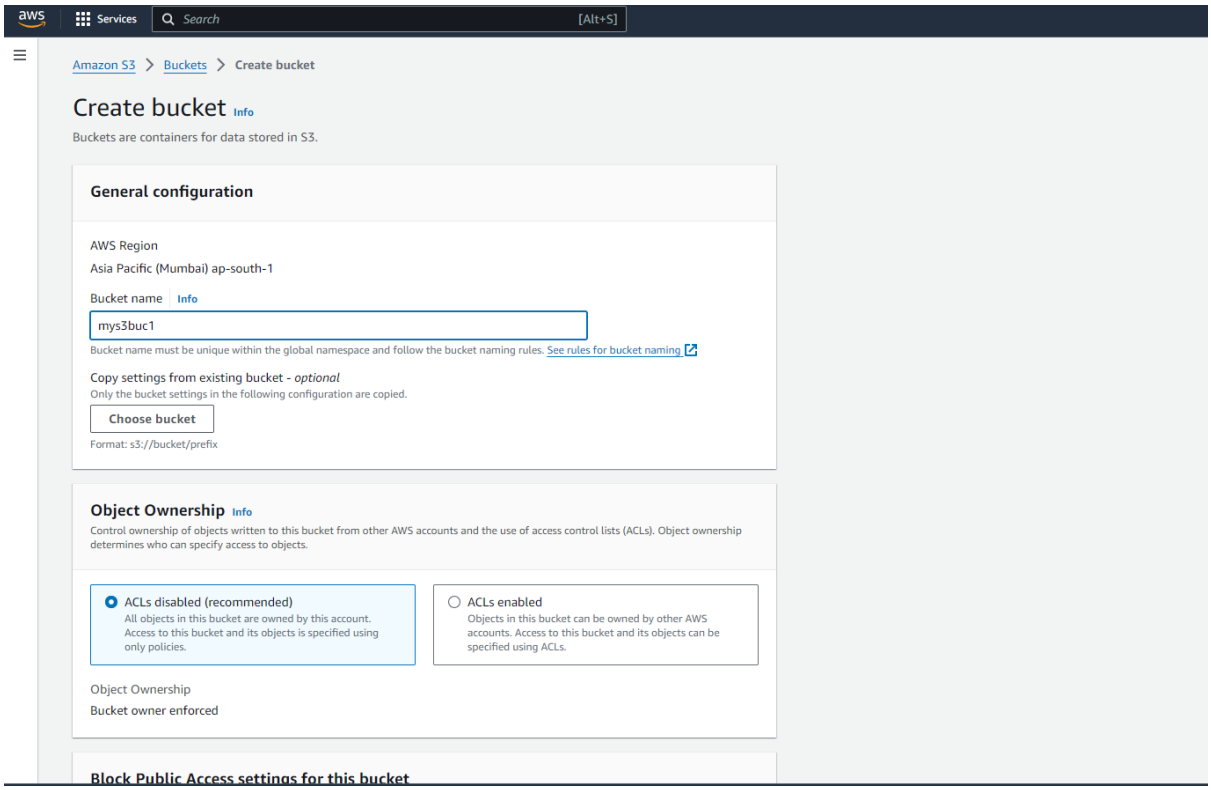
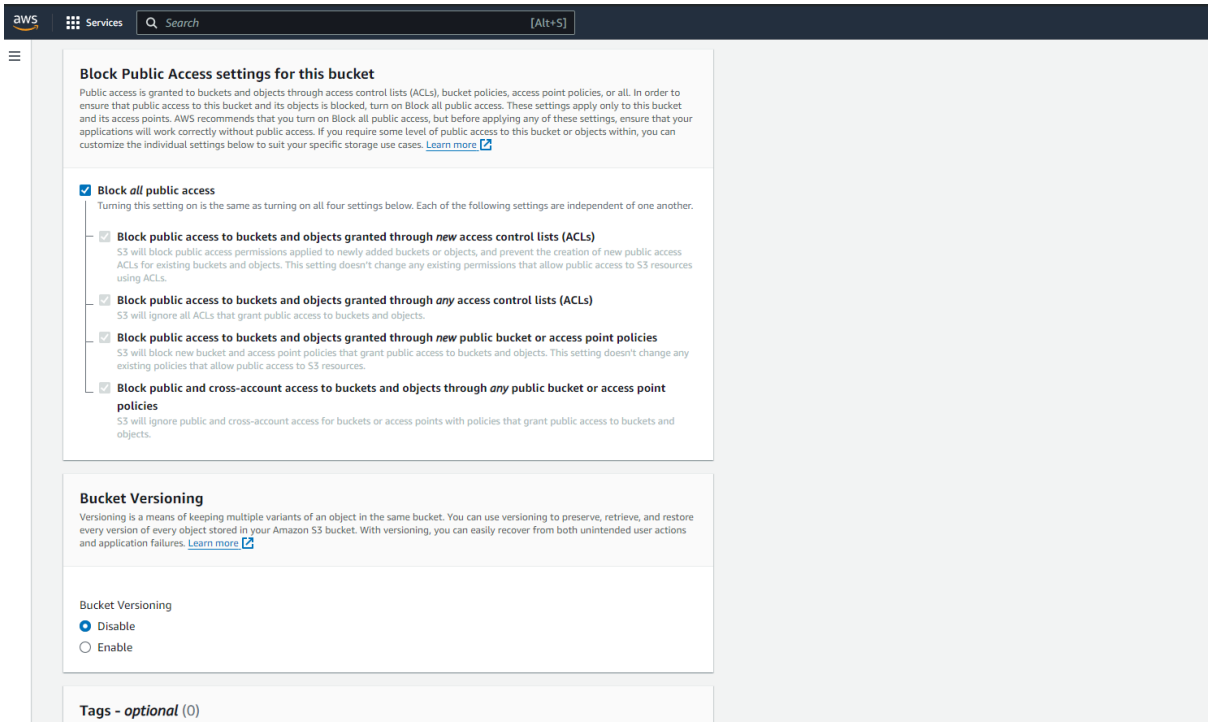
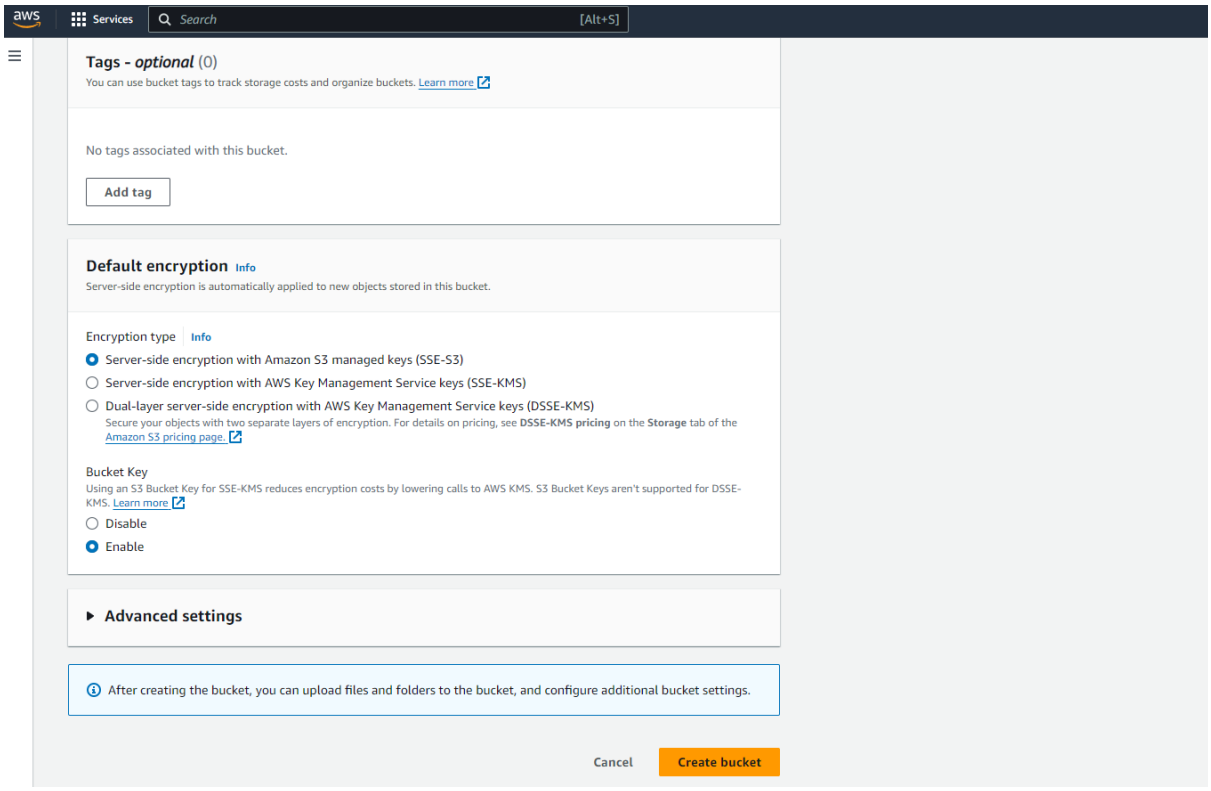
TASK - 15

