata [17.9 kB]
Get:20 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/multiverse amd64 Packages [9652 B]
Get:21 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/multiverse Translation-en [3260 B]
Get:22 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-updates/multiverse amd64 c-n-f Metadata [444 B]
Get:23 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/main amd64 Packages [40.7 kB]
Get:24 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/main Translation-en [9800 B]
Get:25 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/main amd64 c-n-f Metadata [392 B]
Get:26 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/restricted amd64 c-n-f Metadata [116 B]
Get:27 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/universe amd64 Packages [19.5 kB]
Get:28 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/universe Translation-en [14.0 kB]
Get:29 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/universe amd64 c-n-f Metadata [392 B]
Get:30 http://us-east-1.ec2.archive.ubuntu.com/ubuntu jammy-backports/multiverse amd64 c-n-f Metadata [116 B]
Get:31 http://security.ubuntu.com/ubuntu jammy-security/main amd64 Packages [680 kB]
Get:32 http://security.ubuntu.com/ubuntu jammy-security/main Translation-en [139 kB]
Get:33 http://security.ubuntu.com/ubuntu jammy-security/main amd64 c-n-f Metadata [8528 B]
```

Install nodejs by giving sudo install nodejs



```
ubuntu@ip-172-31-63-31:~$ sudo apt install nodejs
Selecting previously unselected package nodejs-doc.
Preparing to unpack .../4-nodejs-doc_12.22.9~dfsg-1ubuntu3_all.deb ...
Unpacking nodejs-doc (12.22.9~dfsg-1ubuntu3) ...
Selecting previously unselected package nodejs.
Preparing to unpack .../5-nodejs_12.22.9~dfsg-1ubuntu3_amd64.deb ...
Unpacking nodejs (12.22.9~dfsg-1ubuntu3) ...
Setting up javascript-common (11+mu1) ...
Setting up libc-ares2:amd64 (1.18.1-1ubuntu0.22.04.1) ...
Setting up libnode72:amd64 (12.22.9~dfsg-1ubuntu3) ...
Setting up libjs-highlight.js (9.18.5+dfsg1-1) ...
Setting up nodejs (12.22.9~dfsg-1ubuntu3) ...
update-alternatives: using /usr/bin/nodejs to provide /usr/bin/js (js) in auto mode
Setting up nodejs-doc (12.22.9~dfsg-1ubuntu3) ...
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for libc-bin (2.35-0ubuntu3.1) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
ubuntu@ip-172-31-63-31:~$ sudo apt install nodejs
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
nodejs is already the newest version (12.22.9~dfsg-1ubuntu3).
0 upgraded, 0 newly installed, 0 to remove and 38 not upgraded.
ubuntu@ip-172-31-63-31:~$
```

Now allocate an Elastic IP address

The screenshot shows the AWS Management Console with the URL us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#Addresses. The left sidebar is collapsed, and the main content area displays the 'Elastic IP addresses' page. At the top right, there is a large orange button labeled 'Allocate Elastic IP address'. Below it, a table lists 'Allocated IPv4 addr...' and 'Type' columns. A search bar at the top says 'Filter Elastic IP addresses'. The bottom of the page includes standard AWS navigation links like Feedback, Language, and a footer with copyright information and date.

The screenshot shows the 'Allocate Elastic IP address' configuration dialog. It has several sections: 'Amazon's pool of IPv4 addresses' (radio button selected), 'Global static IP addresses' (disabled), 'Tags - optional' (disabled), and 'Add new tag' (button). At the bottom right is a large orange 'Allocate' button. The footer of the dialog includes standard AWS navigation links and a footer with copyright information and date.

Associate the Elastic IP with the Instance

The screenshot shows the AWS EC2 Management Console interface. A green success message at the top states "Elastic IP address allocated successfully. Elastic IP address 54.158.197.207". Below this, the "Elastic IP addresses (1/1)" section displays a single entry: "54.158.197.207" (Allocated IPv4 address), "Public IP" (Type), and "eipalloc-00a75583651ea0cd9" (Allocation ID). The "Summary" tab is selected. The left sidebar shows navigation options like EC2 Dashboard, Instances, and Launch Templates.

The screenshot shows the "Associate Elastic IP Address" dialog box. Under "Resource type", "Instance" is selected. A warning message states: "If you associate an Elastic IP address with an instance that already has an Elastic IP address associated, the previously associated Elastic IP address will be disassociated, but the address will still be allocated to your account." Below this, it says: "If no private IP address is specified, the Elastic IP address will be associated with the primary private IP address." In the "Instance" field, "i-0c301771d32d36c85" is selected. In the "Private IP address" field, "172.31.63.31" is entered. Under "Reassociation", there is a checkbox "Allow this Elastic IP address to be reassociated" which is unchecked. At the bottom right are "Cancel" and "Associate" buttons. The status bar at the bottom indicates the time as 14:59 and the date as 05-03-2023.