Create a S3 bucket, with no public access and upload files to the bucket & view the logs for the uploaded files.

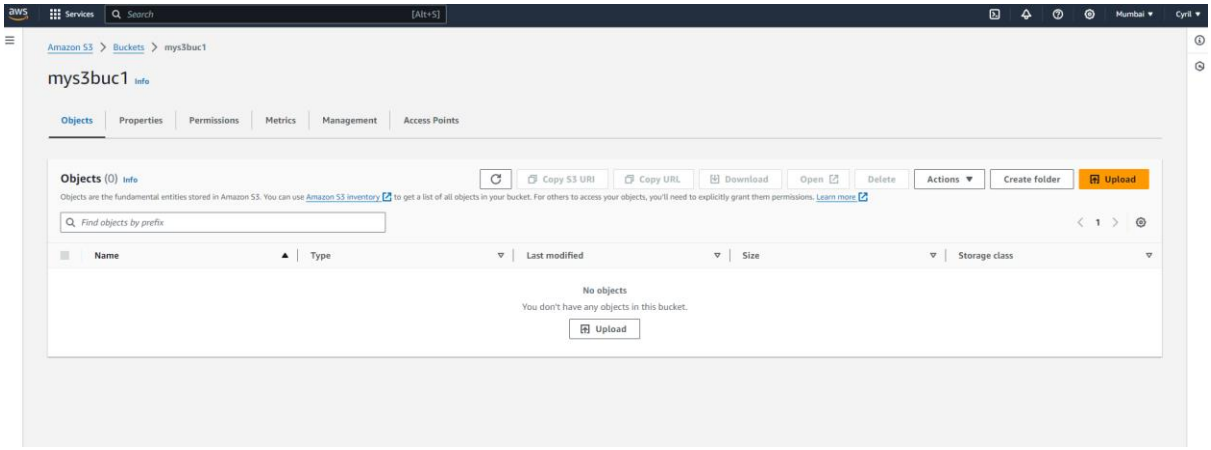
Creating a S3 bucket with no public access:

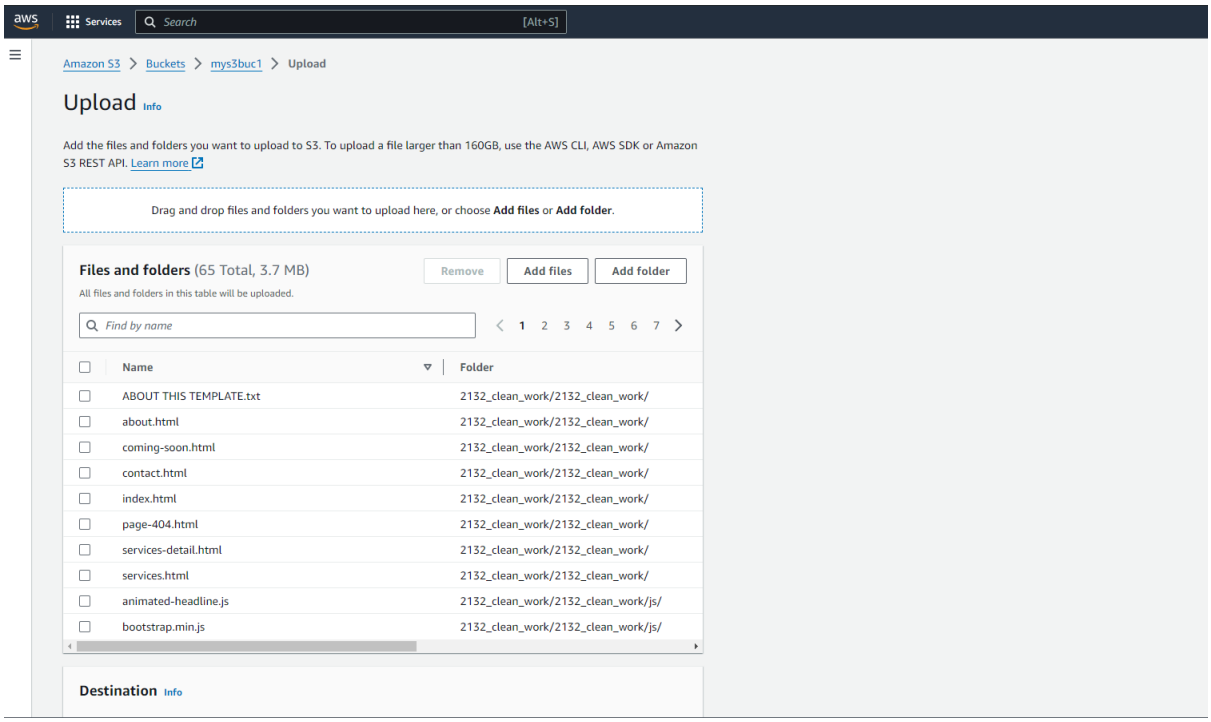



aws
Services
Search
[Alt+S]
Block Public Access settings for this bucket
Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to this bucket and its objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to this bucket or objects within, you can customize the individual settings below to suit your specific storage use cases. Learn more
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.
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 - optional (0)


aws
Services
Search
[Alt+S]
Tags - optional (0)
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
Server-side encryption is automatically applied to new objects stored in this bucket.
Encryption type Info
Server-side encryption with Amazon S3 managed keys (SSE-S3)
Server-side encryption with AWS Key Management Service keys (SSE-KMS)
Dual-layer server-side encryption with AWS Key Management Service keys (DSSE-KMS)
Secure your objects with two separate layers of encryption. For details on pricing, see DSSE-KMS pricing on the Storage tab of the Amazon S3 pricing page.
Bucket Key
Using an S3 Bucket Key for SSE-KMS reduces encryption costs by lowering calls to AWS KMS. S3 Bucket Keys aren't supported for DSSE-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

Uploading files to the bucket:





☐	index.html	2132_clean_work/2132_clean_work/
☐	page-404.html	2132_clean_work/2132_clean_work/
☐	services-detail.html	2132_clean_work/2132_clean_work/
☐	services.html	2132_clean_work/2132_clean_work/
☐	animated-headline.js	2132_clean_work/2132_clean_work/js/
☐	bootstrap.min.js	2132_clean_work/2132_clean_work/js/

Destination Info

Destination

s3://mys3buc1

▶ **Destination details**

Bucket settings that impact new objects stored in the specified destination.

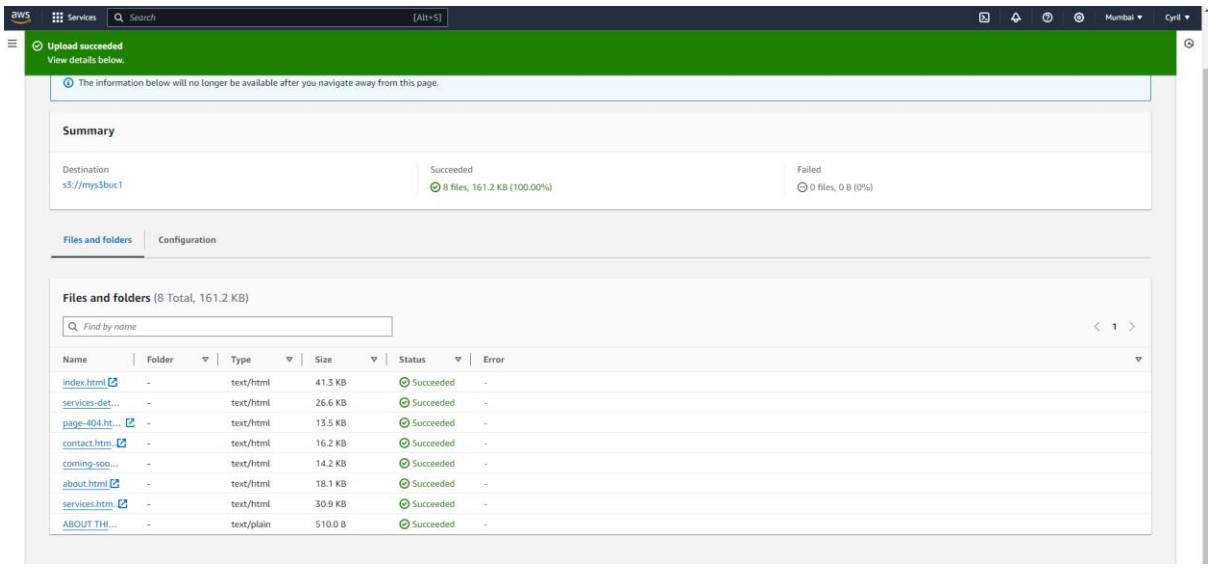
▶ **Permissions**

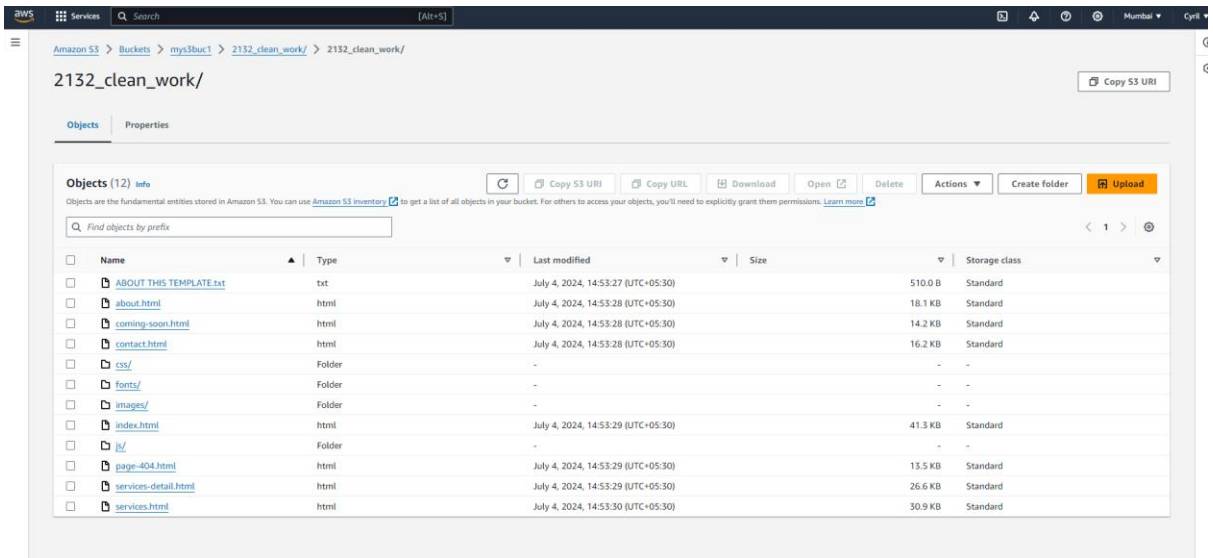
Grant public access and access to other AWS accounts.

▶ **Properties**

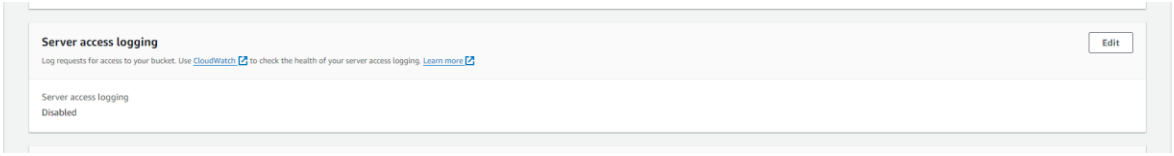
Specify storage class, encryption settings, tags, and more.