Instance has been associated

The screenshot shows the AWS EC2 Management Console interface. In the top navigation bar, there are several tabs: Case History | AWS Support, EC2 Management Console, Instances | EC2 Management, Subnets | VPC Management, and others. The main content area displays a table titled "Instances (1/1) Info". The table has columns for Name, Instance ID, Instance state, Instance type, Status check, Alarm status, and Availability Zone. One row is shown, with "ubuntuser" as the name, "i-0c301771d32d36c85" as the instance ID, "Running" as the state, "t2.micro" as the type, "2/2 checks passed" as the status, "No alarms" as the alarm status, and "us-east-1e" as the availability zone. Below the table, a detailed view for the instance "i-0c301771d32d36c85 (ubuntuser)" is expanded. It shows various details such as Answer private resource DNS name (IPv4 A), Instance type (t2.micro), Auto-assigned IP address (VPC ID: vpc-0c83813b9542f4dbc), IAM Role (Subnet ID: subnet-0a0b3bc6e73b841e5), Elastic IP addresses (54.158.197.207 [Public IP]), and AWS Compute Optimizer finding (Opt-in to AWS Compute Optimizer for recommendations). The bottom of the screen shows the Windows taskbar with various pinned icons like File Explorer, Edge, and Mail.

Now create an S3 bucket

The screenshot shows the AWS S3 bucket creation wizard. The top navigation bar includes tabs for Case History | AWS Support, EC2 Management Console, Instances | EC2 Management, S3 bucket, Subnets | VPC Management, and others. The main area is titled "Create bucket" with a "General configuration" section. It contains fields for "Bucket name" (set to "ubuntubuck") and "AWS Region" (set to "US East (Ohio) us-east-2"). Below these, there's a note about "Copy settings from existing bucket - optional" and a "Choose bucket" button. At the bottom, there's an "Object Ownership" section with a dropdown menu set to "Amazon S3 owns objects". The bottom of the screen shows the Windows taskbar with various pinned icons like File Explorer, Edge, and Mail.

The screenshot shows the AWS S3 console with the URL s3.console.aws.amazon.com/s3/bucket/create?region=us-east-2. The page displays the 'Object Ownership' section. It includes two options: 'ACLs disabled (recommended)' (selected) and 'ACLs enabled'. A note states: 'All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.' Another note indicates: 'Starting in April 2023, to disable ACLs when creating buckets by using the S3 console, you will no longer need the s3:PutBucketOwnershipControls permission. Learn more'.