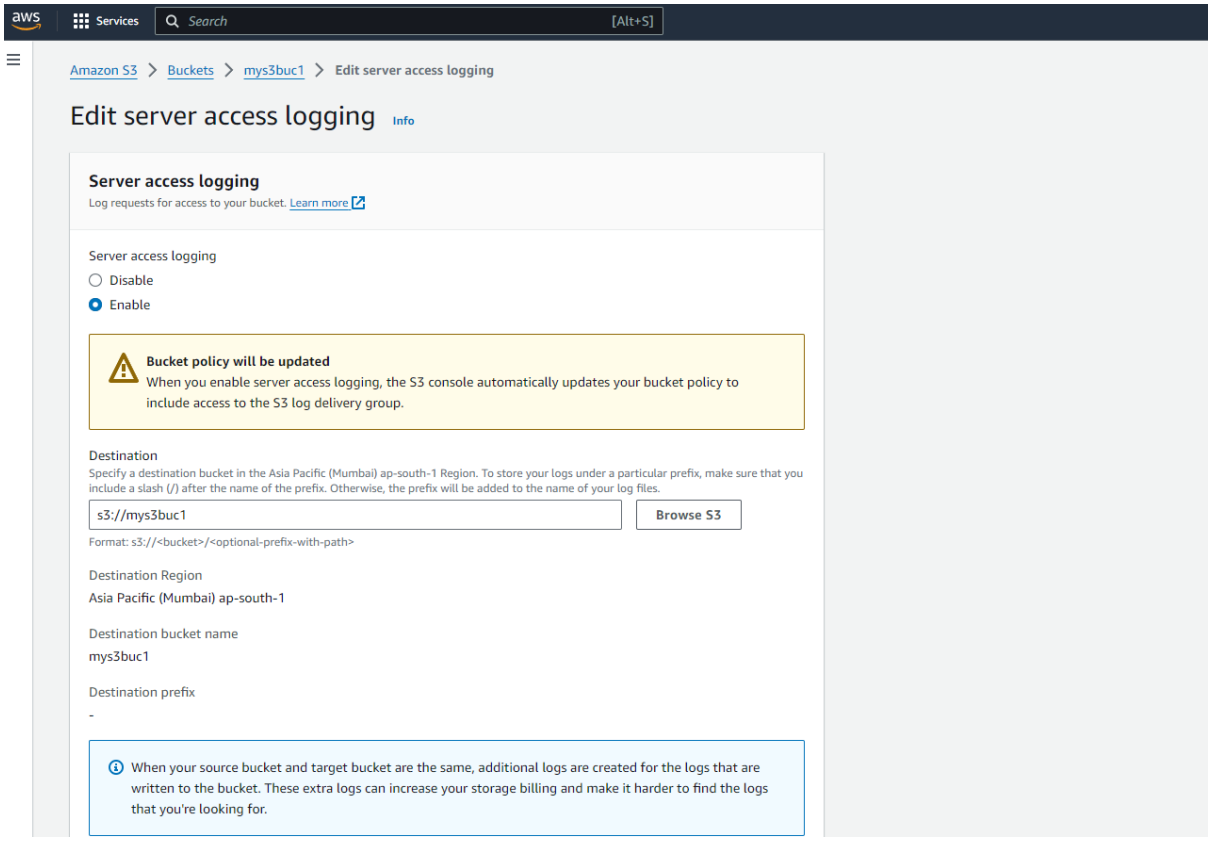
Cancel | Upload



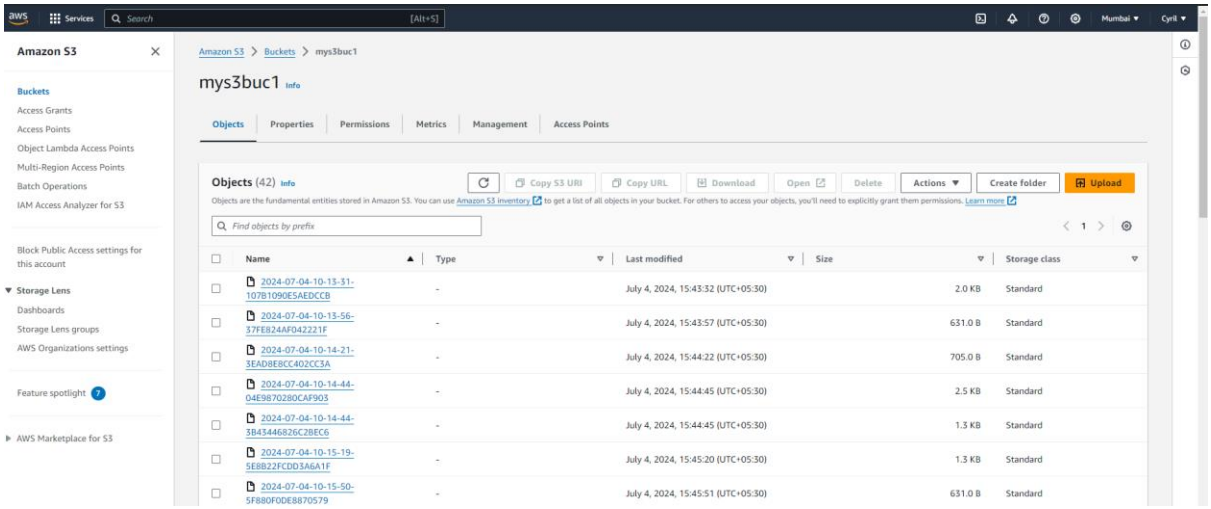


Accessing the log of the bucket:



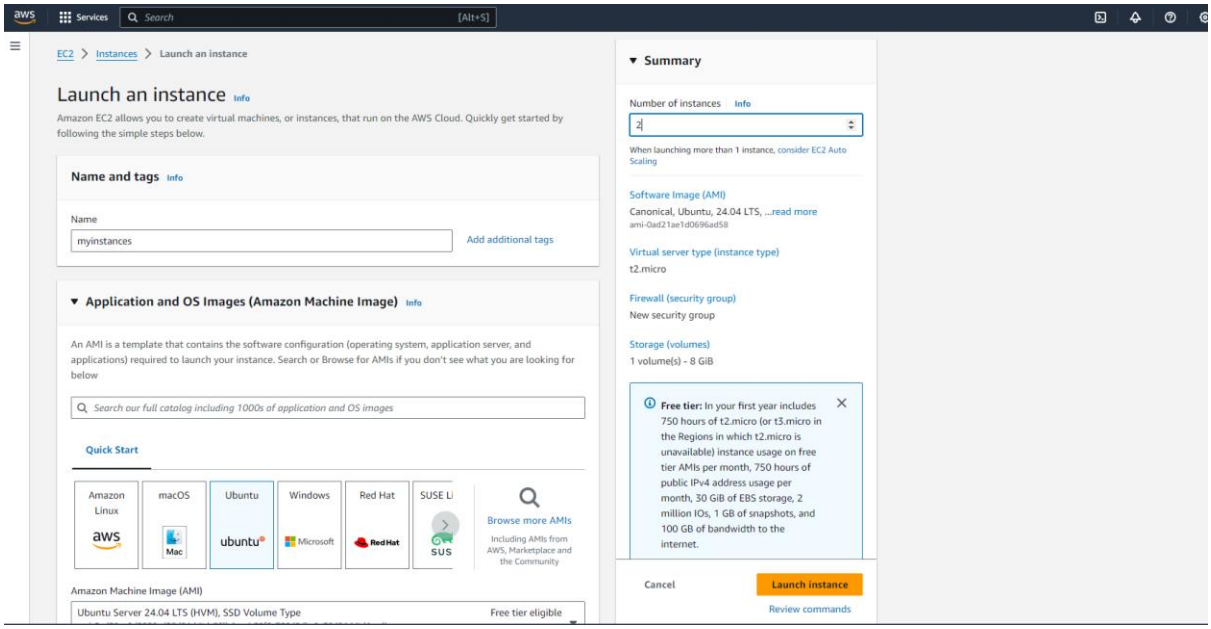


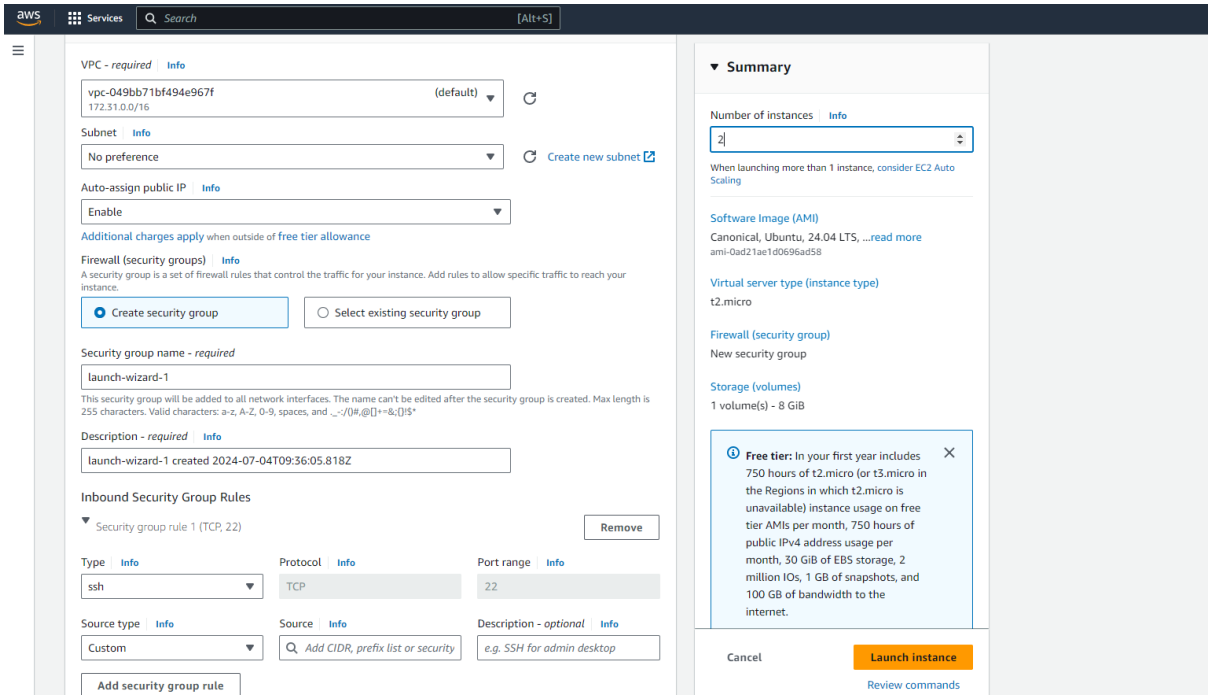
S3 bucket logs:

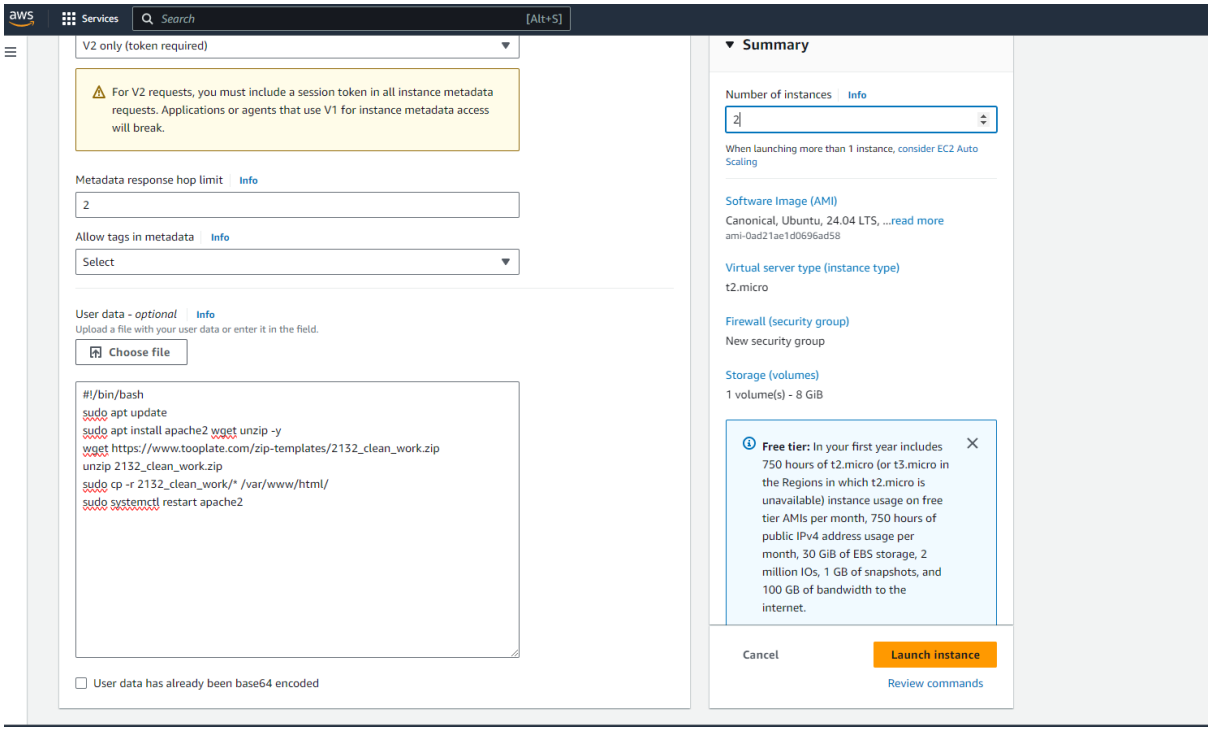


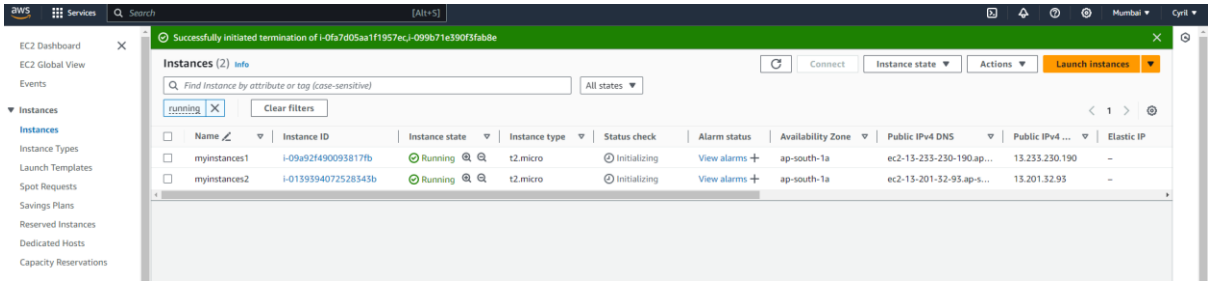
Launch two ec2-instances and connect it to a application load balancer, where the output traffic from the server must be an load balancer IP address