Object Ownership

Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

ACLs disabled (recommended)
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

ACLs enabled
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

Object Ownership
Bucket owner enforced

Upcoming permission changes to disable ACLs
Starting in April 2023, to disable ACLs when creating buckets by using the S3 console, you will no longer need the s3:PutBucketOwnershipControls permission. [Learn more](#)

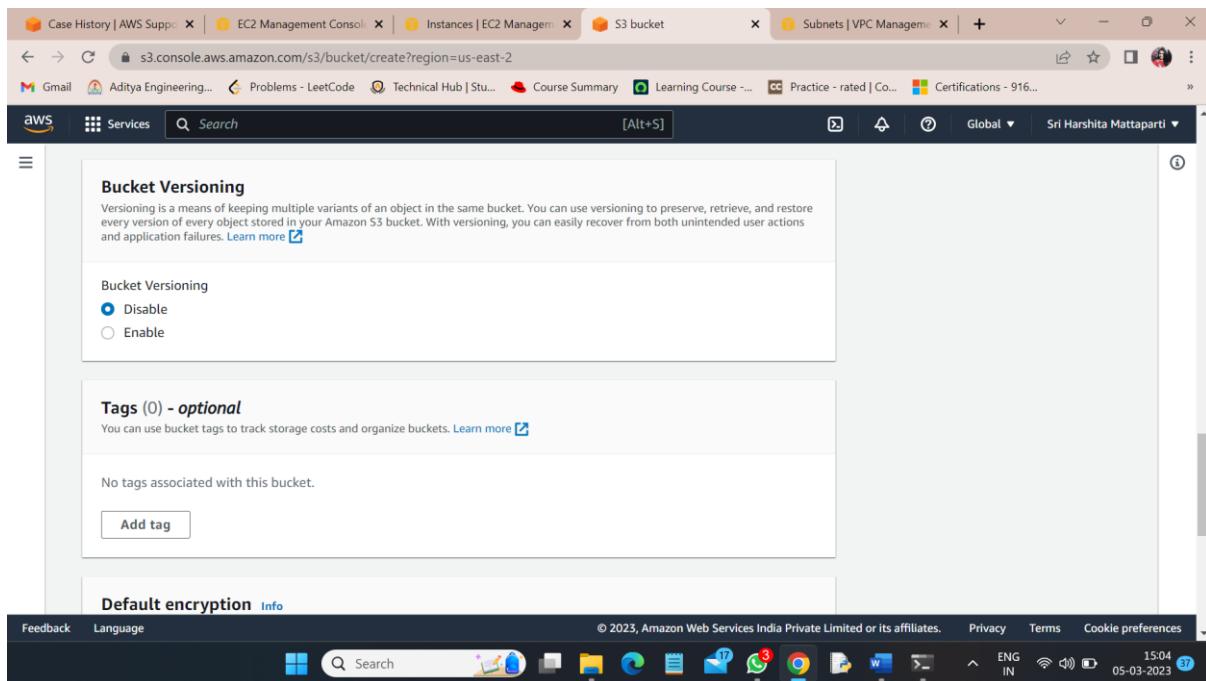
Block Public Access settings for this bucket

Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences 15:03 ENG IN 05-03-2023

The screenshot shows the AWS S3 console with the URL s3.console.aws.amazon.com/s3/bucket/create?region=us-east-2. The page displays the 'Block Public Access settings for this bucket' section. It explains that public access is granted through ACLs, bucket policies, access point policies, or all. It recommends turning on 'Block all public access' to ensure public access to the bucket is blocked. Below this, there are five checkboxes for different access control settings:

- Block all public access**
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.
- Block public access to buckets and objects granted through new access control lists (ACLs)**
S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
- Block public access to buckets and objects granted through any access control lists (ACLs)**
S3 will ignore all ACLs that grant public access to buckets and objects.
- Block public access to buckets and objects granted through new public bucket or access point policies**
S3 will block new bucket and access point policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
- Block public and cross-account access to buckets and objects through any public bucket or access point policies**
S3 will ignore public and cross-account access for buckets or access points with policies that grant public access to buckets and objects.

Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences 15:03 ENG IN 05-03-2023



Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. [Learn more](#)

Bucket Versioning

Disable
 Enable

Tags (0) - optional

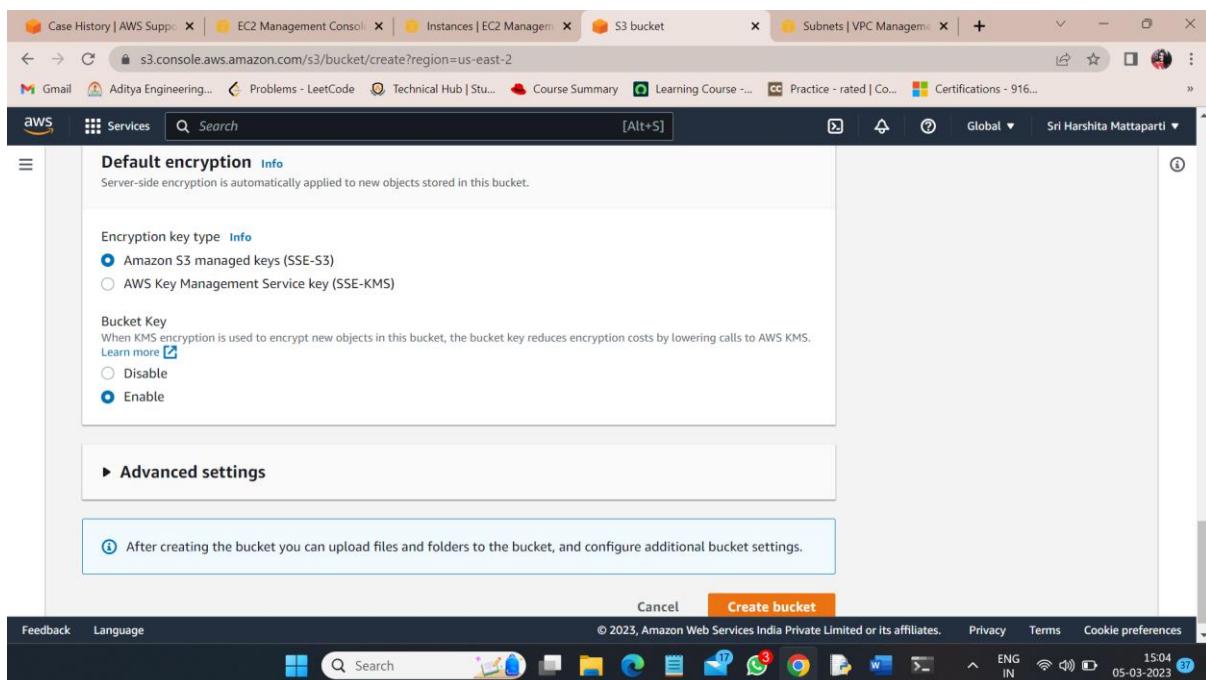
You can use bucket tags to track storage costs and organize buckets. [Learn more](#)

No tags associated with this bucket.

[Add tag](#)

Default encryption [Info](#)

Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences 15:04 IN 05-03-2023



Default encryption [Info](#)

Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption key type [Info](#)

Amazon S3 managed keys (SSE-S3)
 AWS Key Management Service key (SSE-KMS)

Bucket Key

When KMS encryption is used to encrypt new objects in this bucket, the bucket key reduces encryption costs by lowering calls to AWS KMS. [Learn more](#)

Disable
 Enable

Advanced settings

After creating the bucket you can upload files and folders to the bucket, and configure additional bucket settings.

[Cancel](#) [Create bucket](#)

Feedback Language © 2023, Amazon Web Services India Private Limited or its affiliates. Privacy Terms Cookie preferences 15:04 IN 05-03-2023

The screenshot shows the AWS S3 console with a success message: "Successfully created bucket 'ubuntu-buck'". The message also suggests uploading files and folders or configuring additional settings, with a "View details" button. On the left, a sidebar lists various S3 features like Buckets, Access Points, and Storage Lens. The main area displays an "Account snapshot" and a table of buckets, showing one named "ubuntu-buck" created on March 5, 2023.

Create an IAM Role for uploading objects

The screenshot shows the AWS IAM Management console with a banner about IAM Roles Anywhere. The "Roles" section displays two roles: "AWSServiceRoleForSupport" and "AWSServiceRoleForTrustedAdvisor", both associated with the "support" service. The left sidebar includes sections for Access management (Roles, Policies, Identity providers, Account settings), Access reports (Access analyzer, Archive rules, Analyzers, Settings), and general navigation (Feedback, Language).

Select an Entity

The screenshot shows the 'Create role' wizard in the AWS IAM console. The top banner announces the new IAM roles experience, stating 'We've redesigned the IAM roles experience to make it easier to use. Let us know what you think.' The main section is titled 'Select trusted entity' with an 'Info' link. It displays a 'Trusted entity type' section containing five options: 'AWS service' (selected), 'AWS account', 'Web identity', 'SAML 2.0 federation', and 'Custom trust policy'. Below this is a 'Use case' section with the note 'Allow an AWS service like EC2, Lambda, or others to perform actions in this account.' A 'Feedback' button is visible at the bottom left.

This screenshot shows the same 'Create role' wizard, but with the original interface. The 'Trusted entity type' section includes 'AWS service' (selected), 'AWS account', 'Web identity', 'SAML 2.0 federation', and 'Custom trust policy'. The 'Use case' section is identical. The 'Common use cases' section below lists 'EC2' (selected) and 'Lambda'. A dropdown menu for 'Use cases for other AWS services' is open, showing the placeholder 'Choose a service to view use case'. A 'Next' button is located at the bottom right.

Select the Policy

The screenshot shows the AWS IAM Management console with the URL us-east-1.console.aws.amazon.com/iamv2/home?region=us-east-1#/roles/create?commonUseCase=EC2&step=addPermission&trustedEntityType=.... The page is titled "Permissions policies (Selected 1/817) Info". It displays a list of policies filtered by "s3". One policy, "AmazonS3FullAccess", is selected and highlighted with a blue border. Other policies listed include "AmazonDMSRedshi...", "QuickSightAccessF...", "AmazonS3ReadOnl...", "AmazonS3Outposts...", "AWSBackupService...", "AWSBackupService...", "AmazonS3ObjectLa...", and "AmazonS3Outposts...". The interface includes a search bar, a filter button, and a "Create policy" button.

Give a name to the role

The screenshot shows the AWS IAM Management console with the URL us-east-1.console.aws.amazon.com/iamv2/home?region=us-east-1#/roles/create?commonUseCase=EC2&policies=arn%3aaws%3aiam%3A%3aws.... The page is titled "Name, review, and create". It shows "Role details" with a "Role name" field containing "ubuntu" and a "Description" field containing "Allows EC2 instances to call AWS services on your behalf.". Below this, a code editor window displays the JSON policy document:

```
1  {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
```

Screenshot of the AWS IAM Roles page showing a newly created role named "ubuntu".

The page displays a table of roles:

Role name	Trusted entities	Last activity
AWSServiceRoleForSupport	AWS Service: support (Service-Linked Role)	6 hours ago
AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service-Linked Role)	-
ubuntu	AWS Service: ec2	-

Below the table, there is a "Roles Anywhere" section with a "Manage" button.

Screenshot of the AWS IAM Role details page for the "ubuntu" role.

The "Summary" tab is selected, showing:

- Creation date: March 05, 2023, 15:12 (UTC+05:30)
- ARN: arn:aws:iam::631414935263:role/ubuntu
- Last activity: None
- Maximum session duration: 1 hour

The "Permissions" tab is selected, showing one managed policy:

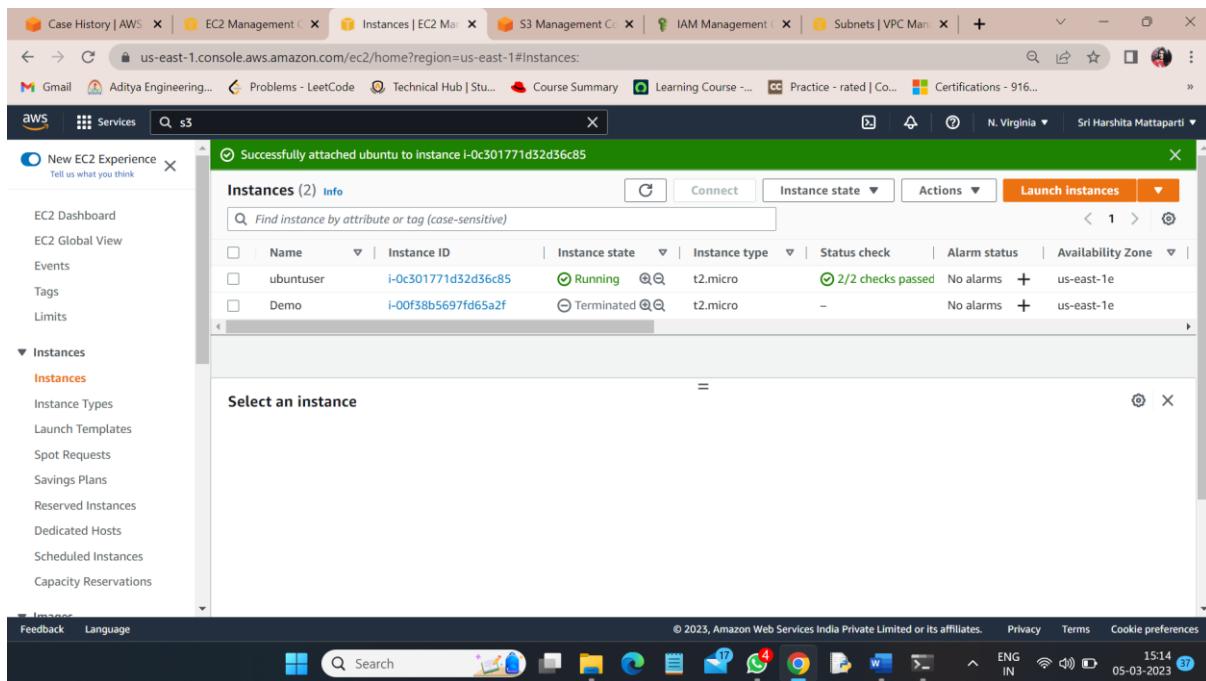
Policy name	Type	Description
(1) Info		

Other tabs include Trust relationships, Tags, Access Advisor, and Revoke sessions.

Assign Instance with the Role

The screenshot shows the AWS EC2 Instances page. A single instance, 'ubuntuser' (Instance ID: i-0c301771d32d36c85), is listed as 'Running'. The 'Actions' menu is open, and the 'Modify IAM role' option is highlighted. The instance summary table includes details like Public IPv4 address (54.158.197.207), Private IPv4 addresses (172.31.63.31), and Public IPv4 DNS (ec2-54-158-197-207.compute-1.amazonaws.com).

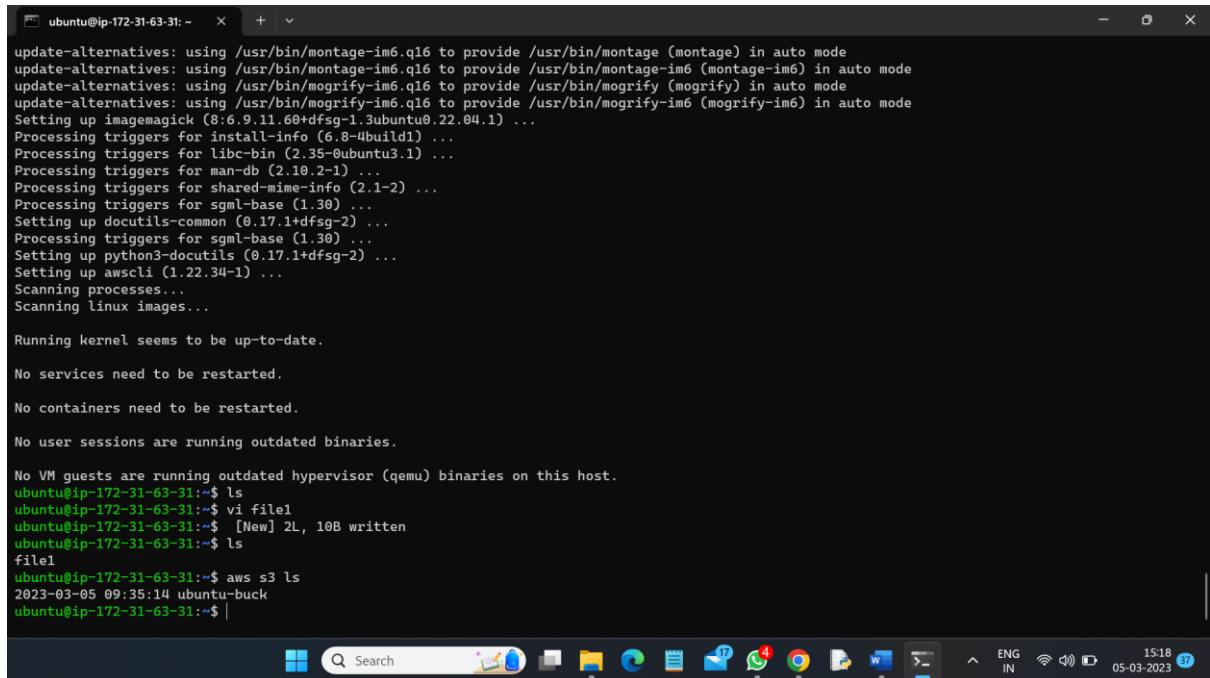
The screenshot shows the 'Modify IAM role' dialog box. The instance ID 'i-0c301771d32d36c85 (ubuntuser)' is selected. In the 'IAM role' section, the dropdown menu shows 'ubuntu' and a 'Create new IAM role' button. At the bottom, there are 'Cancel' and 'Update IAM role' buttons.



Now give sudo apt install awscli

```
ubuntu@ip-172-31-63-31: ~ + ~
Last login: Sun Mar 5 09:26:16 2023 from 223.187.56.108
ubuntu@ip-172-31-63-31:~$ sudo apt install awscli
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
bzip2 docutils-common fontconfig fontconfig-config fonts-droid-fallback fonts-noto-mono fonts-urw-base35 ghostscript groff gsfonts
hicolor-icon-theme imagemagick imagemagick-6-common imagemagick-6.q16 libaoam3 libavahi-client3 libavahi-common-data libavahi-common3
libcairo2 libcurl5 libdatriel libdavid1d5 libde265-0 libdeflate0 libdjvuibre-text libdjvuibre2l libfftw3-double3 libfontconfig1 libgomp1
libgraphite2-3 libgs9 libgs9-common libharfbuzz0b libheif1 libice6 libidn12 libijs-0.35 libilmbase25 libimagequant0 libjbig0 libjbig2dec0
libjpeg-turbo8 libjpeg8 libjxr-tools libjxr0 liblcms2-2 liblqr-1-0 libltdl7 libmagickcore-6.q16-6 libmagickcore-6.q16-6-extra
libmagickwand-6.q16-6 libnetpbm10 libopenexr25 libopenjp2-7 libpango-1.0-0 libpangocairo-1.0-0 libpangoft2-1.0-0 libpaper-utils libpaper1
libpixman-1-0 libraqm0 libsm6 libthai-data libthai0 libtiff5 libwebp7 libwebpdmux2 libwebpnum3 libwmflite-0.2-7 libx265-199 libxaw7
libxcb-render0 libxcb-shm0 libxmu6 libxp4 libxrender1 libxt6 mailcap mime-support netpbm poppler-data psutils python3-botocore
python3-dateutil python3-docutils python3-jmespath python3-olefile python3-pil python3-pygments python3-roman python3-rsa python3-s3transfer
sgml-base x11-common xml-core
Suggested packages:
bzip2-doc docutils-noto fonts-freefont-otf | fonts-freefont-ttf fonts-texgyre ghostscript-x imagemagick-doc autotrace cups-bsd | lpr | lprng
enscript ffmpeg gimp gnuplot grads graphviz hp2xx html2ps libwmf-bin mplayer povray radiance sane-utils texlive-base-bin transfig
ufraw-batch xdg-utils cups-common libfftw3-bin libfftw3-dev liblcms2-utils inkscape poppler-utils fonts-japanese-mincho
| fonts-ipafont-mincho fonts-japanese-gothic | fonts-ipafont-gothic fonts-arpthic-ukai fonts-arpthic-uming fonts-nanum docutils-doc
fonts-linuxlibertine | ttf-linux-libertine texlive-lang-french texlive-latex-base texlive-latex-recommended python3-pil-doc
python3-pygments-doc ttf-bitstream-vera sgml-base-doc debhelper
The following NEW packages will be installed:
awscli bzip2 docutils-common fontconfig fontconfig-config fonts-droid-fallback fonts-noto-mono fonts-urw-base35 ghostscript groff gsfonts
hicolor-icon-theme imagemagick imagemagick-6-common imagemagick-6.q16 libaoam3 libavahi-client3 libavahi-common-data libavahi-common3
libcairo2 libcurl5 libdatriel libdavid1d5 libde265-0 libdeflate0 libdjvuibre-text libdjvuibre2l libfftw3-double3 libfontconfig1 libgomp1
libgraphite2-3 libgs9 libgs9-common libharfbuzz0b libheif1 libice6 libidn12 libijs-0.35 libilmbase25 libimagequant0 libjbig0 libjbig2dec0
libjpeg-turbo8 libjpeg8 libjxr-tools libjxr0 liblcms2-2 liblqr-1-0 libltdl7 libmagickcore-6.q16-6 libmagickcore-6.q16-6-extra
libmagickwand-6.q16-6 libnetpbm10 libopenexr25 libopenjp2-7 libpango-1.0-0 libpangocairo-1.0-0 libpangoft2-1.0-0 libpaper-utils libpaper1
libpixman-1-0 libraqm0 libsm6 libthai-data libthai0 libtiff5 libwebp7 libwebpdmux2 libwebpnum3 libwmflite-0.2-7 libx265-199 libxaw7
libxcb-render0 libxcb-shm0 libxmu6 libxp4 libxrender1 libxt6 mailcap mime-support netpbm poppler-data psutils python3-botocore
python3-dateutil python3-docutils python3-jmespath python3-olefile python3-pil python3-pygments python3-roman python3-rsa python3-s3transfer
sgml-base x11-common xml-core
```

Now create any file, aws s3 ls command will give the list of buckets in S3



```
update-alternatives: using /usr/bin/montage-im6.q16 to provide /usr/bin/montage (montage) in auto mode
update-alternatives: using /usr/bin/montage-im6.q16 to provide /usr/bin/montage-im6 (montage-im6) in auto mode
update-alternatives: using /usr/bin/mogrify-im6.q16 to provide /usr/bin/mogrify (mogrify) in auto mode
update-alternatives: using /usr/bin/mogrify-im6.q16 to provide /usr/bin/mogrify-im6 (mogrify-im6) in auto mode
Setting up imagemagick (8:6.9.11.60+dfsg-1.3ubuntu0.22.04.1) ...
Processing triggers for install-info (6.8-4build1) ...
Processing triggers for libc-bin (2.35-0ubuntu3.1) ...
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for shared-mime-info (2.1-2) ...
Processing triggers for sgml-base (1.30) ...
Setting up docutils-common (0.17.1+dfsg-2) ...
Processing triggers for sgml-base (1.30) ...
Setting up python3-docutils (0.17.1+dfsg-2) ...
Setting up awscli (1.22.34-1) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

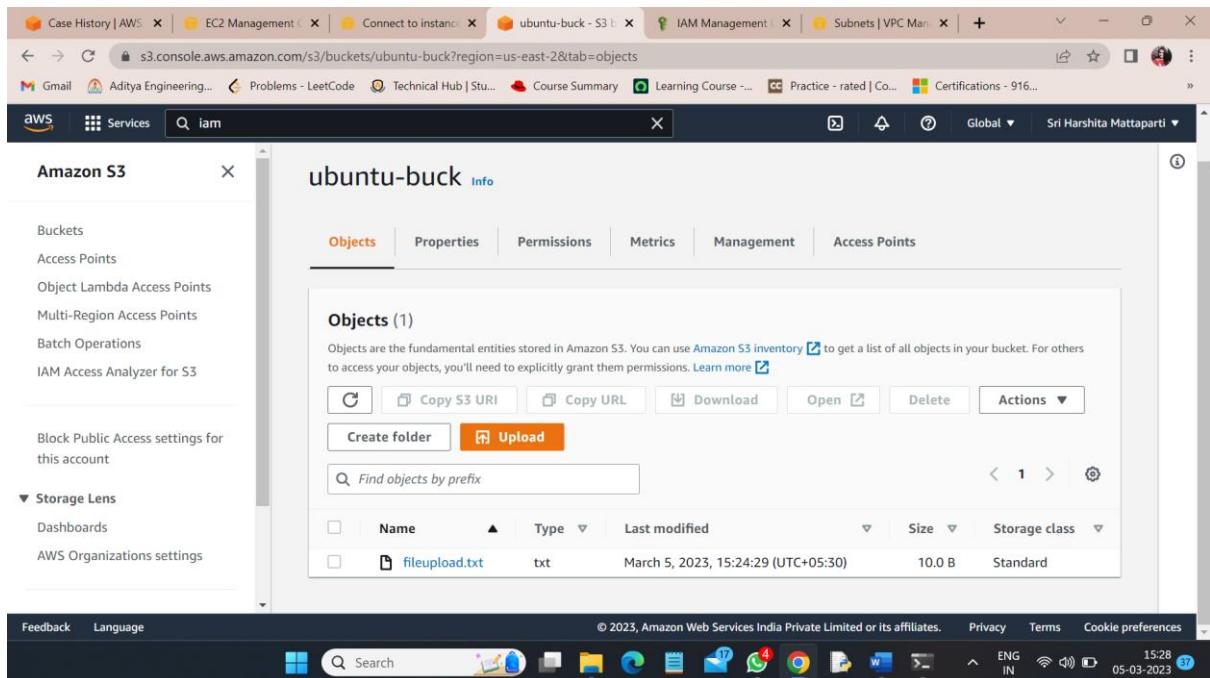
No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
ubuntu@ip-172-31-63-31:~$ ls
ubuntu@ip-172-31-63-31:~$ vi file1
ubuntu@ip-172-31-63-31:~$ [New] 2L, 10B written
ubuntu@ip-172-31-63-31:~$ ls
file1
ubuntu@ip-172-31-63-31:~$ aws s3 ls
2023-03-05 09:35:14 ubuntu-buck
ubuntu@ip-172-31-63-31:~$ |
```

Upload the file into the bucket

```
ubuntu@ip-172-31-63-31:~$ aws s3 cp file1 s3://ubuntu-buck/fileupload.txt
upload: ./file1 to s3://ubuntu-buck/fileupload.txt
ubuntu@ip-172-31-63-31:~$ |
```

The file has been uploaded



The screenshot shows the AWS S3 console interface. On the left, there's a sidebar with navigation links like 'Case History | AWS', 'EC2 Management', 'Connect to instance', 'ubuntu-buck - S3 b...', 'IAM Management', 'Subnets | VPC Man...', 'Services' (selected), and 'iam'. The main area is titled 'ubuntu-buck info' and shows the 'Objects' tab selected. It displays a single object named 'fileupload.txt' with the following details:

Name	Type	Last modified	Size	Storage class
fileupload.txt	txt	March 5, 2023, 15:24:29 (UTC+05:30)	10.0 B	Standard

Now edit the bucket policy

The screenshot shows the AWS S3 Policy editor interface. On the left, a sidebar lists various AWS services like Case History, EC2 Manager, Connect, S3 Manager, IAM Manager, Subnets, Settings, and others. The main area is titled "Policy" and displays the following JSON code:

```
1+ {  
2     "Version": "2012-10-17",  
3     "Statement": [  
4         {  
5             "Sid": "PublicReadGetObject",  
6             "Effect": "Allow",  
7             "Principal": "*",  
8             "Action": [  
9                 "s3:GetObject"  
10            ],  
11            "Resource": [  
12                "arn:aws:s3:::ubuntu-buck/*"  
13            ]  
14        }  
15    ]  
16}
```

To the right of the policy code, there's a panel titled "Edit statement PublicReadGetObject" with a "Remove" button. Below it, a section titled "1. Add actions" has a "Choose a service" dropdown set to "Filter services". A list of services is shown, divided into "Included" (S3) and "Available" (AMP, API Gateway, API Gateway V2, ASC, Access Analyzer). At the bottom of the policy editor, there are links for "Feedback", "Language", and the AWS logo.

Now the object has got the public access

The screenshot shows the AWS S3 Buckets page. The left sidebar is identical to the previous screenshot. The main content area shows an "Account snapshot" section with a "View Storage Lens dashboard" button. Below it is a table titled "Buckets (1) Info" with one entry:

Name	AWS Region	Access	Creation date
ubuntu-buck	US East (Ohio) us-east-2	Public	March 5, 2023, 15:05:14 (UTC+05:30)

At the bottom of the page, there are links for "Feedback", "Language", and the AWS logo.

Copy the object url

The screenshot shows the AWS S3 Object Overview page for a file named 'fileupload.txt'. The 'Properties' tab is selected. A green notification box at the bottom right says 'Object URL Copied' with a checkmark. The copied URL is displayed below it: <https://ubuntu-buck.s3.us-east-2.amazonaws.com/fileupload.txt>. The left sidebar shows various AWS services like Buckets, Storage Lens, and IAM Access Analyzer.

Paste the url in the browser

The screenshot shows a browser window with the URL <https://ubuntu-buck.s3.us-east-2.amazonaws.com/fileupload.txt> in the address bar. The page content is 'Hai Hello'. The browser taskbar at the bottom shows various open tabs and system status icons.