Launching 2 EC2 instances with the same application

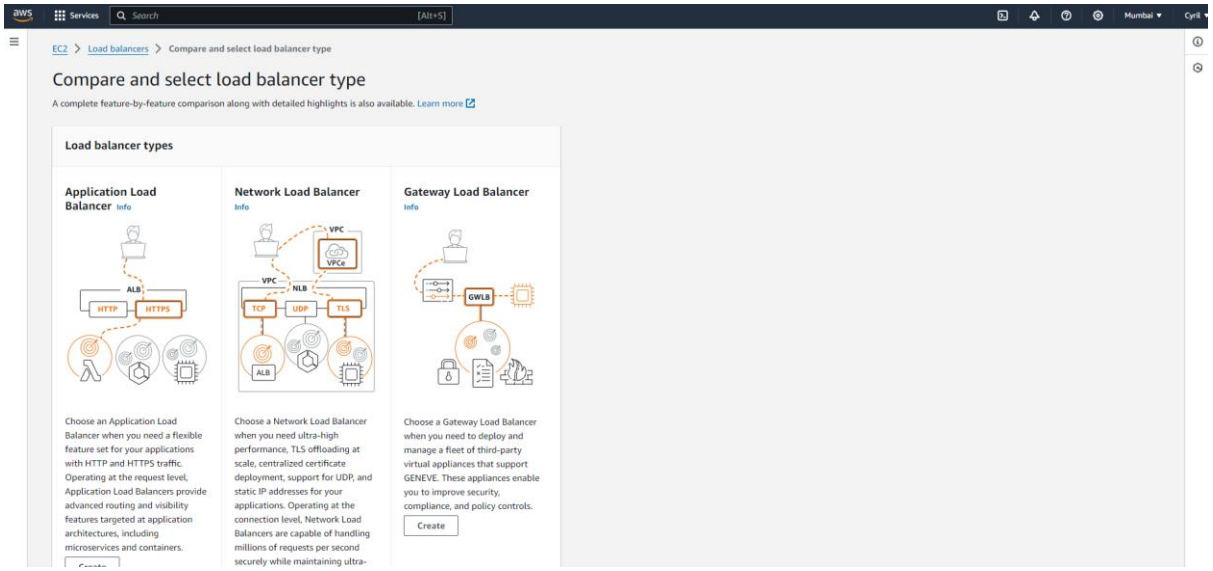


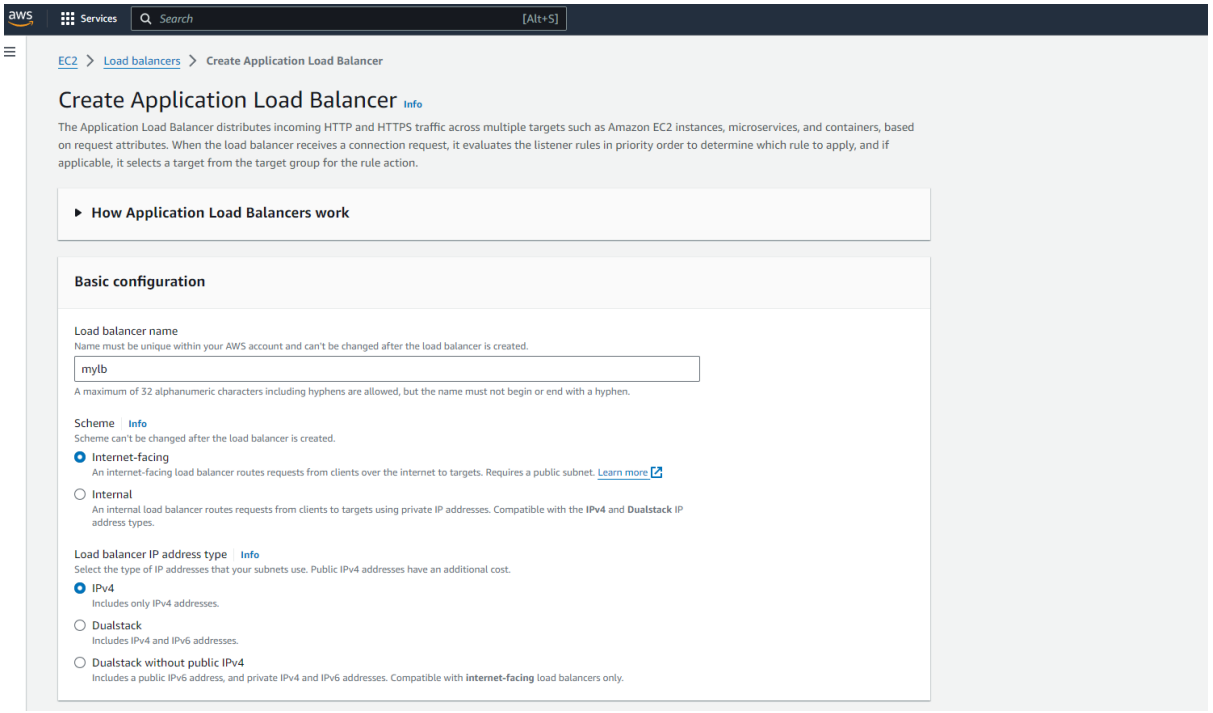

aws
Services
Search
[Alt+S]
VPC - required Info
vpc-049bb71bf494e967f (default)
172.31.0.0/16
Subnet Info
No preference
Create new subnet
Auto-assign public IP Info
Enable
Additional charges apply when outside of free tier allowance
Firewall (security groups) Info
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.
Create security group
Select existing security group
Security group name - required
launch-wizard-1
This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and ._-:/()#,@[]+=&;{}!$*
Description - required Info
launch-wizard-1 created 2024-07-04T09:36:05.818Z
Inbound Security Group Rules
Security group rule 1 (TCP, 22)
Remove
Type Info
ssh
Protocol Info
TCP
Port range Info
22
Source type Info
Custom
Source Info
Add CIDR, prefix list or security
Description - optional Info
e.g. SSH for admin desktop
Add security group rule
Summary
Number of instances Info
2
When launching more than 1 instance, consider EC2 Auto Scaling
Software Image (AMI)
Canonical, Ubuntu, 24.04 LTS, ...read more
ami-0ad21ae1d0696ad58
Virtual server type (instance type)
t2.micro
Firewall (security group)
New security group
Storage (volumes)
1 volume(s) - 8 GiB
Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4 address usage per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.
Cancel
Launch instance
Review commands

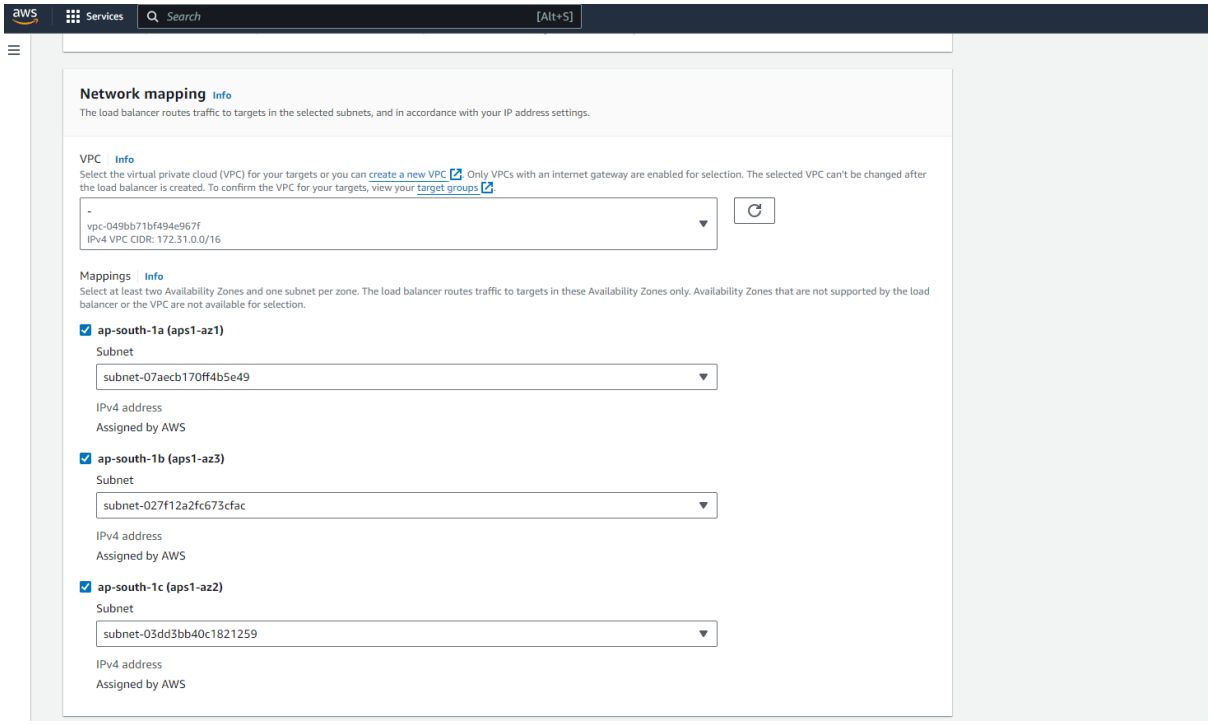

aws
Services
Search
[Alt+S]
V2 only (token required)
For V2 requests, you must include a session token in all instance metadata requests. Applications or agents that use V1 for instance metadata access will break.
Metadata response hop limit Info
2
Allow tags in metadata Info
Select
User data - optional Info
Upload a file with your user data or enter it in the field.
Choose file
#!/bin/bash
sudo apt update
sudo apt install apache2 wget unzip -y
wget https://www.tooplate.com/zip-templates/2132_clean_work.zip
unzip 2132_clean_work.zip
sudo cp -r 2132_clean_work/* /var/www/html/
sudo systemctl restart apache2
User data has already been base64 encoded
Summary
Number of instances Info
2
When launching more than 1 instance, consider EC2 Auto Scaling
Software Image (AMI)
Canonical, Ubuntu, 24.04 LTS, ...read more
ami-0ad21ae1d0696ad58
Virtual server type (instance type)
t2.micro
Firewall (security group)
New security group
Storage (volumes)
1 volume(s) - 8 GiB
Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4 address usage per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.
Cancel
Launch instance
Review commands


aws
Services
Search
[Alt+S]
Mumbai
Cyril
Successfully initiated termination of i-0fa7d05aa1f1957ec,i-099b71e390f3fab8e
EC2 Dashboard
EC2 Global View
Events
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations
Instances (2) Info
Connect
Instance state
Actions
Launch instances
Find Instance by attribute or tag (case-sensitive)
All states
running
Clear filters
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
Availability Zone
Public IPv4 DNS
Public IPv4 ...
Elastic IP
myinstances1
i-09a92f490093817fb
Running
t2.micro
Initializing
View alarms
ap-south-1a
ec2-13-233-230-190.ap...
13.233.230.190
myinstances2
i-0139394072528343b
Running
t2.micro
Initializing
View alarms
ap-south-1a
ec2-13-201-32-93.ap-s...
13.201.32.93

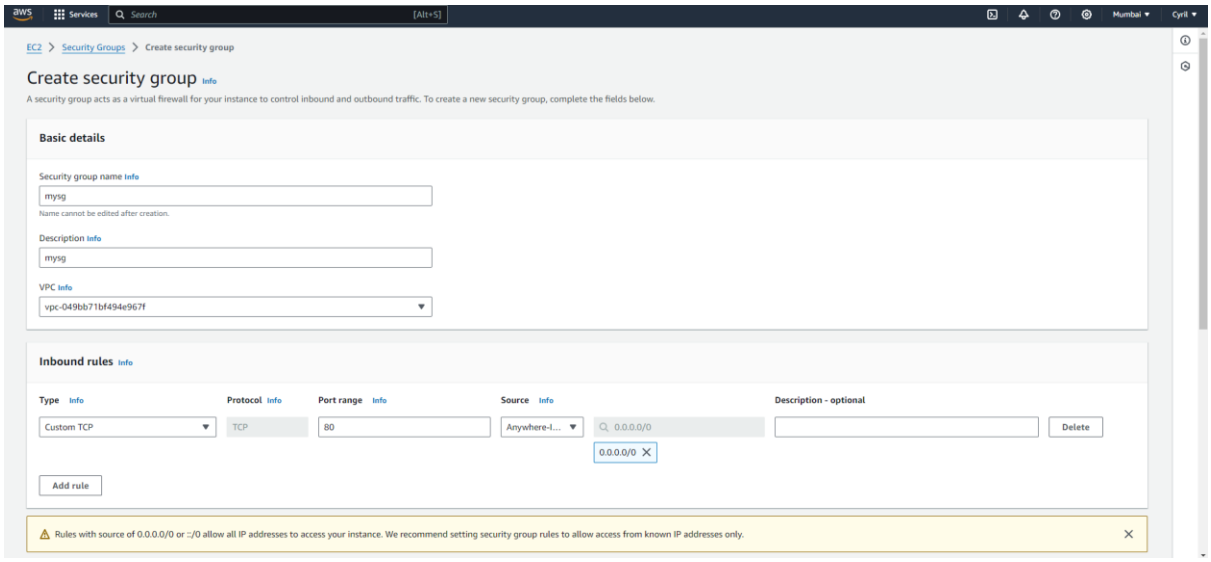
Creating a Load Balancer:



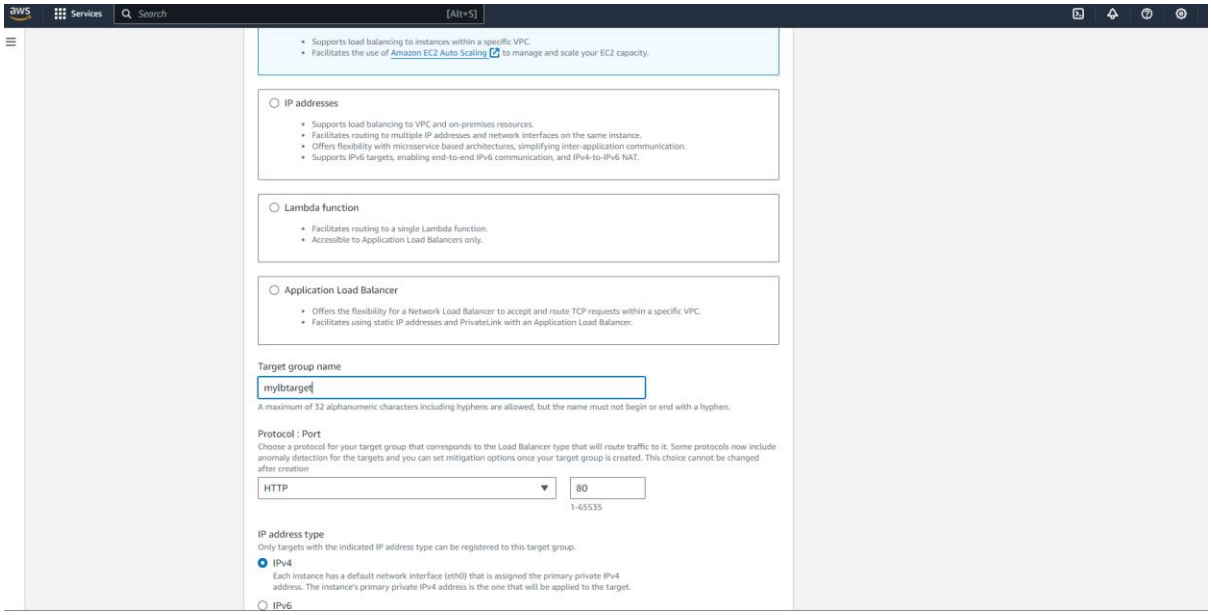


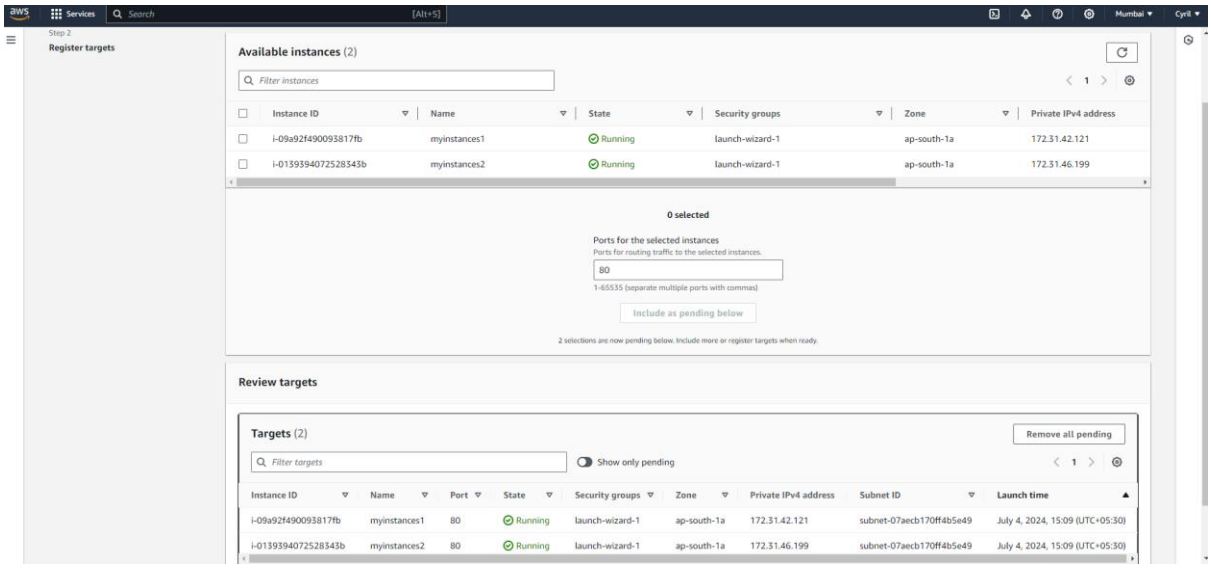


Creating Security Group for the load balancer:

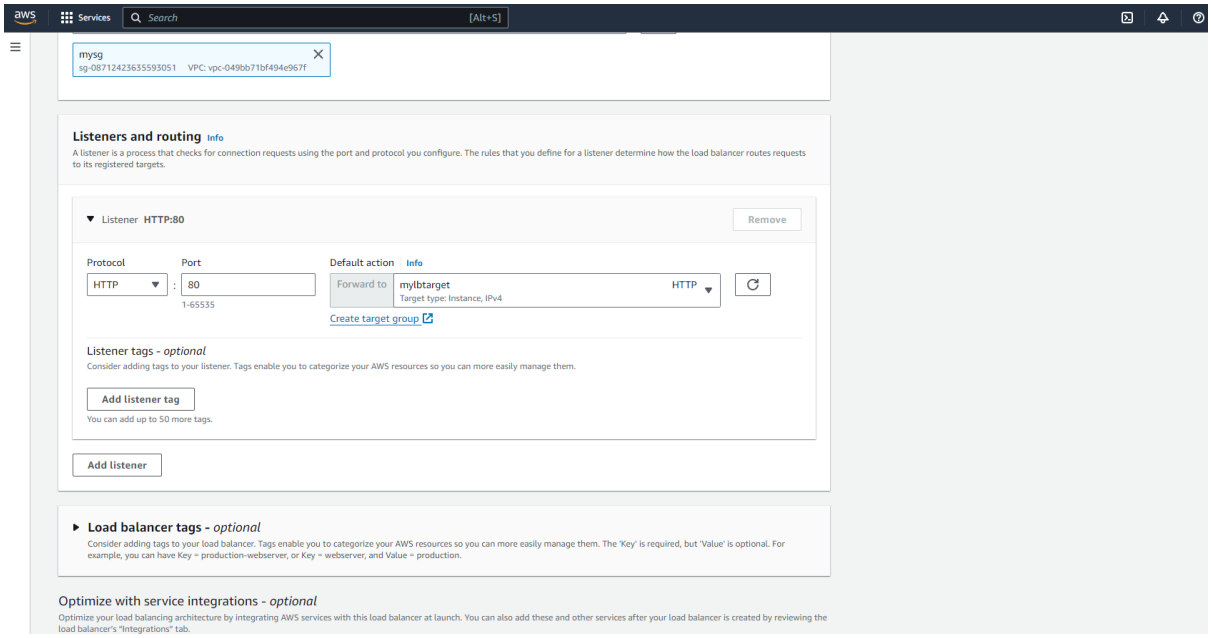


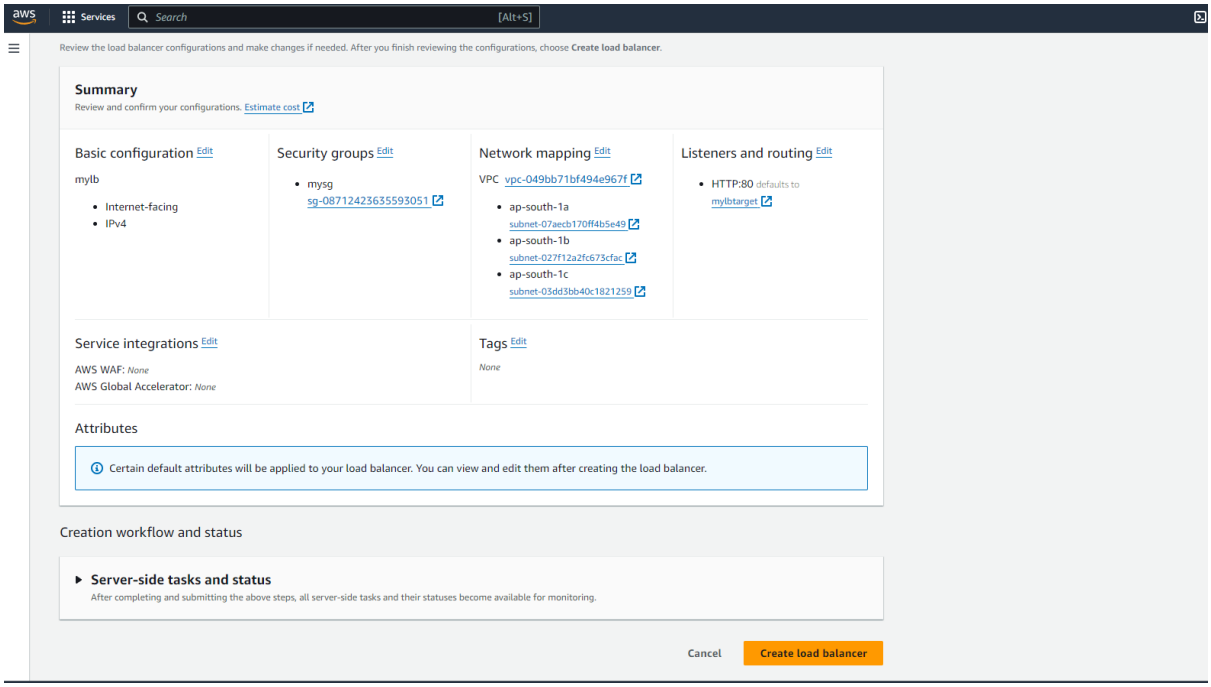
Creating Target Group:





Continuation of Load Balancer Creation:





Connecting to the instance through the load balancer DNS name: