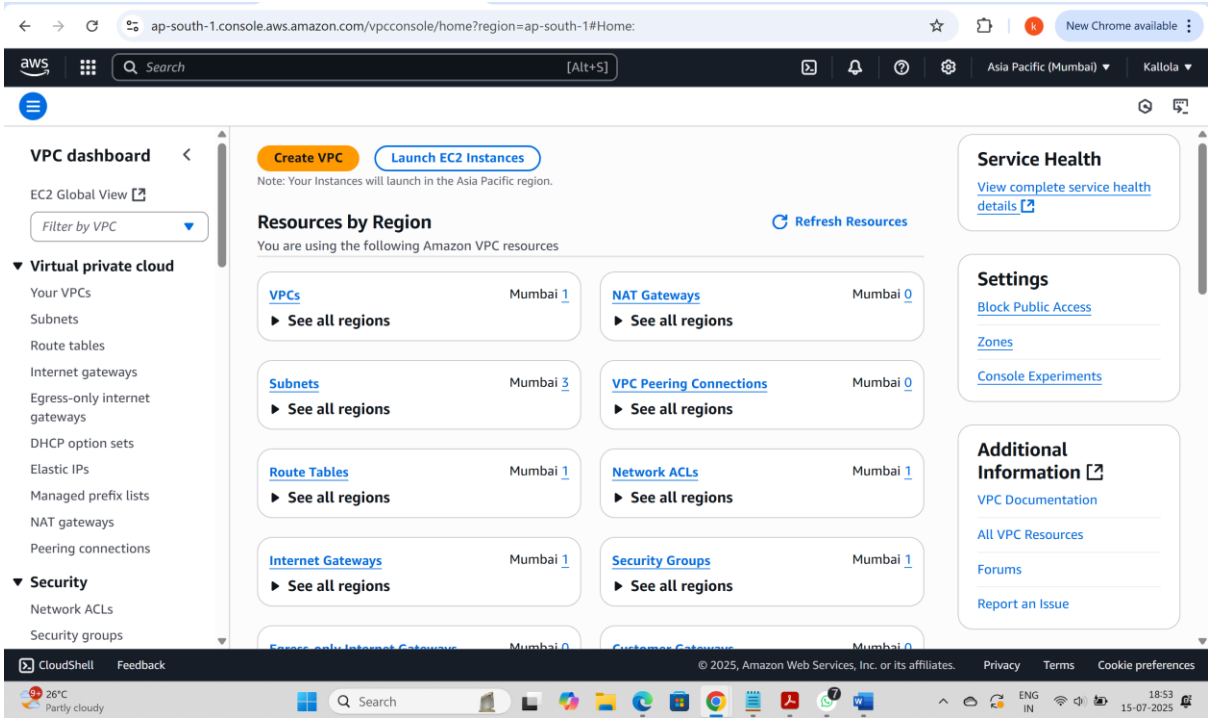
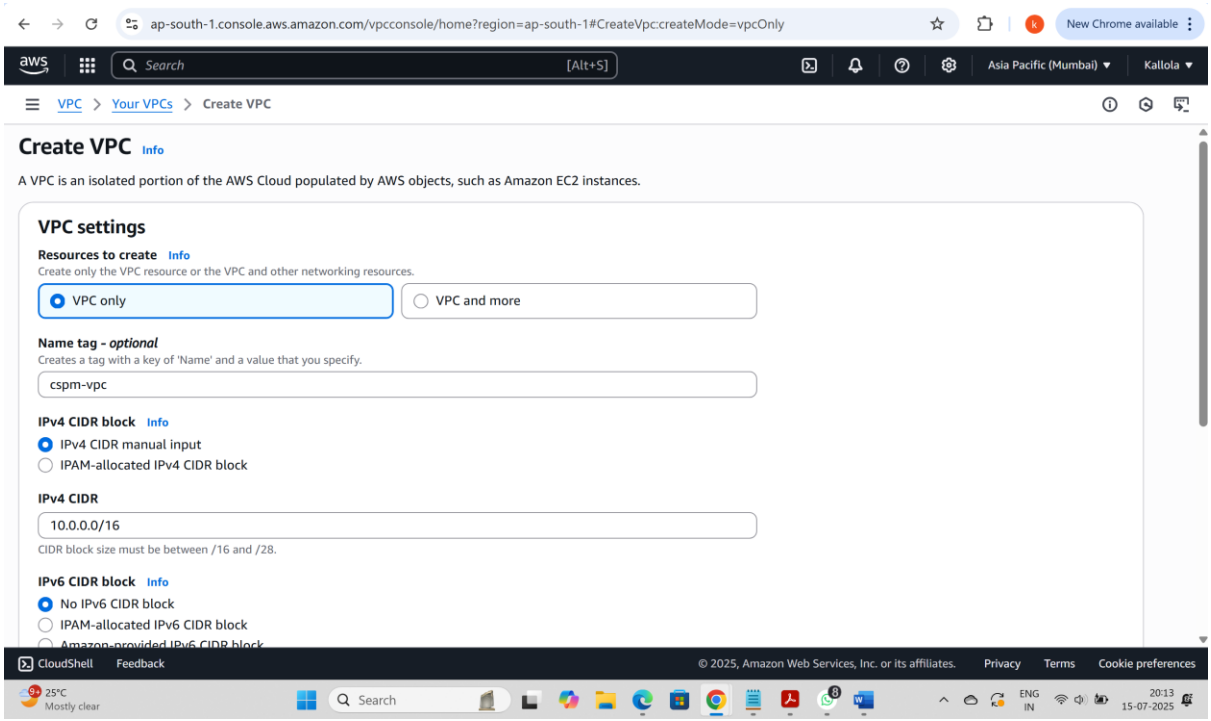
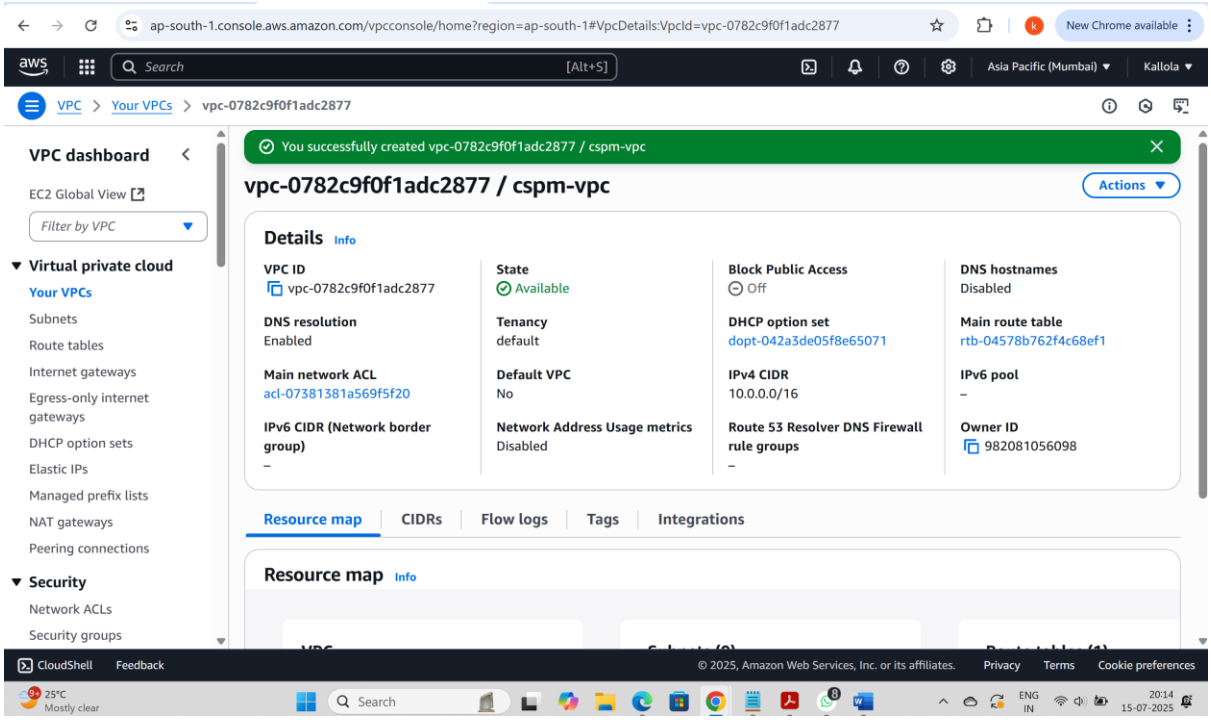
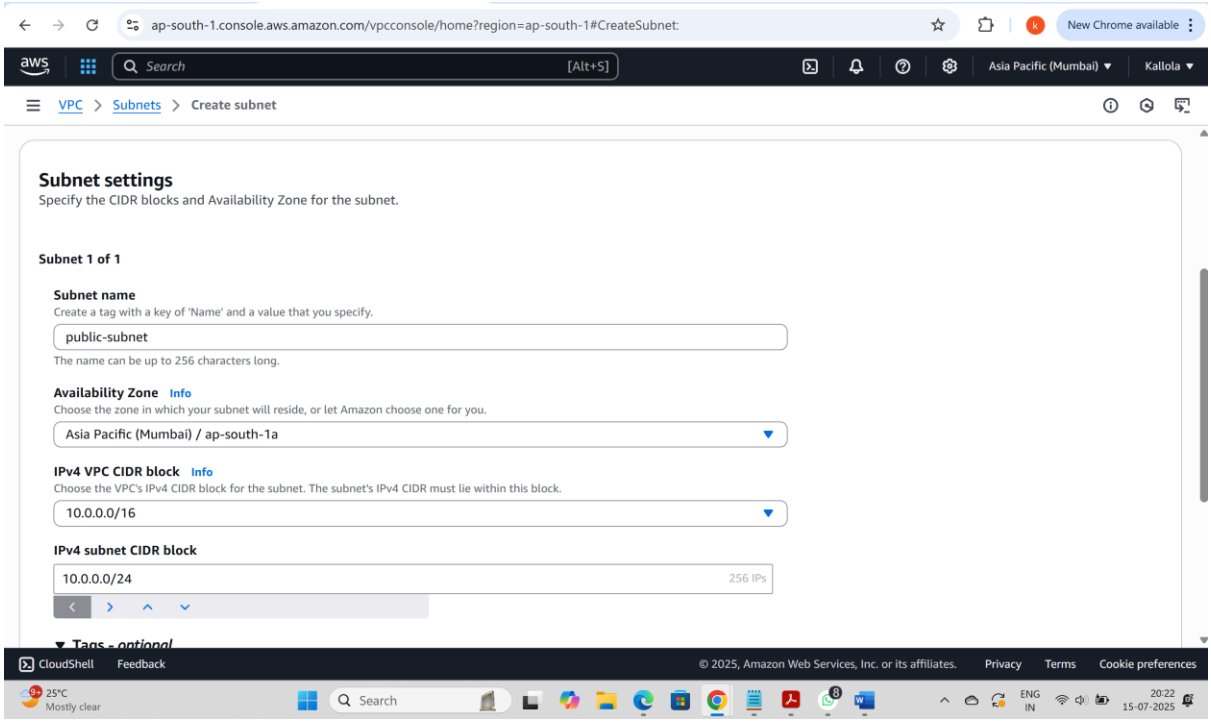
PHASE 1: **Create a Custom VPC**

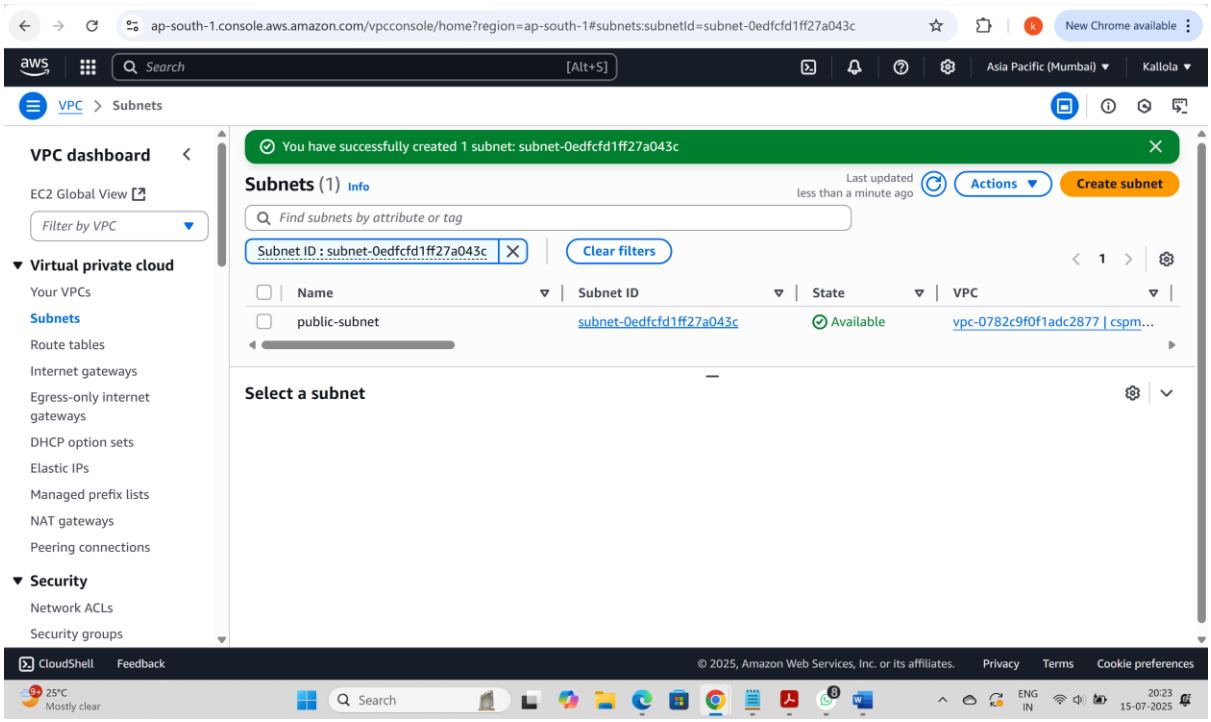




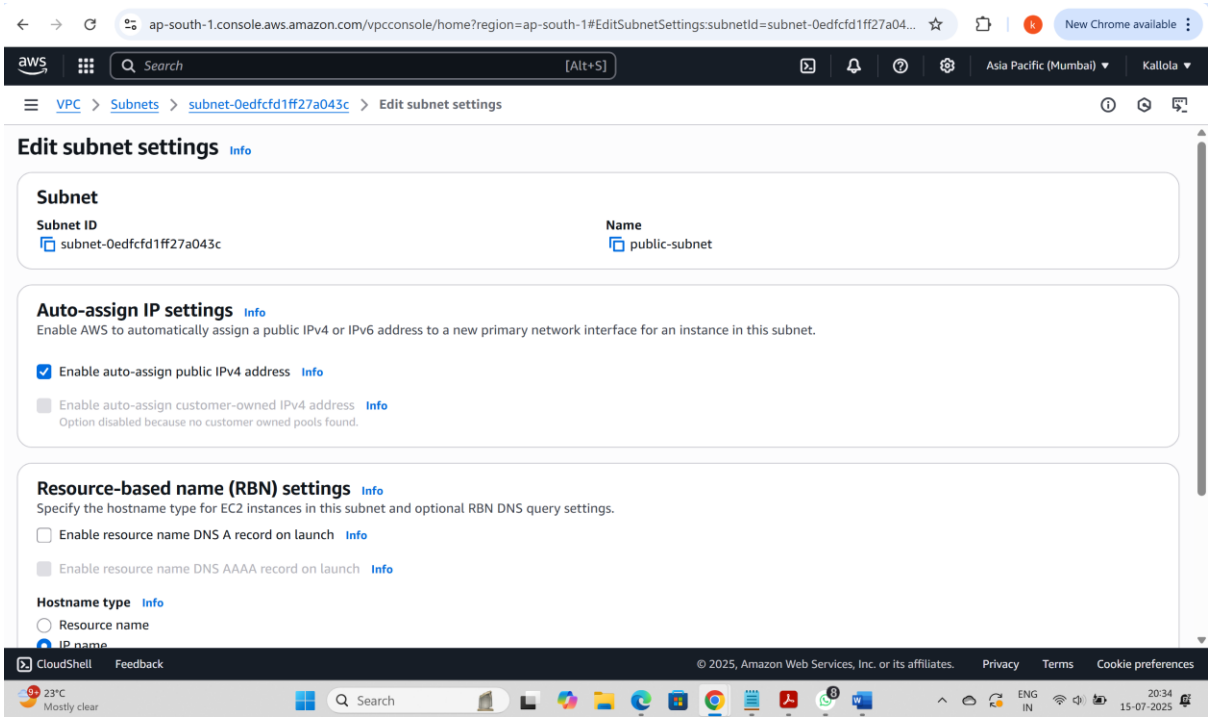


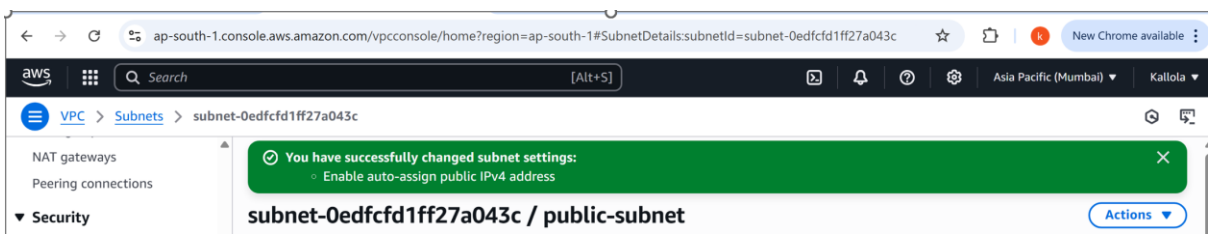
PHASE 2: **Add Subnet**



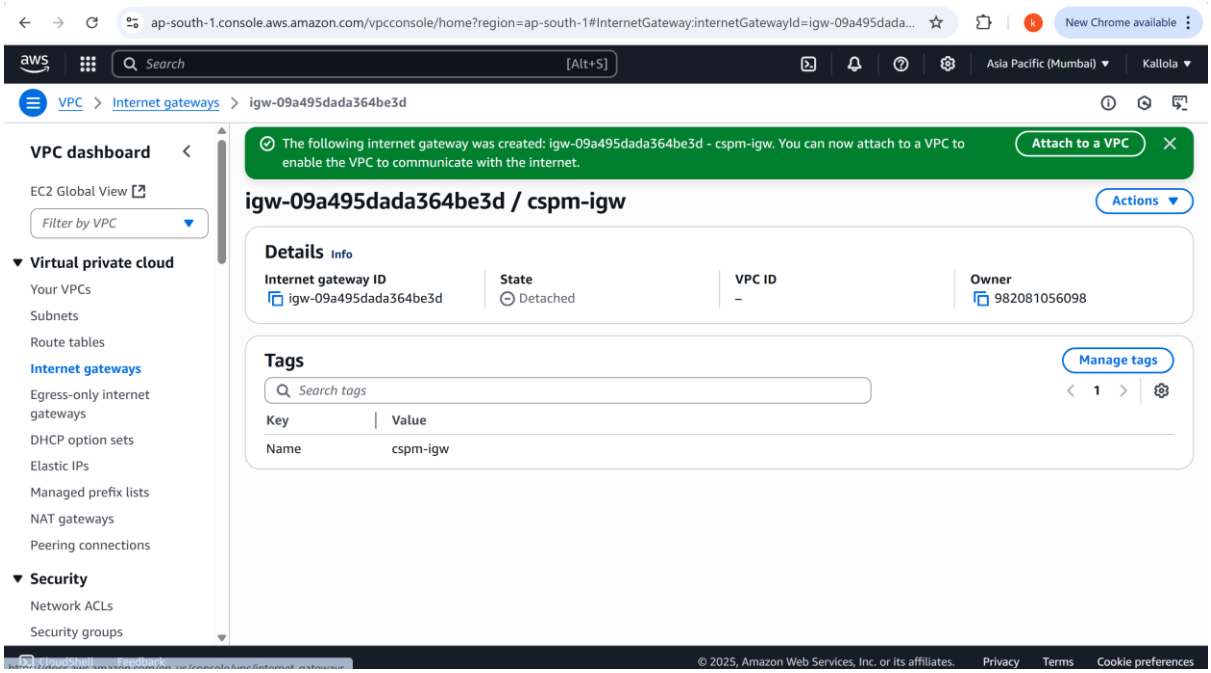


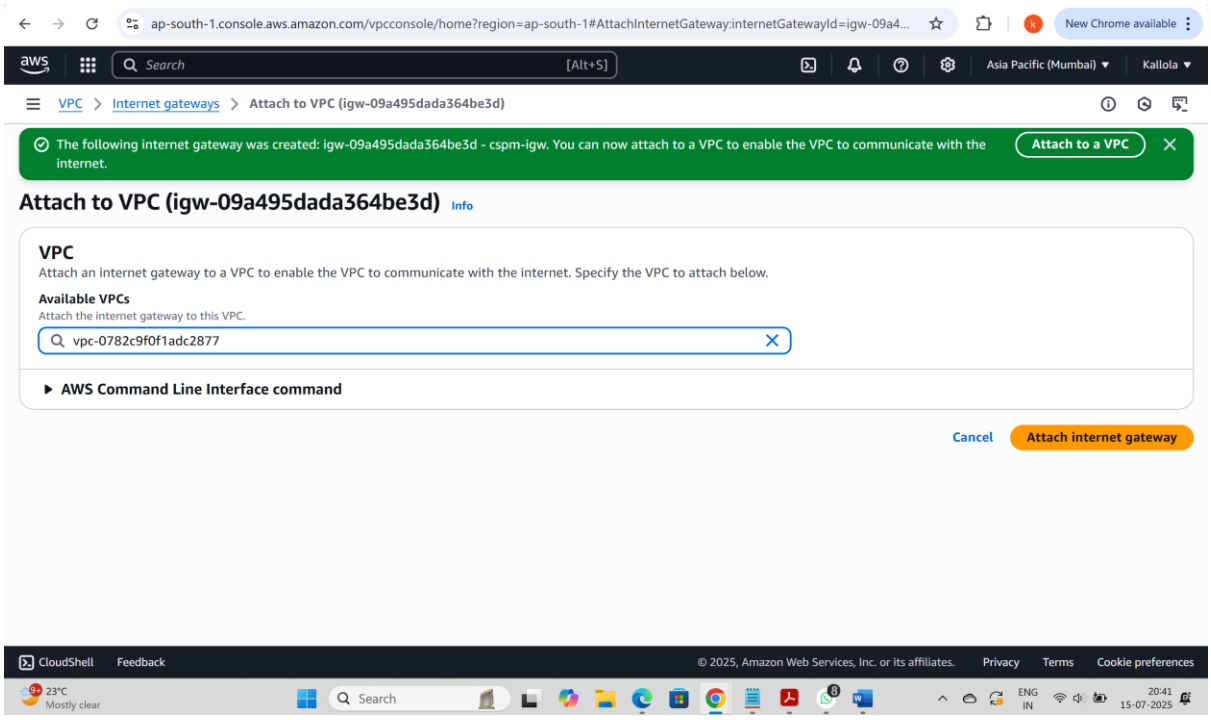
Enable auto-assign public IP:

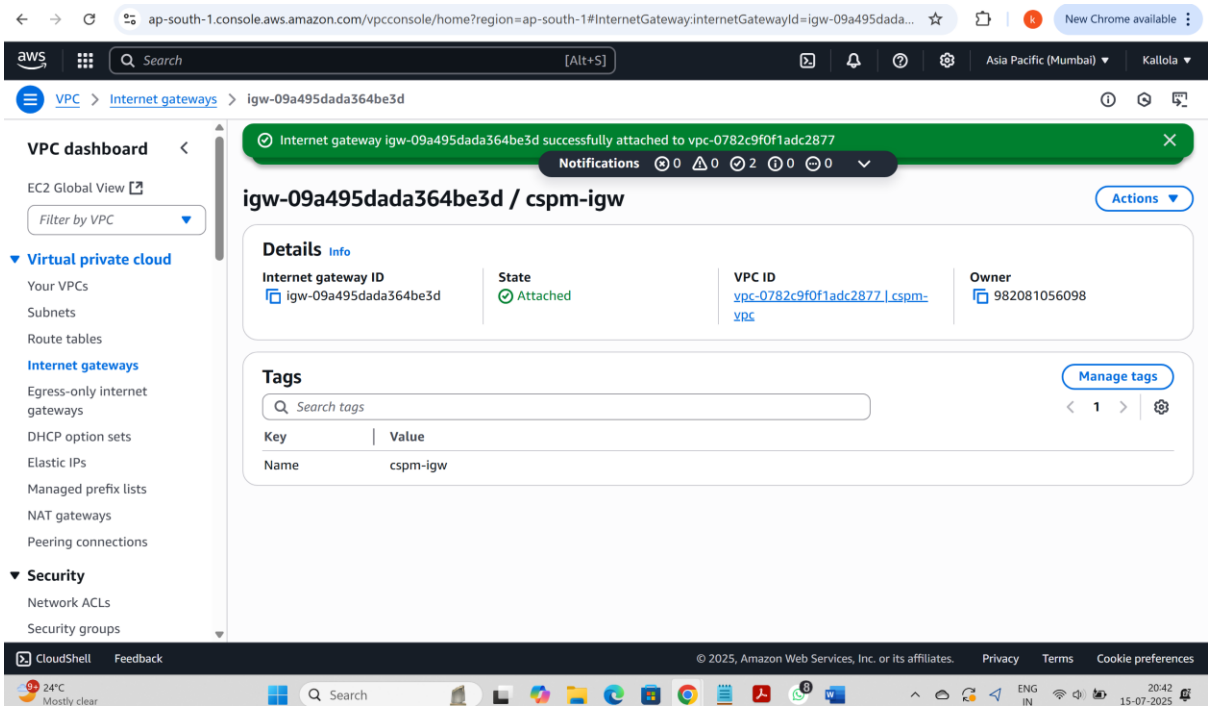


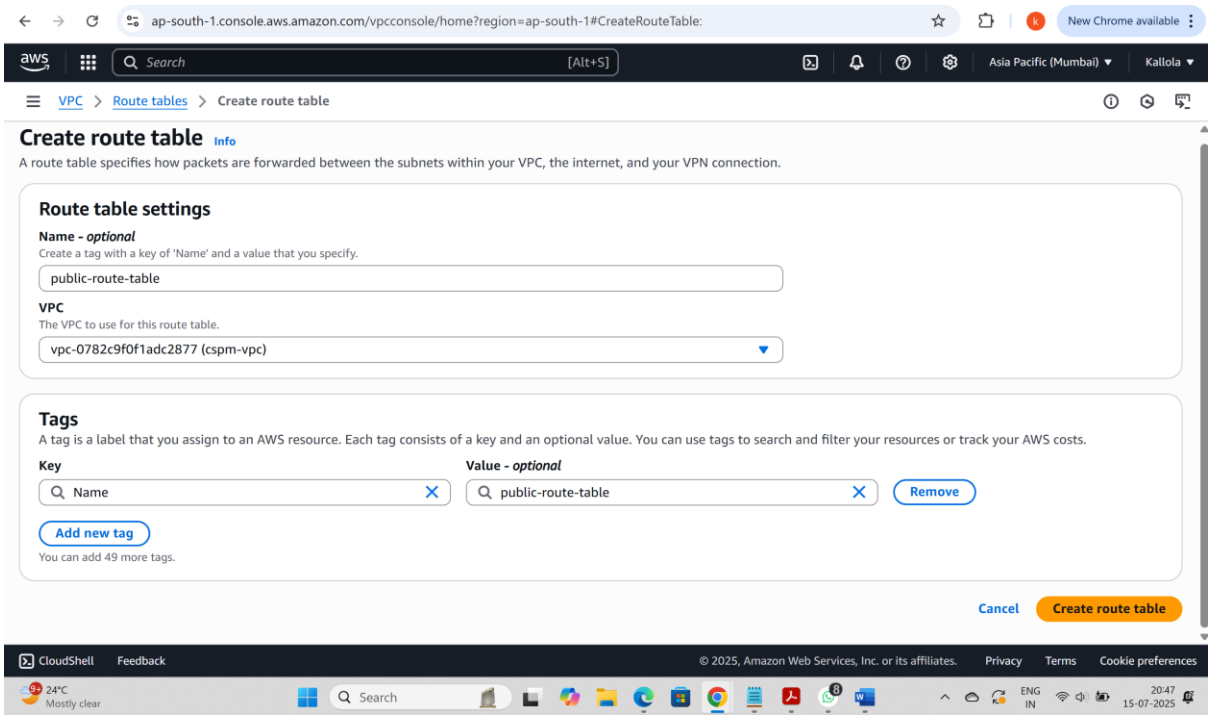


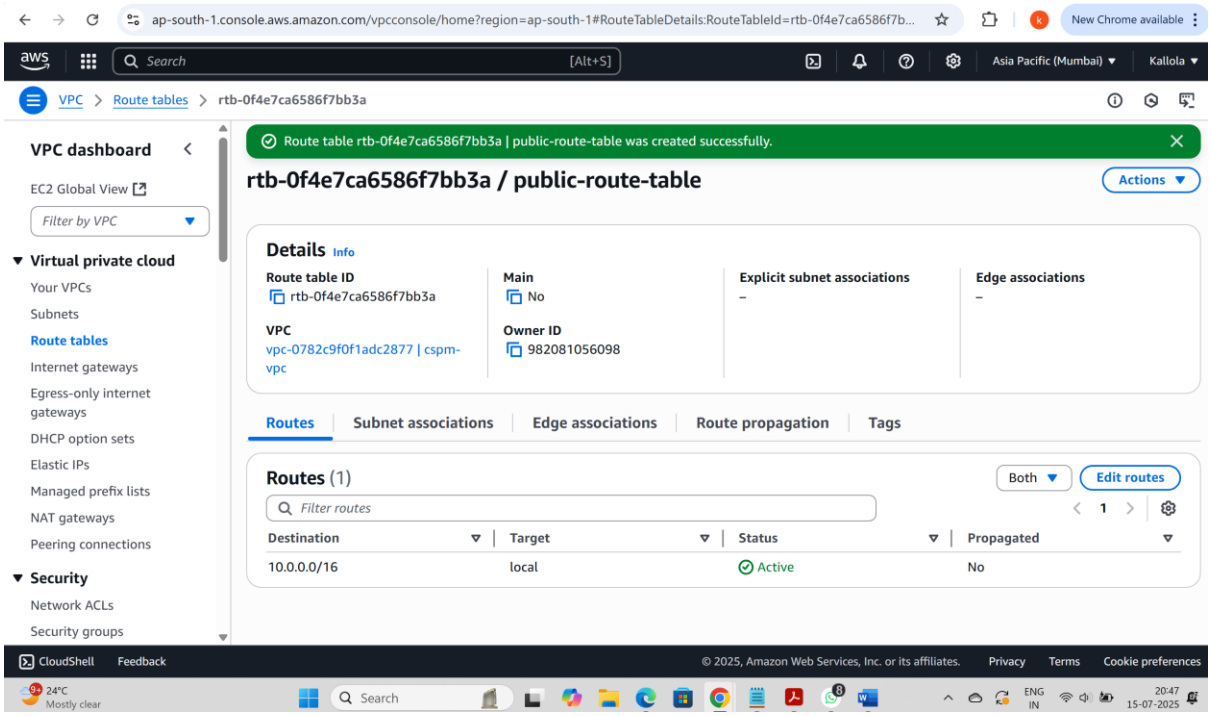
PHASE 3: **Add Internet Gateway & Routing**

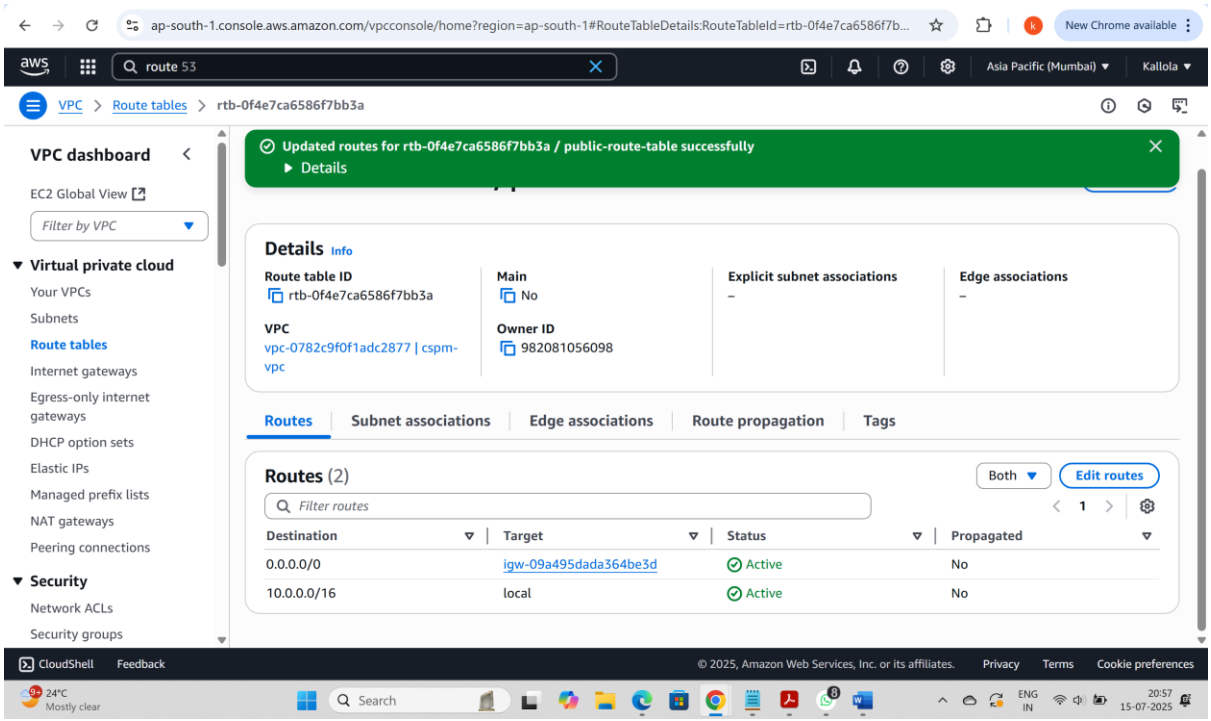




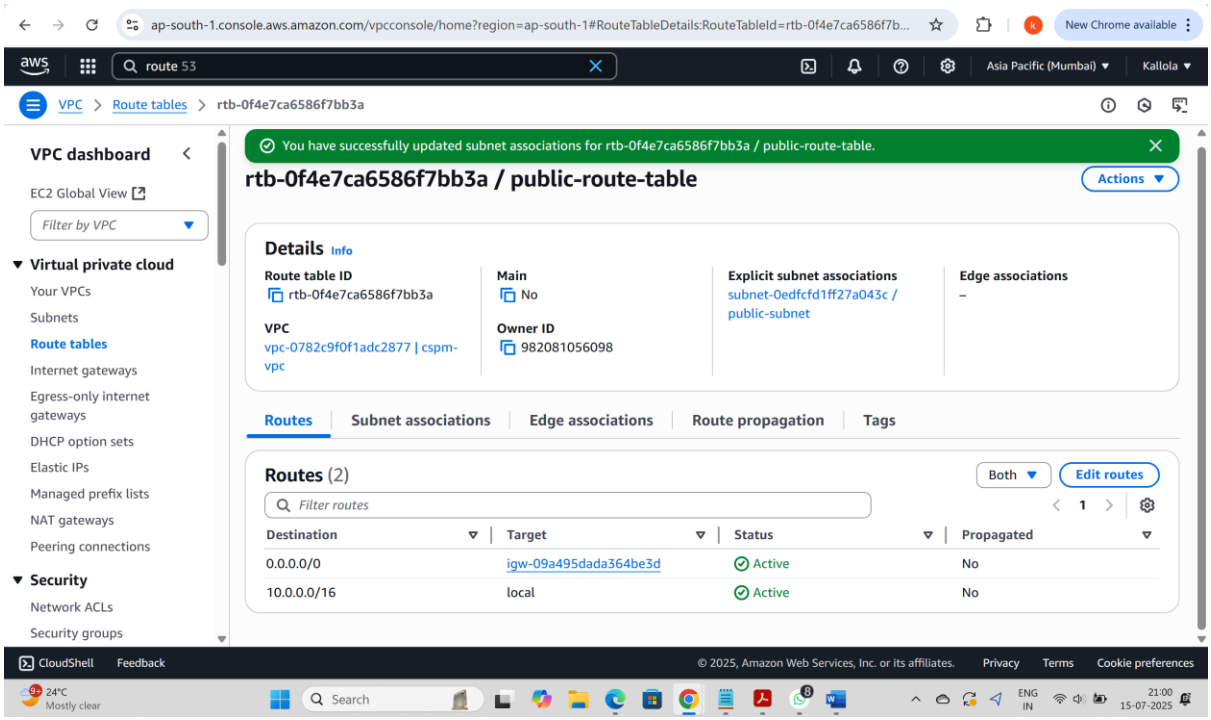

ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#InternetGateway:internetGatewayId=igw-09a495dada...
New Chrome available
Search
[Alt+S]
Asia Pacific (Mumbai)
Kallola
VPC > Internet gateways > igw-09a495dada364be3d
VPC dashboard
EC2 Global View
Filter by VPC
Virtual private cloud
Your VPCs
Subnets
Route tables
Internet gateways
Egress-only internet gateways
DHCP option sets
Elastic IPs
Managed prefix lists
NAT gateways
Peering connections
Security
Network ACLs
Security groups
Internet gateway igw-09a495dada364be3d successfully attached to vpc-0782c9f0f1adc2877
Notifications 0 0 2 0 0
igw-09a495dada364be3d / cspm-igw
Actions
Details Info
Internet gateway ID
igw-09a495dada364be3d
State
Attached
VPC ID
vpc-0782c9f0f1adc2877 | cspm-vpc
Owner
982081056098
Tags
Manage tags
Search tags
Key
Value
Name
cspm-igw
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
24°C
Mostly clear
Search
ENG
IN
20:42
15-07-2025


ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#CreateRouteTable:
New Chrome available
Search
[Alt+S]
Asia Pacific (Mumbai)
Kallola
VPC > Route tables > Create route table
Create route table Info
A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.
Route table settings
Name - optional
Create a tag with a key of 'Name' and a value that you specify.
public-route-table
VPC
The VPC to use for this route table.
vpc-0782c9f0f1adc2877 (cspm-vpc)
Tags
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.
Key
Value - optional
Name
public-route-table
Remove
Add new tag
You can add 49 more tags.
Cancel
Create route table
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences
24°C
Mostly clear
Search
ENG
IN
20:47
15-07-2025

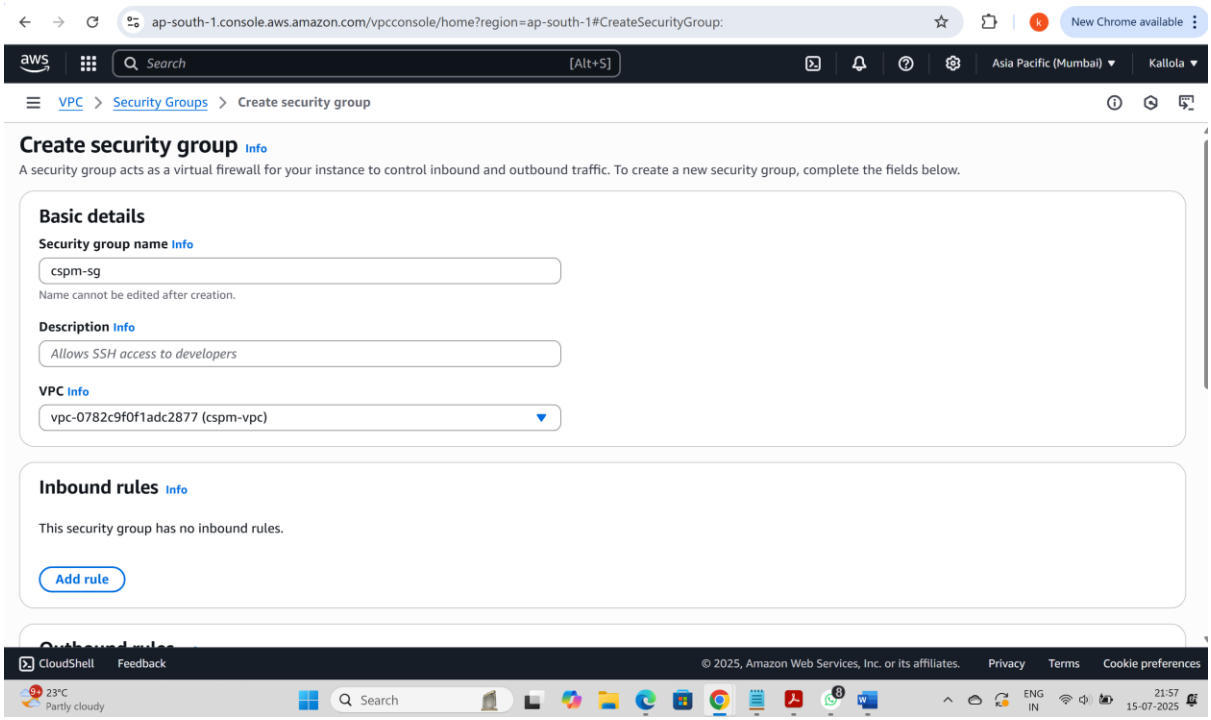


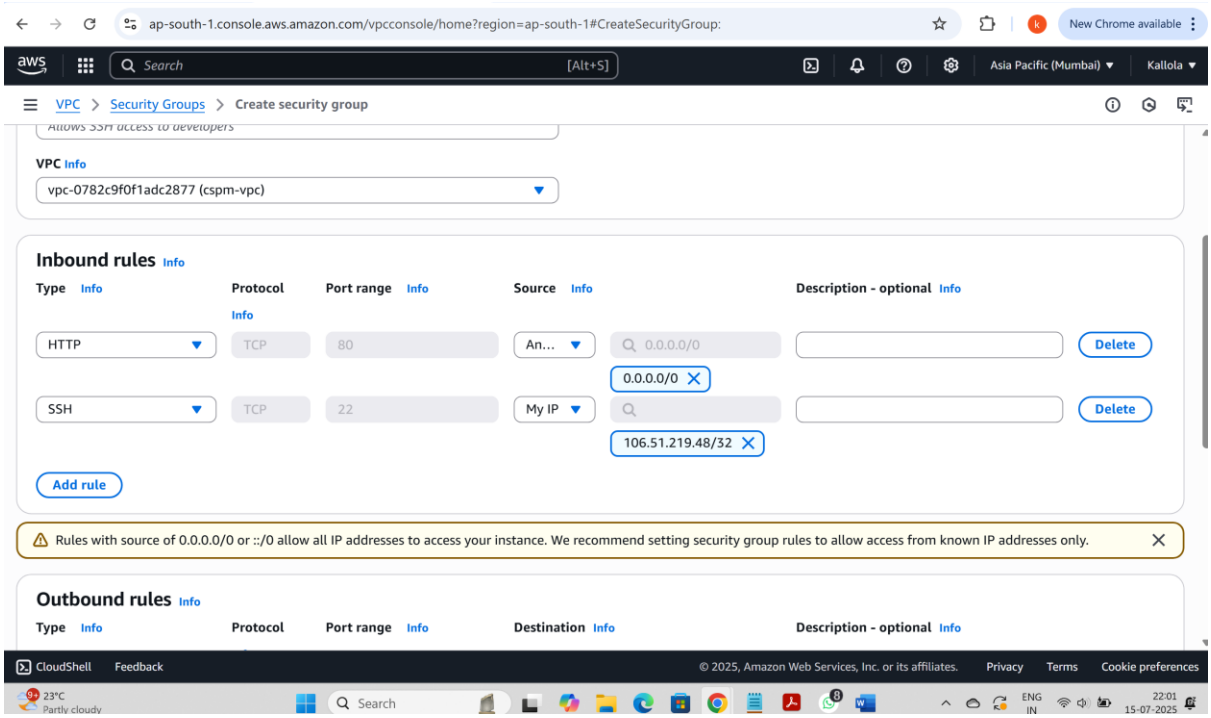


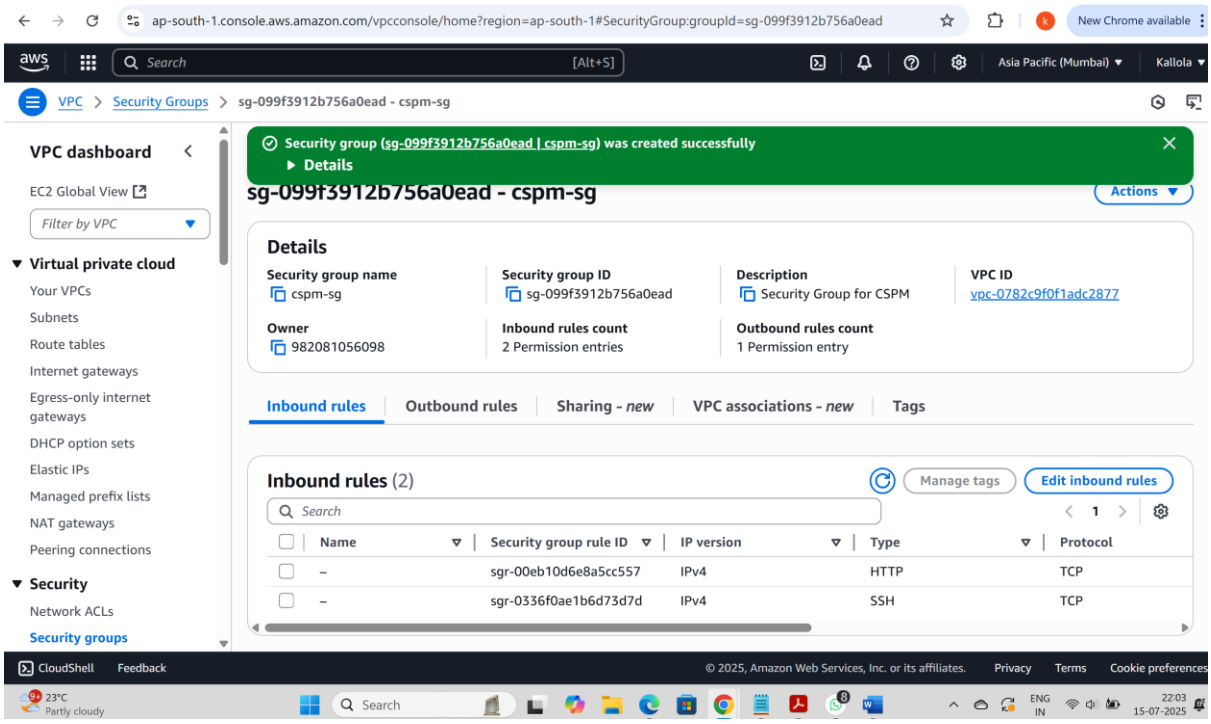
Associate the route table with public-subnet:



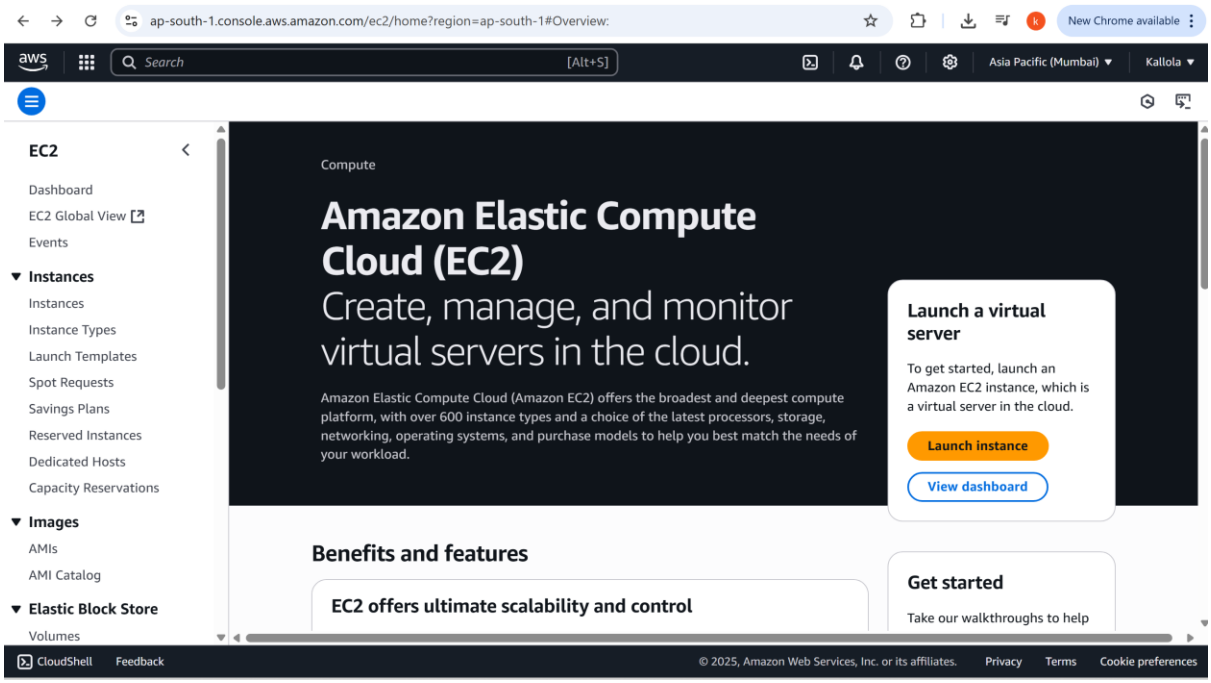
PHASE 4: **Create Security Group**

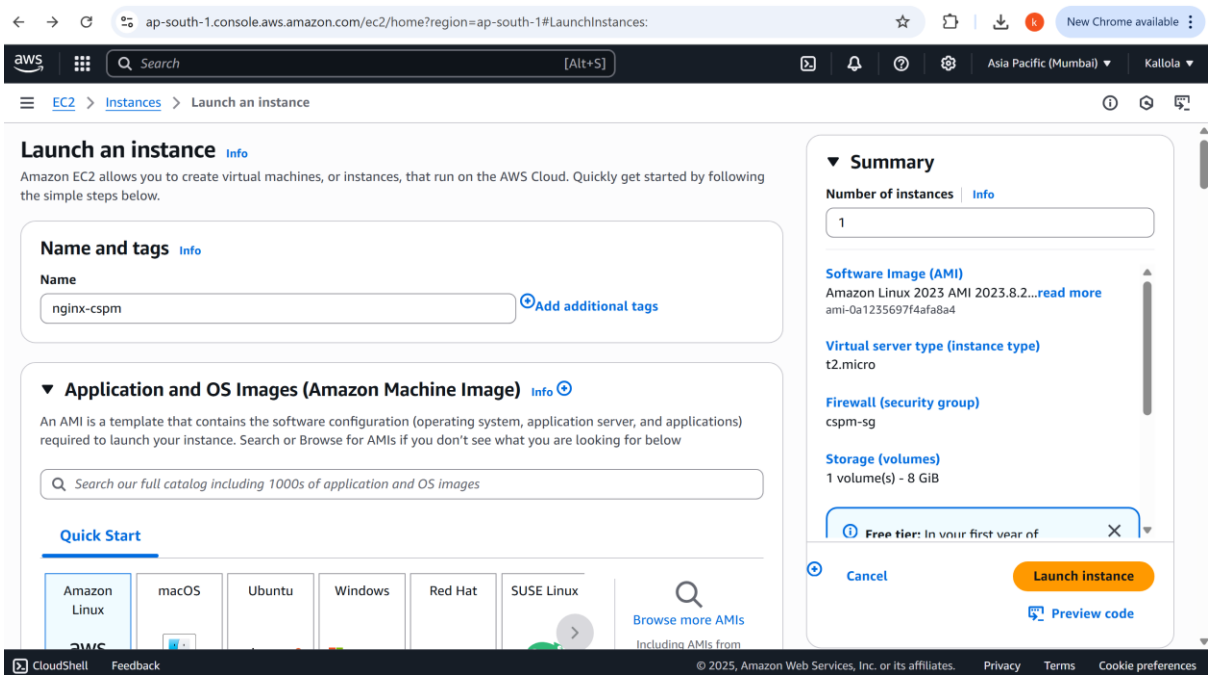


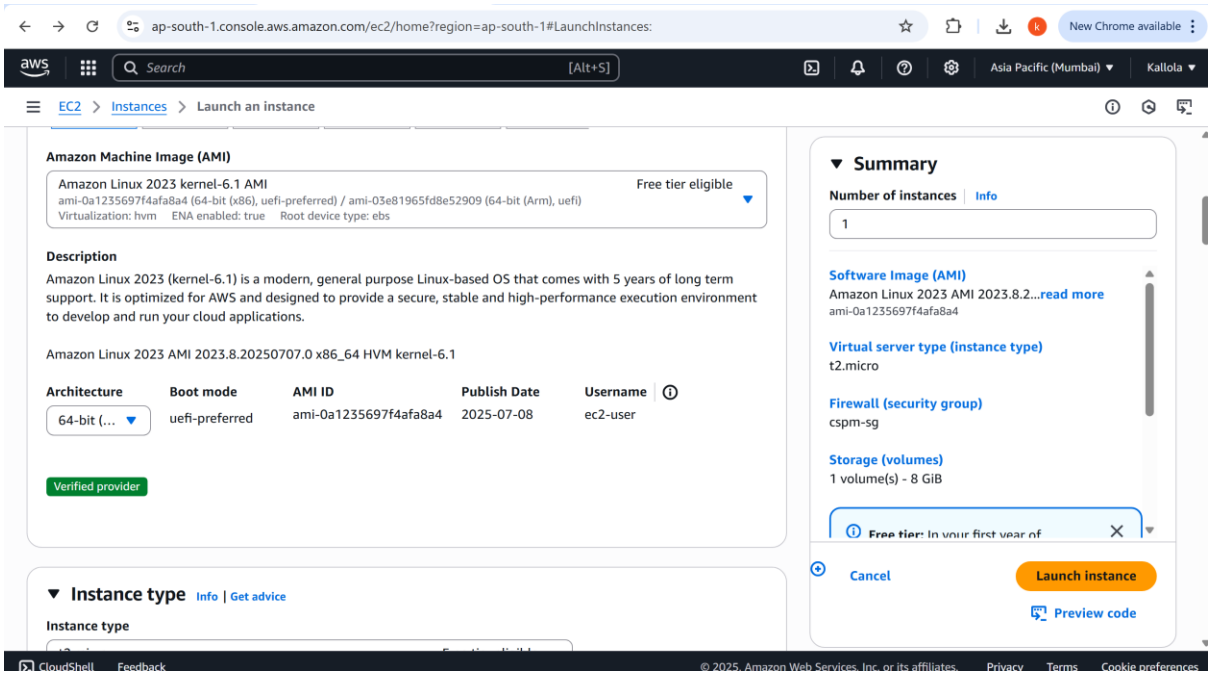


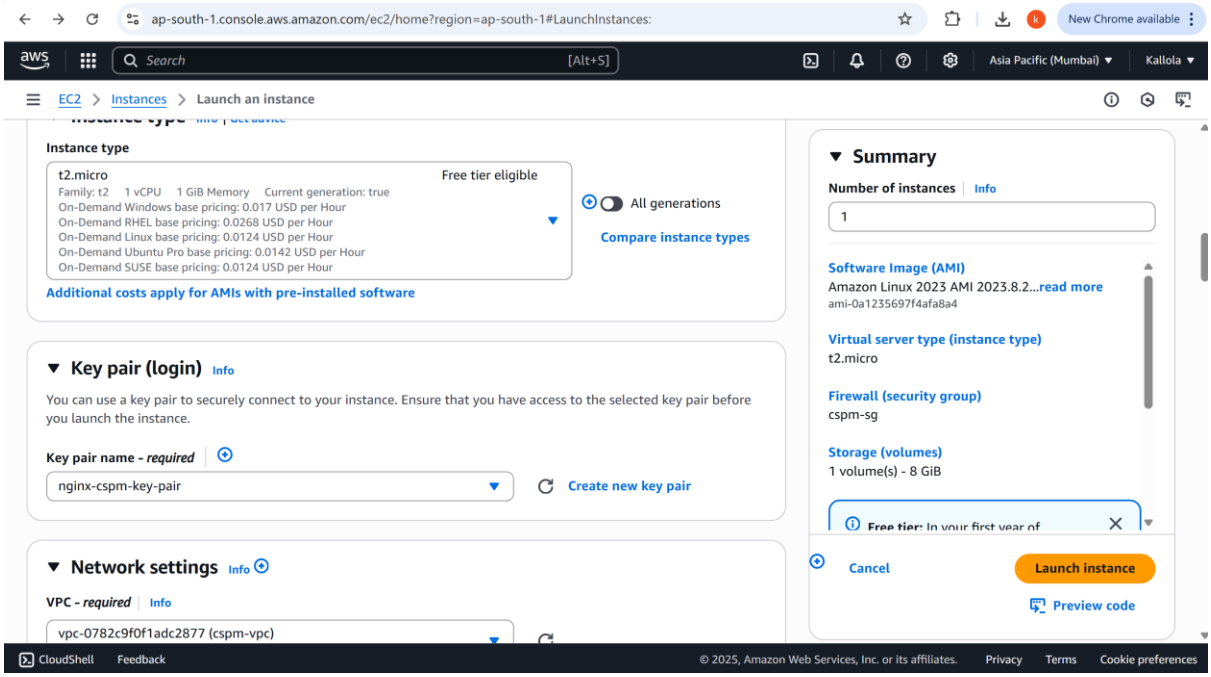


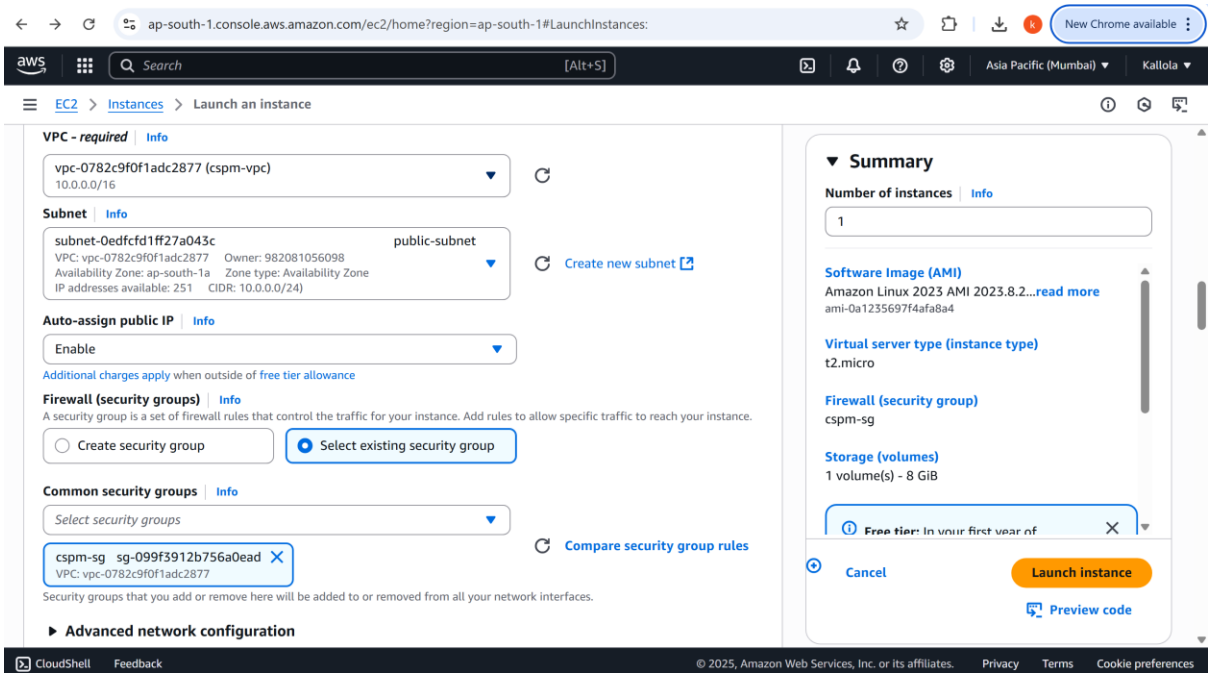
PHASE 5: **Launch EC2 Instance**

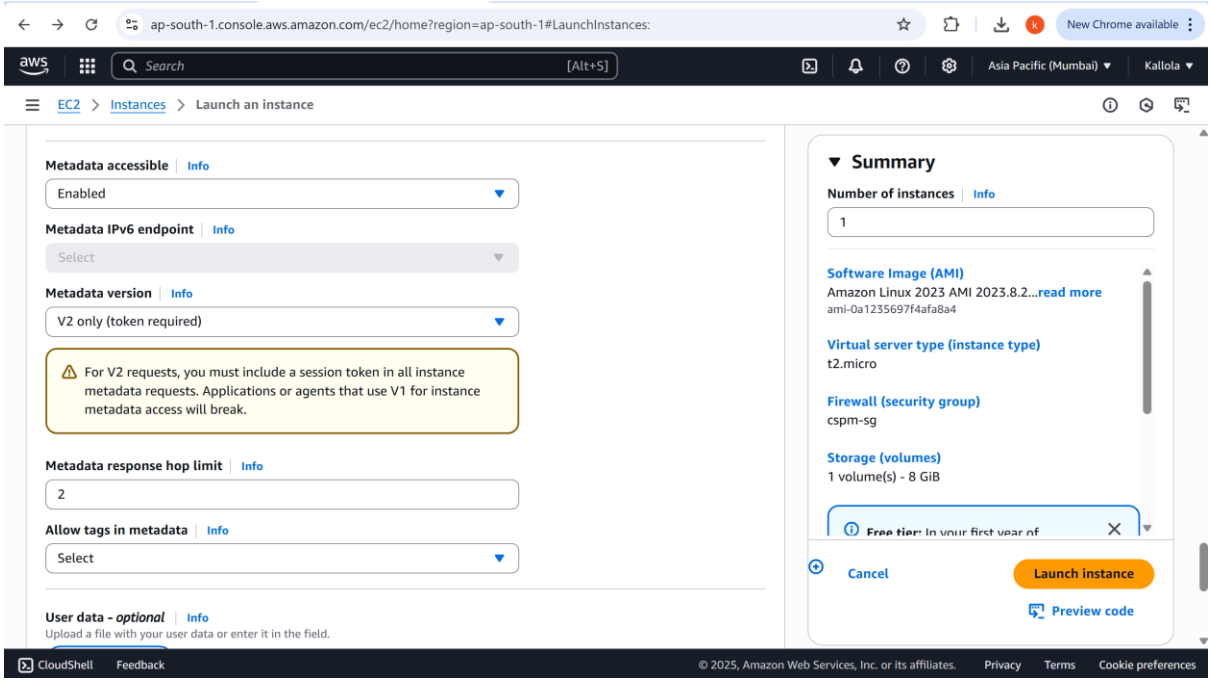

ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#Overview:
New Chrome available
Search
[Alt+S]
Asia Pacific (Mumbai)
Kallola
EC2
Dashboard
EC2 Global View
Events
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations
Images
AMIs
AMI Catalog
Elastic Block Store
Volumes
Compute
Amazon Elastic Compute Cloud (EC2)
Create, manage, and monitor virtual servers in the cloud.
Amazon Elastic Compute Cloud (Amazon EC2) offers the broadest and deepest compute platform, with over 600 instance types and a choice of the latest processors, storage, networking, operating systems, and purchase models to help you best match the needs of your workload.
Launch a virtual server
To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.
Launch instance
View dashboard
Benefits and features
EC2 offers ultimate scalability and control
Get started
Take our walkthroughs to help
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

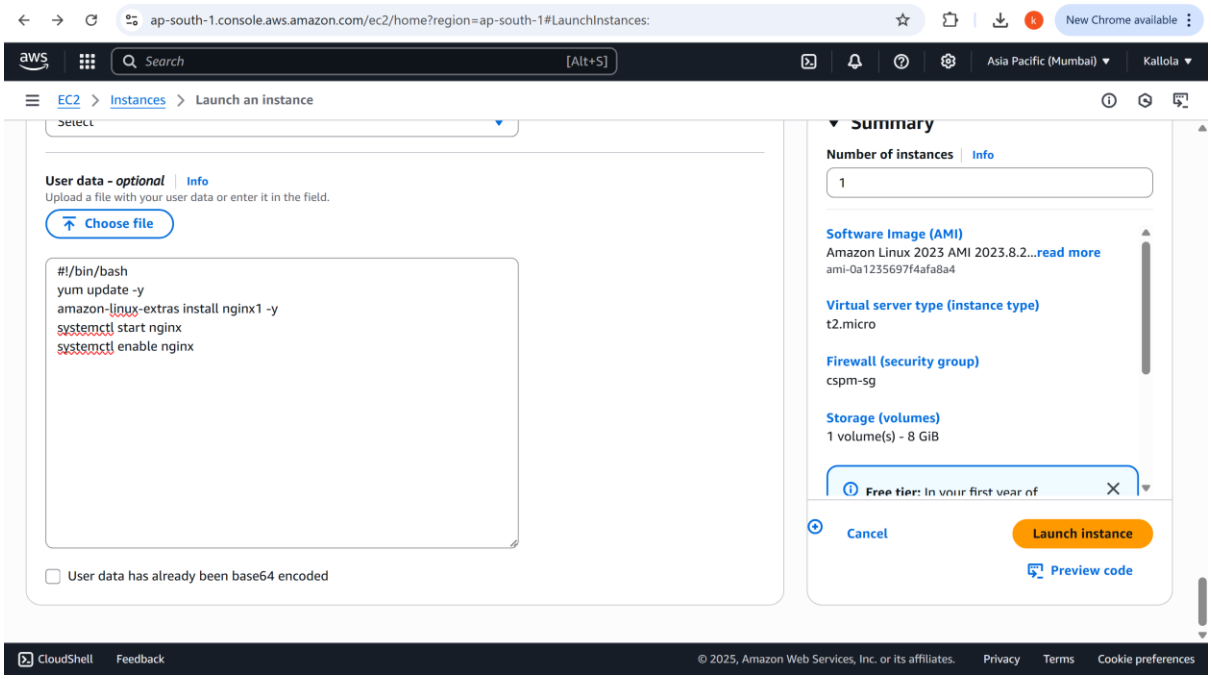

ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#LaunchInstances:
New Chrome available
Search
[Alt+S]
Asia Pacific (Mumbai)
Kallola
EC2 > Instances > Launch an instance
Launch an instance Info
Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.
Name and tags Info
Name
nginx-cspm
Add additional tags
Application and OS Images (Amazon Machine Image) Info
An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below
Search our full catalog including 1000s of application and OS images
Quick Start
Amazon Linux
macOS
Ubuntu
Windows
Red Hat
SUSE Linux
Browse more AMIs
Including AMIs from
Summary
Number of instances Info
1
Software Image (AMI)
Amazon Linux 2023 AMI 2023.8.2...read more
ami-0a1235697f4afa8a4
Virtual server type (instance type)
t2.micro
Firewall (security group)
cspm-sg
Storage (volumes)
1 volume(s) - 8 GiB
Free tier: In your first year of
Cancel
Launch instance
Preview code
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

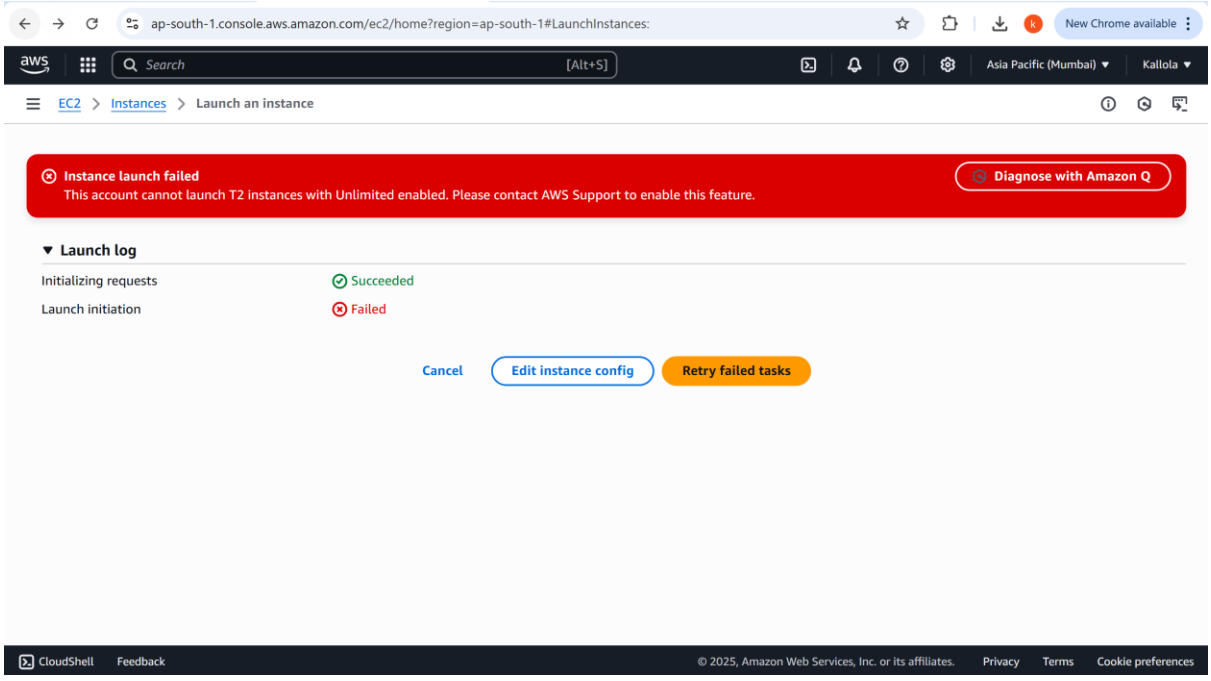

ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#LaunchInstances:
New Chrome available
Search [Alt+S]
Asia Pacific (Mumbai)
Kallola
EC2 > Instances > Launch an instance
Amazon Machine Image (AMI)
Amazon Linux 2023 kernel-6.1 AMI
Free tier eligible
ami-0a1235697f4afa8a4 (64-bit (x86), uefi-preferred) / ami-03e81965fd8e52909 (64-bit (Arm), uefi)
Virtualization: hvm ENA enabled: true Root device type: ebs
Description
Amazon Linux 2023 (kernel-6.1) is a modern, general purpose Linux-based OS that comes with 5 years of long term support. It is optimized for AWS and designed to provide a secure, stable and high-performance execution environment to develop and run your cloud applications.
Amazon Linux 2023 AMI 2023.8.20250707.0 x86_64 HVM kernel-6.1
Architecture
Boot mode
AMI ID
Publish Date
Username
64-bit (...
uefi-preferred
ami-0a1235697f4afa8a4
2025-07-08
ec2-user
Verified provider
Instance type Info | Get advice
Instance type
Summary
Number of instances Info
1
Software Image (AMI)
Amazon Linux 2023 AMI 2023.8.2...read more
ami-0a1235697f4afa8a4
Virtual server type (instance type)
t2.micro
Firewall (security group)
cspm-sg
Storage (volumes)
1 volume(s) - 8 GiB
Free tier: In your first year of
Cancel
Launch instance
Preview code
CloudShell Feedback
© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

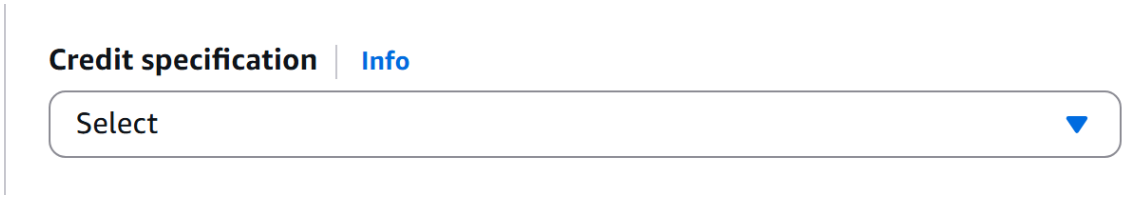

ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#LaunchInstances:
New Chrome available
Search [Alt+S]
Asia Pacific (Mumbai)
Kallola
EC2 > Instances > Launch an instance
Instance type
t2.micro
Free tier eligible
Family: t2 1 vCPU 1 GiB Memory Current generation: true
On-Demand Windows base pricing: 0.017 USD per Hour
On-Demand RHEL base pricing: 0.0268 USD per Hour
On-Demand Linux base pricing: 0.0124 USD per Hour
On-Demand Ubuntu Pro base pricing: 0.0142 USD per Hour
On-Demand SUSE base pricing: 0.0124 USD per Hour
All generations
Compare instance types
Additional costs apply for AMIs with pre-installed software
Key pair (login) Info
You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.
Key pair name - required
nginx-cspm-key-pair
Create new key pair
Network settings Info
VPC - required Info
vpc-0782c9f0f1adc2877 (cspm-vpc)
Summary
Number of instances Info
1
Software Image (AMI)
Amazon Linux 2023 AMI 2023.8.2...read more
ami-0a1235697f4afa8a4
Virtual server type (instance type)
t2.micro
Firewall (security group)
cspm-sg
Storage (volumes)
1 volume(s) - 8 GiB
Free tier: In your first year of
Cancel
Launch instance
Preview code
CloudShell Feedback
© 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

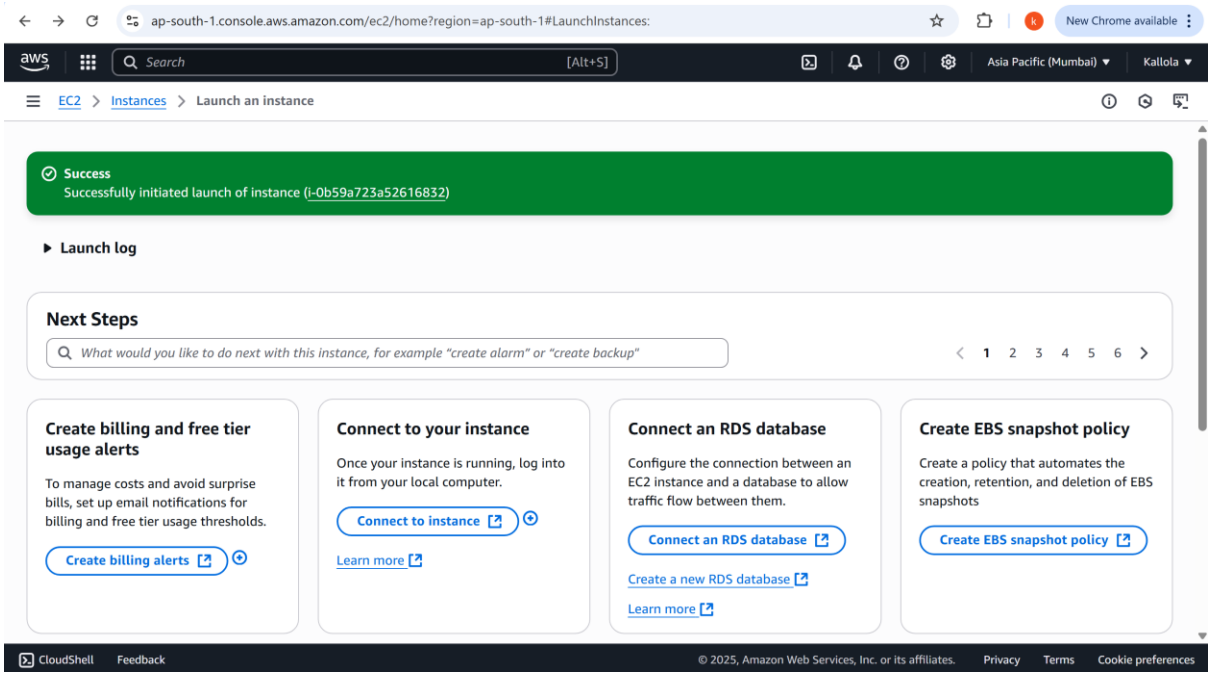

ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#LaunchInstances:
New Chrome available
Search
[Alt+S]
Asia Pacific (Mumbai)
Kallola
EC2 > Instances > Launch an instance
VPC - required | Info
vpc-0782c9f0f1adc2877 (cspm-vpc)
10.0.0.0/16
Subnet | Info
subnet-0edfcfd1ff27a043c public-subnet
VPC: vpc-0782c9f0f1adc2877 Owner: 982081056098
Availability Zone: ap-south-1a Zone type: Availability Zone
IP addresses available: 251 CIDR: 10.0.0.0/24)
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
Common security groups | Info
Select security groups
cspm-sg sg-099f3912b756a0ead
VPC: vpc-0782c9f0f1adc2877
Compare security group rules
Security groups that you add or remove here will be added to or removed from all your network interfaces.
Advanced network configuration
Summary
Number of instances | Info
1
Software Image (AMI)
Amazon Linux 2023 AMI 2023.8.2...read more
ami-0a1235697f4afa8a4
Virtual server type (instance type)
t2.micro
Firewall (security group)
cspm-sg
Storage (volumes)
1 volume(s) - 8 GiB
Free tier: In your first year of
Cancel
Launch instance
Preview code
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

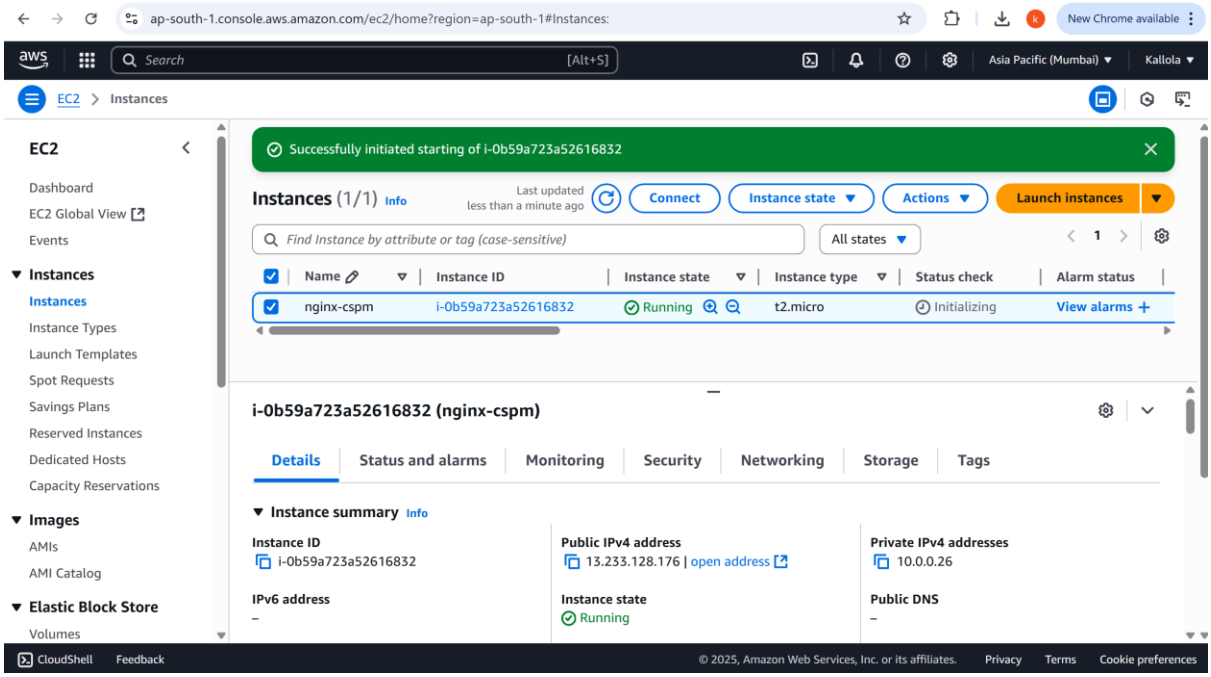

ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#LaunchInstances:
New Chrome available
Search
[Alt+S]
Asia Pacific (Mumbai)
Kallola
EC2 > Instances > Launch an instance
Metadata accessible | Info
Enabled
Metadata IPv6 endpoint | Info
Select
Metadata version | Info
V2 only (token required)
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.
Summary
Number of instances | Info
1
Software Image (AMI)
Amazon Linux 2023 AMI 2023.8.2...read more
ami-0a1235697f4afa8a4
Virtual server type (instance type)
t2.micro
Firewall (security group)
cspm-sg
Storage (volumes)
1 volume(s) - 8 GiB
Free tier: In your first year of
Cancel
Launch instance
Preview code
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#LaunchInstances:
New Chrome available
Search
[Alt+S]
Asia Pacific (Mumbai)
Kallola
EC2 > Instances > Launch an instance
User data - optional | Info
Upload a file with your user data or enter it in the field.
Choose file
#!/bin/bash
yum update -y
amazon-linux-extras install nginx1 -y
systemctl start nginx
systemctl enable nginx
User data has already been base64 encoded
Summary
Number of instances | Info
1
Software Image (AMI)
Amazon Linux 2023 AMI 2023.8.2...read more
ami-0a1235697f4afa8a4
Virtual server type (instance type)
t2.micro
Firewall (security group)
cspm-sg
Storage (volumes)
1 volume(s) - 8 GiB
Free tier: In your first year of
Cancel
Launch instance
Preview code
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#LaunchInstances:
New Chrome available
Search
[Alt+S]
Asia Pacific (Mumbai)
Kallola
EC2 > Instances > Launch an instance
Instance launch failed
This account cannot launch T2 instances with Unlimited enabled. Please contact AWS Support to enable this feature.
Diagnose with Amazon Q
Launch log
Initializing requests
Succeeded
Launch initiation
Failed
Cancel
Edit instance config
Retry failed tasks
CloudShell
Feedback
© 2025, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences


Credit specification | Info
Select





PHASE 6: **Verify Application**

```
Authenticating with public key "Imported-Openssh-Key"

                • MobaXterm Personal Edition v25.2 •
              (SSH client, X server and network tools)

  ▸ SSH session to ec2-user@13.233.128.176
    • Direct SSH      :  ✔
    • SSH compression :  ✔
    • SSH-browser     :  ✔
    • X11-forwarding  :  ✘  (disabled or not supported by server)

  ▸ For more info, ctrl+click on help or visit our website.


A newer release of "Amazon Linux" is available.
  Version 2023.8.20250715:
Run "/usr/bin/dnf check-release-update" for full release and version update info
   ,     #_
   ~\_   ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
[ec2-user@ip-10-0-0-26 ~]$ sudo systemctl status nginx
Unit nginx.service could not be found.
[ec2-user@ip-10-0-0-26 ~]$ sudo yum install nginx -y
Last metadata expiration check: 1 day, 17:54:31 ago on Wed Jul 16 17:57:31 2025.
Dependencies resolved.
================================================================================
 Package                 Architecture   Version                  Repository   Size
================================================================================
Installing:
 nginx                   x86_64         1:1.28.0-1.amzn2023.0.1  amazonlinux  33 k
Installing dependencies:
 generic-logos-httpd     noarch         18.0.0-12.amzn2023.0.3   amazonlinux  19 k
 gperftools-libs         x86_64         2.9.1-1.amzn2023.0.3     amazonlinux 308 k
 libunwind               x86_64         1.4.0-5.amzn2023.0.2     amazonlinux  66 k
 nginx-core              x86_64         1:1.28.0-1.amzn2023.0.1  amazonlinux 669 k
 nginx-filesystem        noarch         1:1.28.0-1.amzn2023.0.1  amazonlinux 9.5 k
```

```
6. 13.233.128.176 (ec2-user) (1)
Running transaction
  Preparing        :                                                        1/1
  Running scriptlet: nginx-filesystem-1:1.28.0-1.amzn2023.0.1.noarch        1/7
  Installing       : nginx-filesystem-1:1.28.0-1.amzn2023.0.1.noarch        1/7
  Installing       : nginx-mimetypes-2.1.49-3.amzn2023.0.3.noarch           2/7
  Installing       : libunwind-1.4.0-5.amzn2023.0.2.x86_64                  3/7
  Installing       : gperftools-libs-2.9.1-1.amzn2023.0.3.x86_64            4/7
  Installing       : nginx-core-1:1.28.0-1.amzn2023.0.1.x86_64              5/7
  Installing       : generic-logos-httpd-18.0.0-12.amzn2023.0.3.noarch      6/7
  Installing       : nginx-1:1.28.0-1.amzn2023.0.1.x86_64                   7/7
  Running scriptlet: nginx-1:1.28.0-1.amzn2023.0.1.x86_64                   7/7
  Verifying        : generic-logos-httpd-18.0.0-12.amzn2023.0.3.noarch      1/7
  Verifying        : gperftools-libs-2.9.1-1.amzn2023.0.3.x86_64            2/7
  Verifying        : libunwind-1.4.0-5.amzn2023.0.2.x86_64                  3/7
  Verifying        : nginx-1:1.28.0-1.amzn2023.0.1.x86_64                   4/7
  Verifying        : nginx-core-1:1.28.0-1.amzn2023.0.1.x86_64              5/7
  Verifying        : nginx-filesystem-1:1.28.0-1.amzn2023.0.1.noarch        6/7
  Verifying        : nginx-mimetypes-2.1.49-3.amzn2023.0.3.noarch           7/7
================================================================================
WARNING:
  A newer release of "Amazon Linux" is available.

  Available Versions:

  Version 2023.8.20250715:
    Run the following command to upgrade to 2023.8.20250715:

      dnf upgrade --releasever=2023.8.20250715

    Release notes:
     https://docs.aws.amazon.com/linux/al2023/release-notes/relnotes-2023.8.20250715.html

================================================================================

Installed:
  generic-logos-httpd-18.0.0-12.amzn2023.0.3.noarch  gperftools-libs-2.9.1-1.amzn2023.0.3.x86_64  libunwind-1.4.0-5.amzn2023.0.2.x86_64
  nginx-1:1.28.0-1.amzn2023.0.1.x86_64               nginx-core-1:1.28.0-1.amzn2023.0.1.x86_64    nginx-filesystem-1:1.28.0-1.amzn2023.0.1.noarch
  nginx-mimetypes-2.1.49-3.amzn2023.0.3.noarch

Complete!
[ec2-user@ip-10-0-0-26 ~]$ sudo systemctl start nginx
[ec2-user@ip-10-0-0-26 ~]$ sudo systemctl enable nginx
Created symlink /etc/systemd/system/multi-user.target.wants/nginx.service → /usr/lib/systemd/system/nginx.service.
[ec2-user@ip-10-0-0-26 ~]$
```

So NGINX is installed and running:-

```
[ec2-user@ip-10-0-0-26 ~]$ sudo systemctl status nginx
● nginx.service - The nginx HTTP and reverse proxy server
     Loaded: loaded (/usr/lib/systemd/system/nginx.service; enabled; preset: disabled)
     Active: active (running) since Fri 2025-07-18 11:54:12 UTC; 10min ago
   Main PID: 34839 (nginx)
      Tasks: 2 (limit: 1111)
     Memory: 2.5M
        CPU: 61ms
     CGroup: /system.slice/nginx.service
             ├─34839 "nginx: master process /usr/sbin/nginx"
             └─34840 "nginx: worker process"

Jul 18 11:54:11 ip-10-0-0-26.ap-south-1.compute.internal systemd[1]: Starting nginx.service - The nginx HTTP and reverse proxy server...
Jul 18 11:54:11 ip-10-0-0-26.ap-south-1.compute.internal nginx[34810]: nginx: the configuration file /etc/nginx/nginx.conf syntax is ok
Jul 18 11:54:11 ip-10-0-0-26.ap-south-1.compute.internal nginx[34810]: nginx: configuration file /etc/nginx/nginx.conf test is successful
Jul 18 11:54:12 ip-10-0-0-26.ap-south-1.compute.internal systemd[1]: Started nginx.service - The nginx HTTP and reverse proxy server.
[ec2-user@ip-10-0-0-26 ~]$
```

PHASE 7: **Run CSPM Scanner**

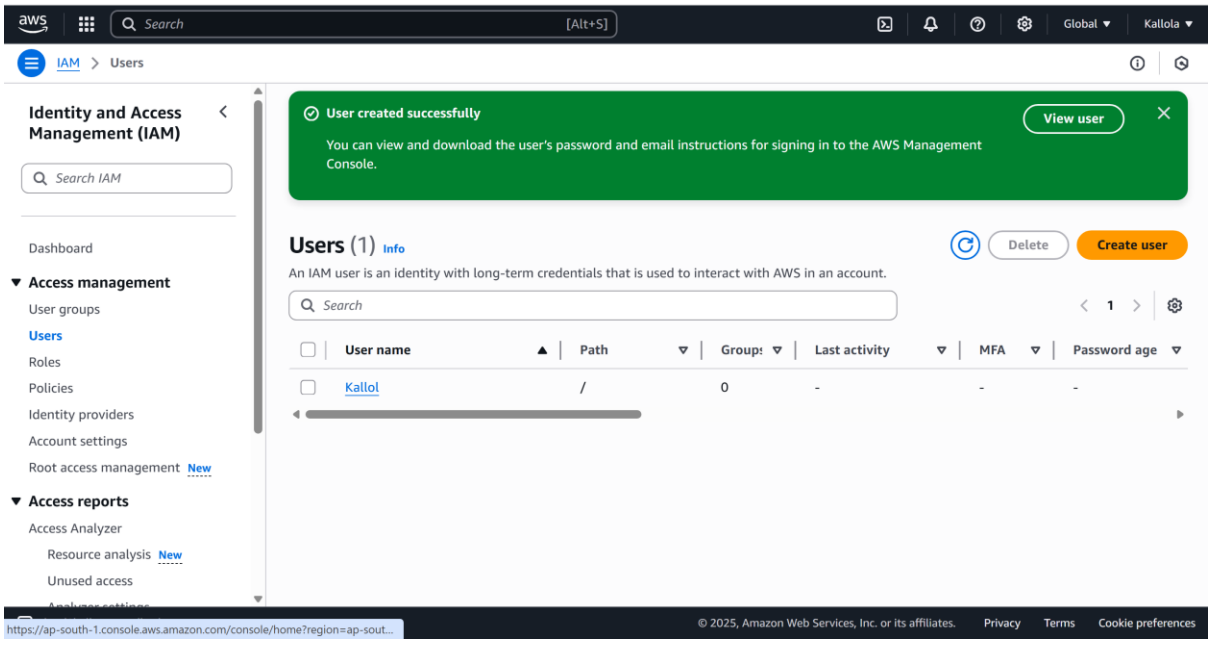
Prowler in your AWS account using CLI

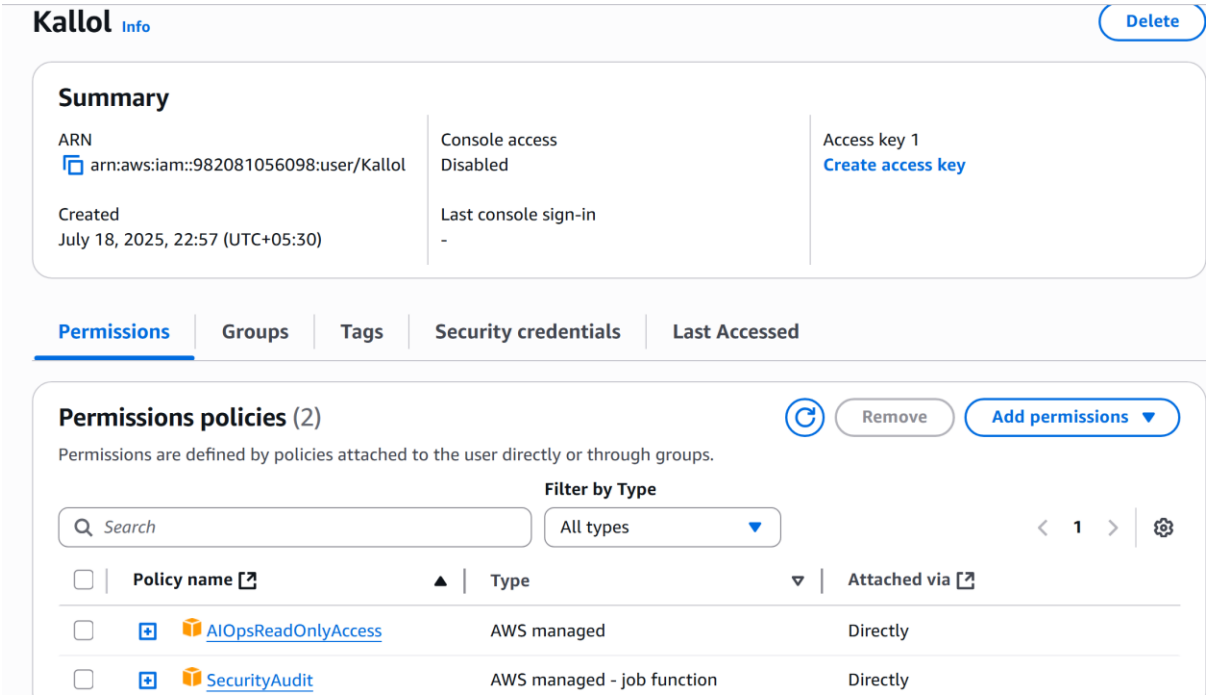
Prowler audits your AWS environment against:

- CIS AWS Foundations Benchmark
- AWS Well-Architected Framework
- GDPR, HIPAA, PCI-DSS, ISO 27001, and more

It checks for issues in IAM, S3, CloudTrail, GuardDuty, Config, and others.

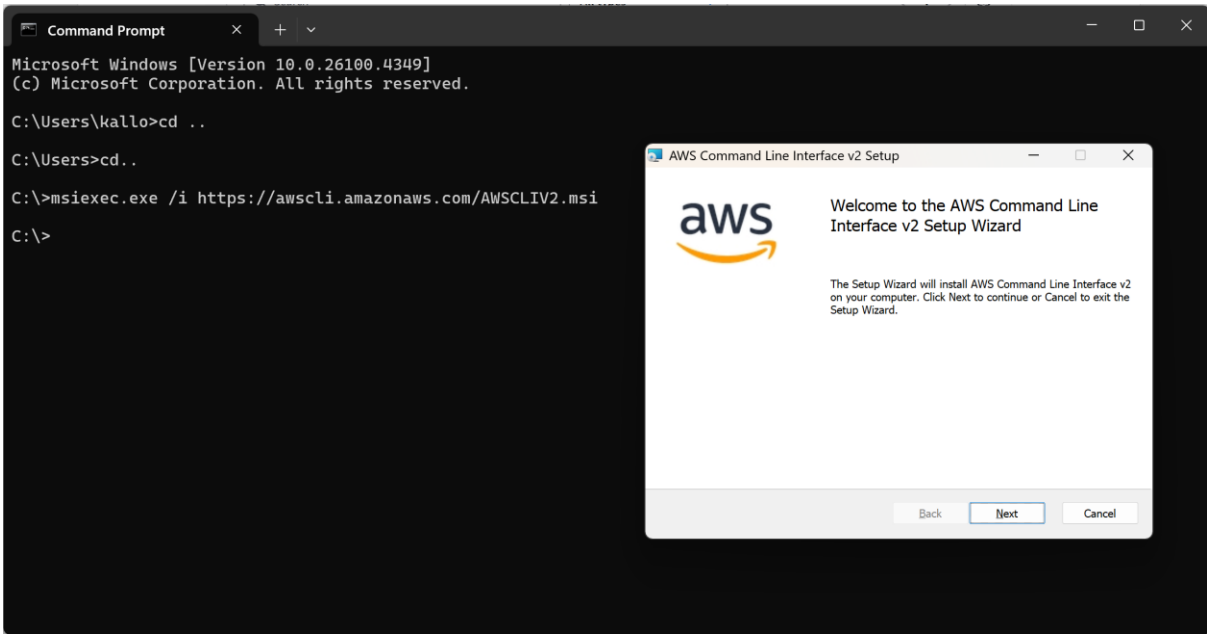
1.Create one IAM user to access aws services and attach SecurityAudit & ReadOnlyAccess policies.

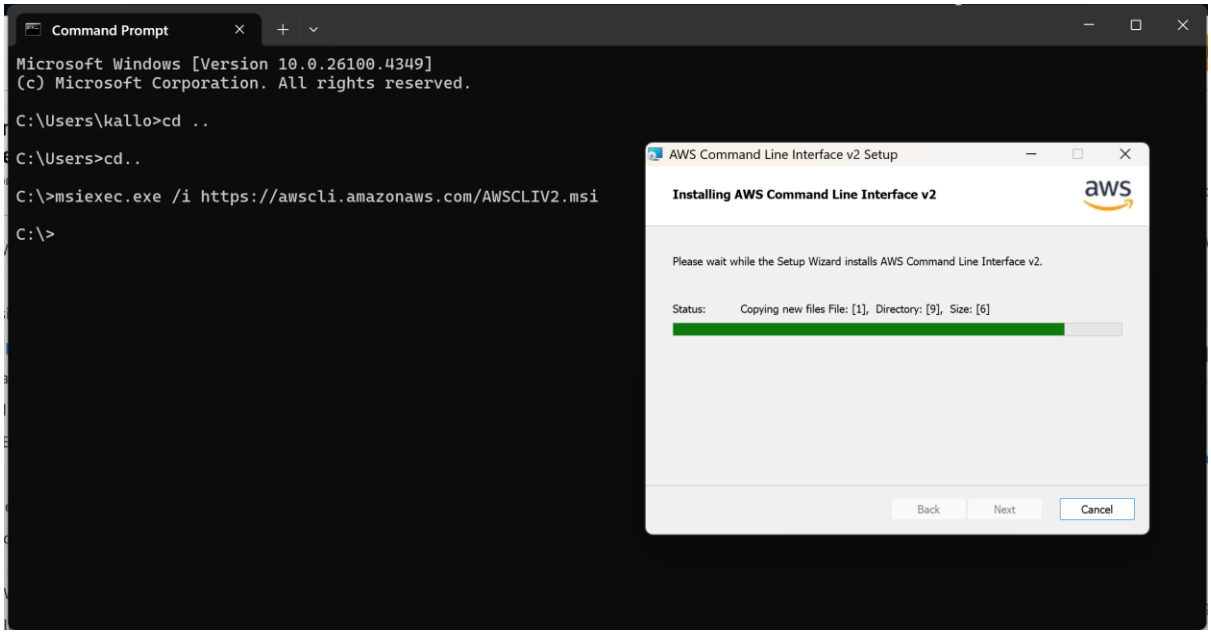




Create access key & download access key & secret key.

2. Install & configure AWS CLI on your laptop.



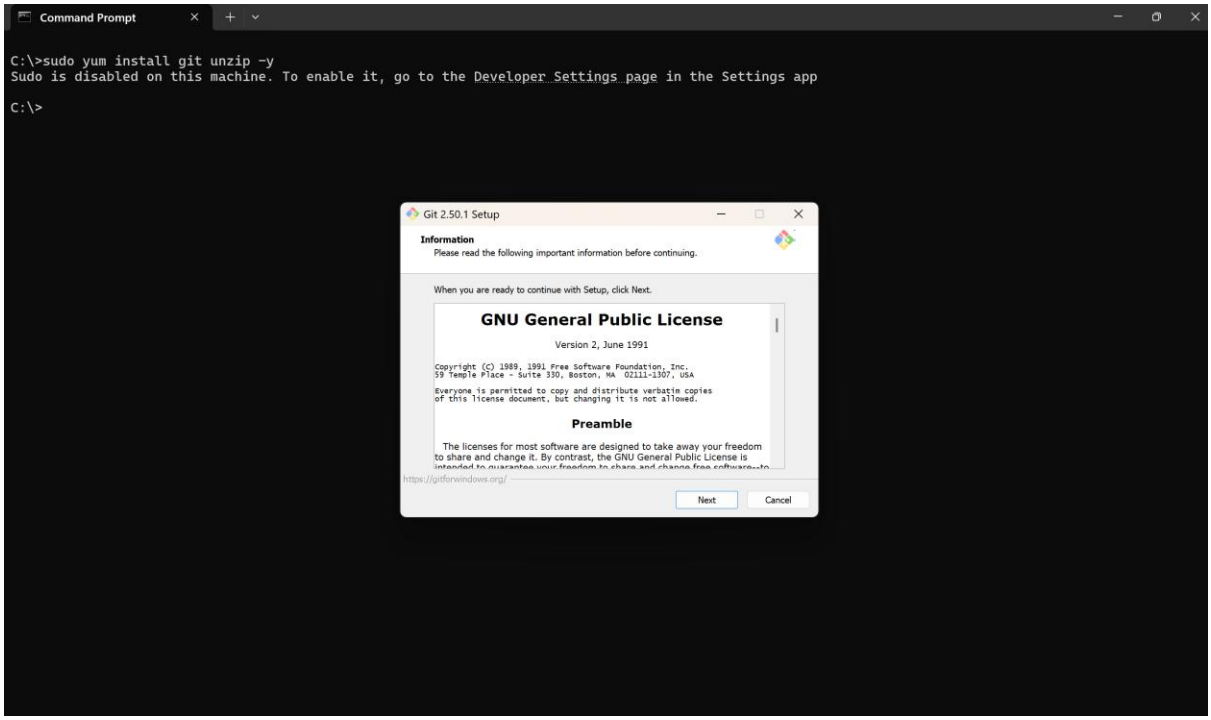



```
C:\>aws --version
aws-cli/2.27.54 Python/3.13.4 Windows/11 exe/AMD64
```

Once finished, you have to configure it.

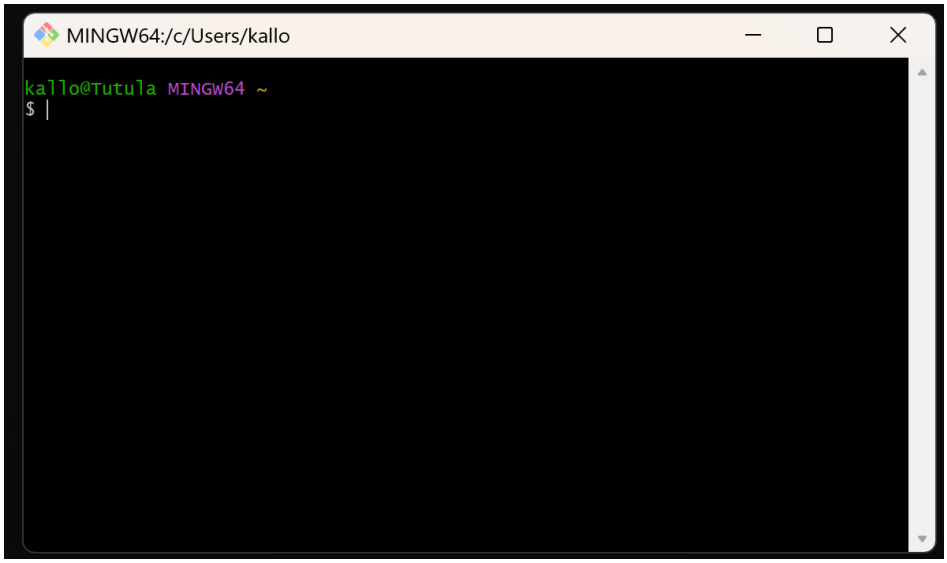
```
C:\>aws configure
AWS Access Key ID [None]: AKIA6JKEXVVRJMH4WKUJ
AWS Secret Access Key [None]: 0i2LarMZQUJ6nFzxwoqbwsi9DbNZBA5N1Y3sHjXA
Default region name [None]: ap-south-1
Default output format [None]: JSON

C:\>
```

3.Git and unzip are installed on your local machine or EC2:



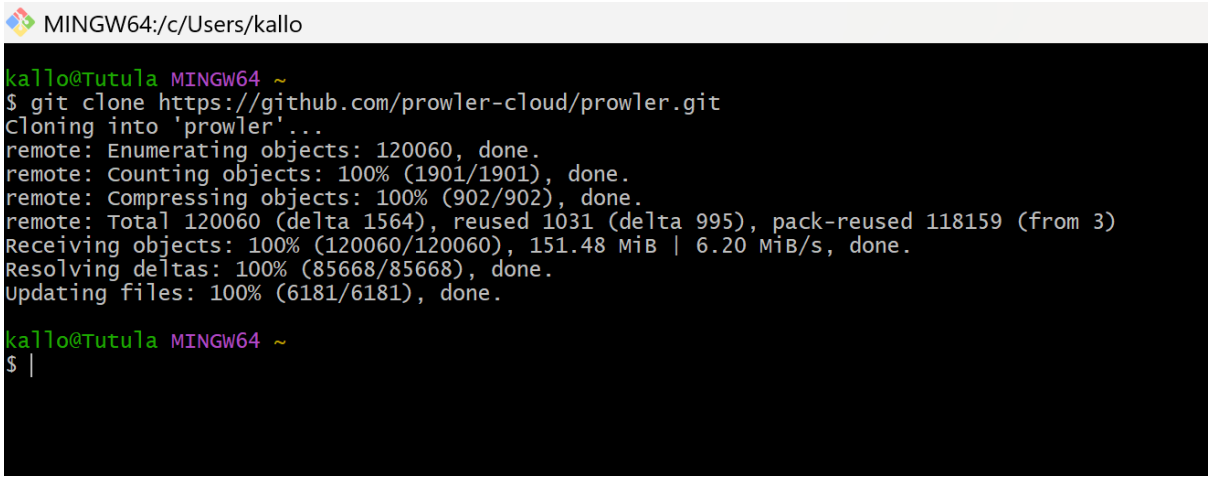
Once finished, Click the Windows Start button, Search for "Git Bash" or "git".

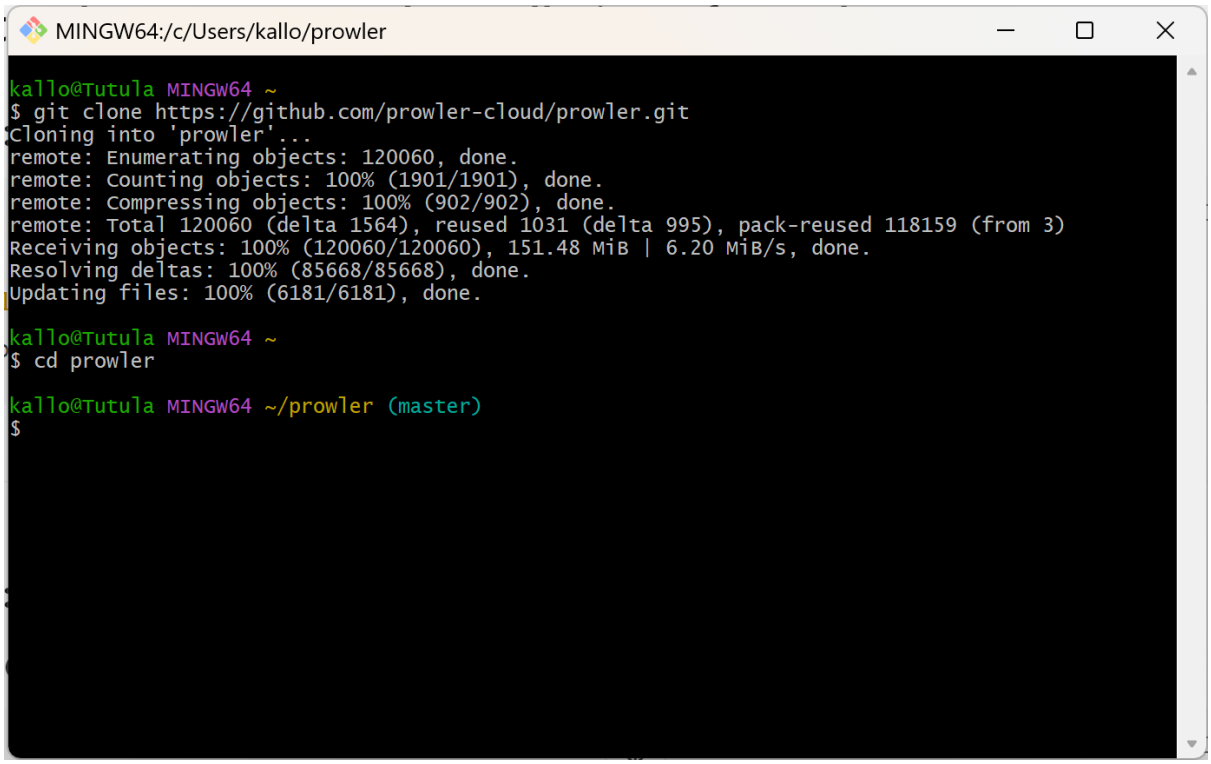
Click on the "Git Bash" application icon to launch it.



Prowler Installation & Run:

Step 1: Clone the Prowler repo





Step 2: Run basic audit

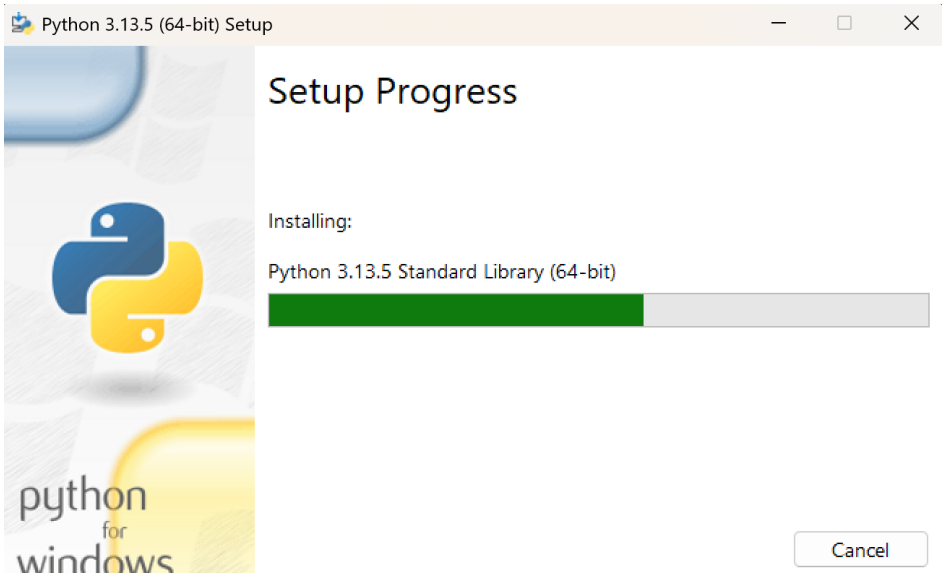
Run the CIS benchmark scan:

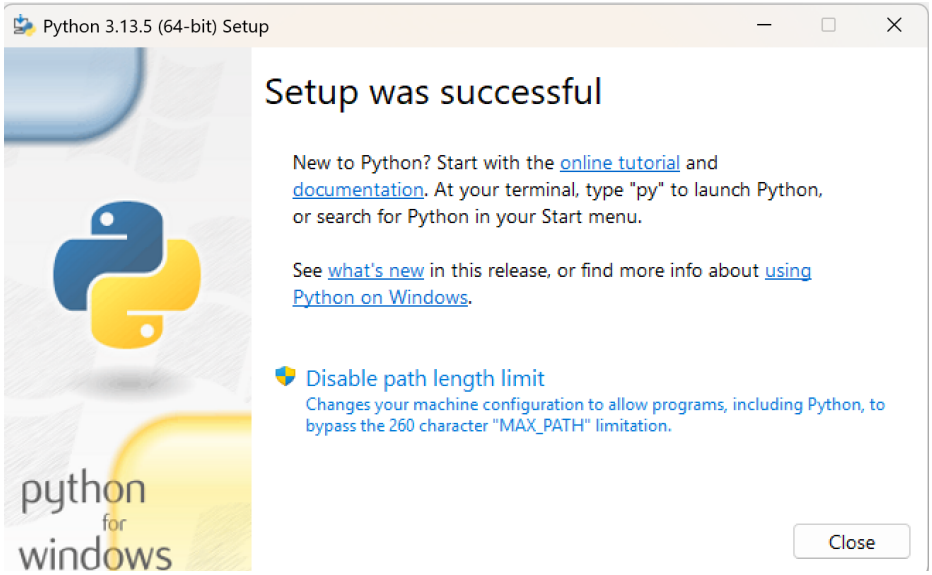
Its not working as the new prowler is python based, hence I have to install python.

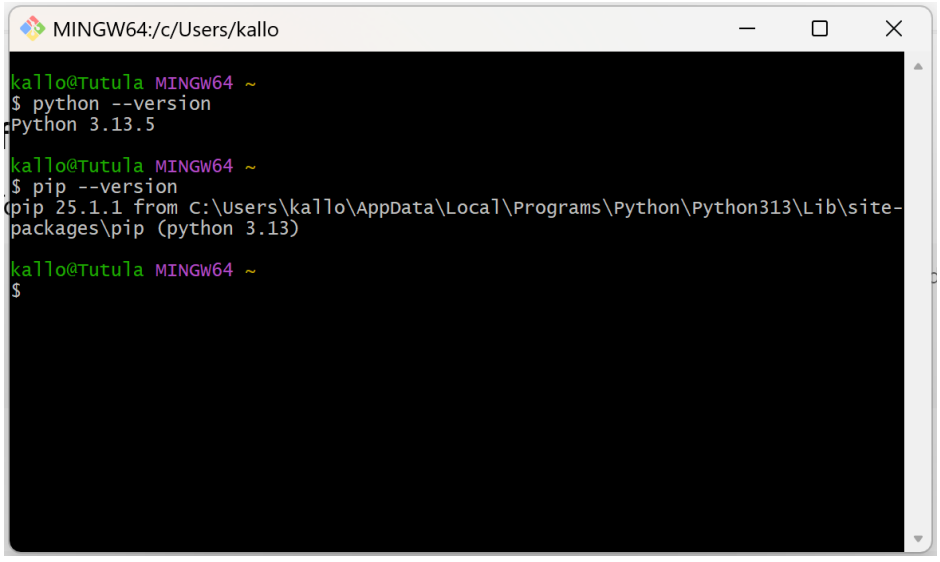
Download and install latest python from https://www.python.org/downloads/windows/

(While installing, **Check the box**: **Add Python to PATH** without fail)

I have selected both the checkboxes & selected install option (ignored custom option)


Python 3.13.5 (64-bit) Setup
Setup Progress
Installing:
Python 3.13.5 Standard Library (64-bit)
Cancel
python
for
windows


Python 3.13.5 (64-bit) Setup
Setup was successful
New to Python? Start with the online tutorial and documentation. At your terminal, type "py" to launch Python, or search for Python in your Start menu.
See what's new in this release, or find more info about using Python on Windows.
Disable path length limit
Changes your machine configuration to allow programs, including Python, to bypass the 260 character "MAX_PATH" limitation.
Close
python
for
windows


MINGW64:/c/Users/kallo
kallo@Tutula MINGW64 ~
$ python --version
Python 3.13.5
kallo@Tutula MINGW64 ~
$ pip --version
pip 25.1.1 from C:\Users\kallo\AppData\Local\Programs\Python\Python313\Lib\site-packages\pip (python 3.13)
kallo@Tutula MINGW64 ~
$

Go to prowler folder

```
kallo@Tutula MINGW64 ~/prowler (master)
$ ll
total 571
-rw-r--r-- 1 kallo 197609   3496 Jul 19 01:02 CODE_OF_CONDUCT.md
-rw-r--r-- 1 kallo 197609    440 Jul 19 01:02 CONTRIBUTING.md
-rw-r--r-- 1 kallo 197609   2380 Jul 19 01:02 Dockerfile
-rw-r--r-- 1 kallo 197609  11549 Jul 19 01:02 LICENSE
-rw-r--r-- 1 kallo 197609   1309 Jul 19 01:02 Makefile
-rw-r--r-- 1 kallo 197609  15246 Jul 19 01:02 README.md
-rw-r--r-- 1 kallo 197609   1709 Jul 19 01:02 SECURITY.md
drwxr-xr-x 1 kallo 197609      0 Jul 19 01:02 api/
-rw-r--r-- 1 kallo 197609    236 Jul 19 01:02 codecov.yml
drwxr-xr-x 1 kallo 197609      0 Jul 19 01:02 contrib/
drwxr-xr-x 1 kallo 197609      0 Jul 19 01:02 dashboard/
-rw-r--r-- 1 kallo 197609   2922 Jul 19 01:02 docker-compose-dev.yml
-rw-r--r-- 1 kallo 197609   2413 Jul 19 01:02 docker-compose.yml
drwxr-xr-x 1 kallo 197609      0 Jul 19 01:02 docs/
drwxr-xr-x 1 kallo 197609      0 Jul 19 01:02 examples/
drwxr-xr-x 1 kallo 197609      0 Jul 19 01:02 kubernetes/
-rw-r--r-- 1 kallo 197609   8400 Jul 19 01:02 mkdocs.yml
drwxr-xr-x 1 kallo 197609      0 Jul 19 01:02 permissions/
-rw-r--r-- 1 kallo 197609 461346 Jul 19 01:02 poetry.lock
drwxr-xr-x 1 kallo 197609      0 Jul 19 13:11 prowler/
-rwxr-xr-x 1 kallo 197609    131 Jul 19 01:02 prowler-cli.py*
-rw-r--r-- 1 kallo 197609   4338 Jul 19 01:02 pyproject.toml
drwxr-xr-x 1 kallo 197609      0 Jul 19 01:02 tests/
drwxr-xr-x 1 kallo 197609      0 Jul 19 01:02 ui/
drwxr-xr-x 1 kallo 197609      0 Jul 19 01:02 util/

kallo@Tutula MINGW64 ~/prowler (master)
$ pwd
/c/Users/kallo/prowler
```

Now **Install Poetry:**

curl -sSL https://install.python-poetry.org | python –

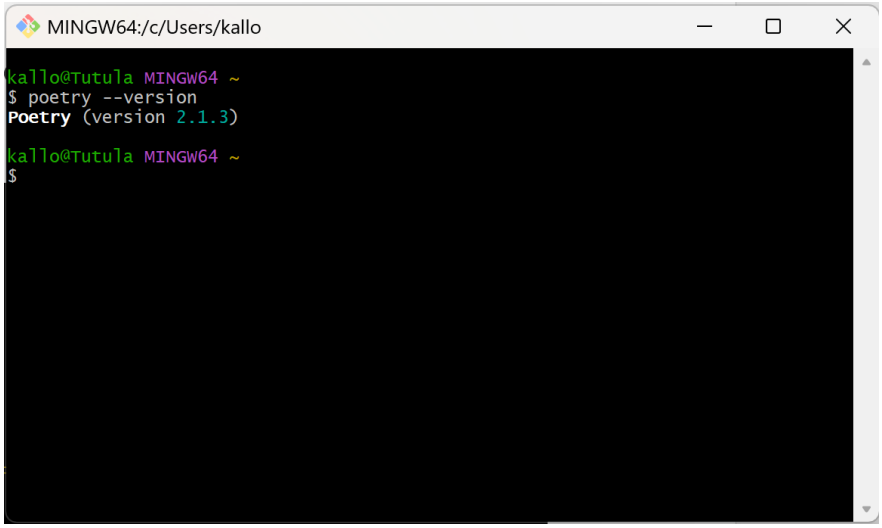
This tool manages Python dependencies.

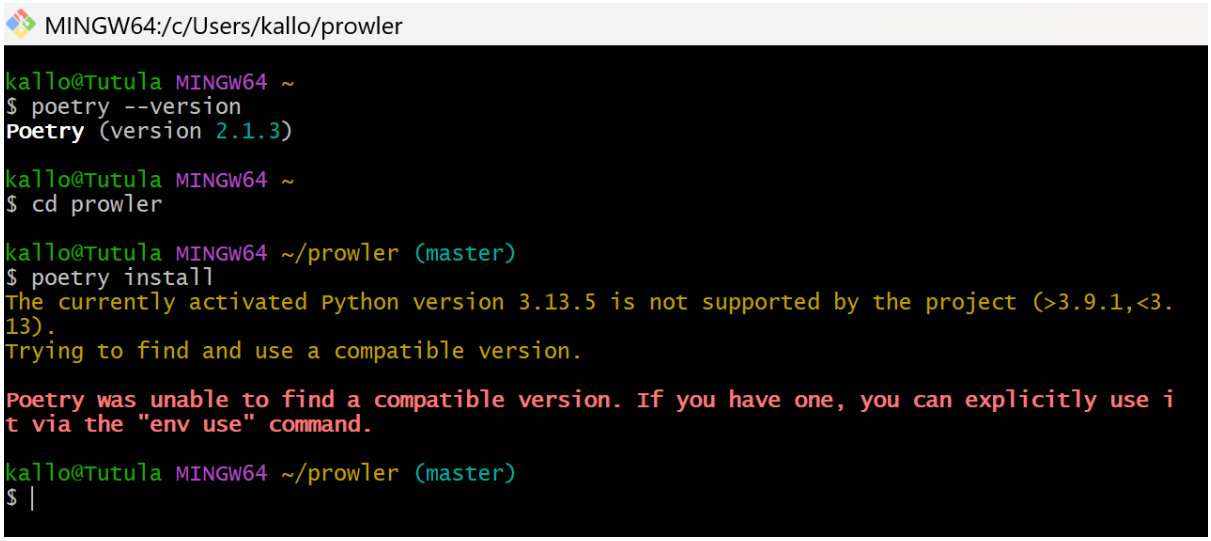
```
kallo@Tutula MINGW64 ~/prowler (master)
$ curl -sSL https://install.python-poetry.org | python -
Retrieving Poetry metadata

# Welcome to Poetry!

This will download and install the latest version of Poetry,
a dependency and package manager for Python.

It will add the `poetry` command to Poetry's bin directory, located at:

C:\Users\kallo\AppData\Roaming\Python\Scripts

You can uninstall at any time by executing this script with the --uninstall option,
and these changes will be reverted.

Installing Poetry (2.1.3): Done

Poetry (2.1.3) is installed now. Great!

To get started you need Poetry's bin directory (C:\Users\kallo\AppData\Roaming\Python\Scripts) in your `PATH`
environment variable.

You can choose and execute one of the following commands in PowerShell:

A. Append the bin directory to your user environment variable `PATH`:

```
[Environment]::SetEnvironmentVariable("Path", [Environment]::GetEnvironmentVariable("Path", "User") + ";C:\Users\kallo\AppData\Roaming\Python\Scripts", "User")
```

B. Try to append the bin directory to PATH every when you run PowerShell (>=6 recommended):

```
echo 'if (-not (Get-Command poetry -ErrorAction Ignore)) { $env:Path += ";C:\Users\kallo\AppData\Roaming\Python\Scripts" }' | Out-File -Append $PROFILE
```

Alternatively, you can call Poetry explicitly with `C:\Users\kallo\AppData\Roaming\Python\Scripts\poetry`.

You can test that everything is set up by executing:

`poetry --version`

kallo@Tutula MINGW64 ~/prowler (master)
$
```

Append the bin directory to your user environment variable `PATH`

C:\Users\kallo\AppData\Roaming\Python\Scripts

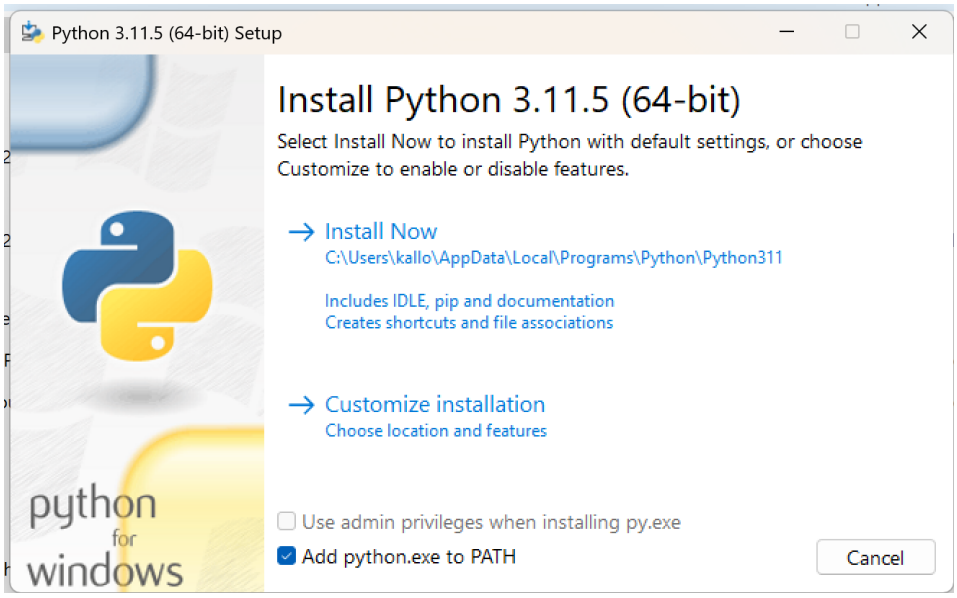
Exit & reconnect Git Bash & run poetry –version

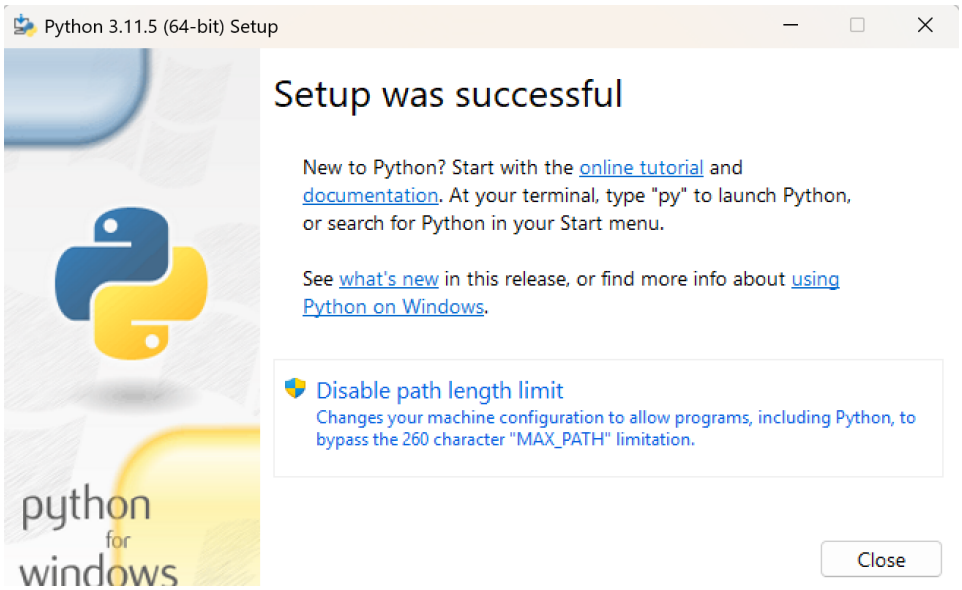


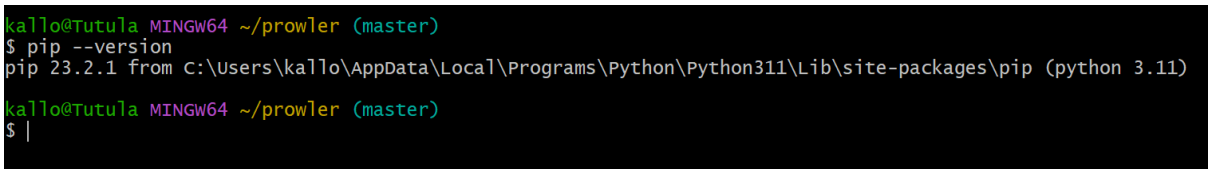


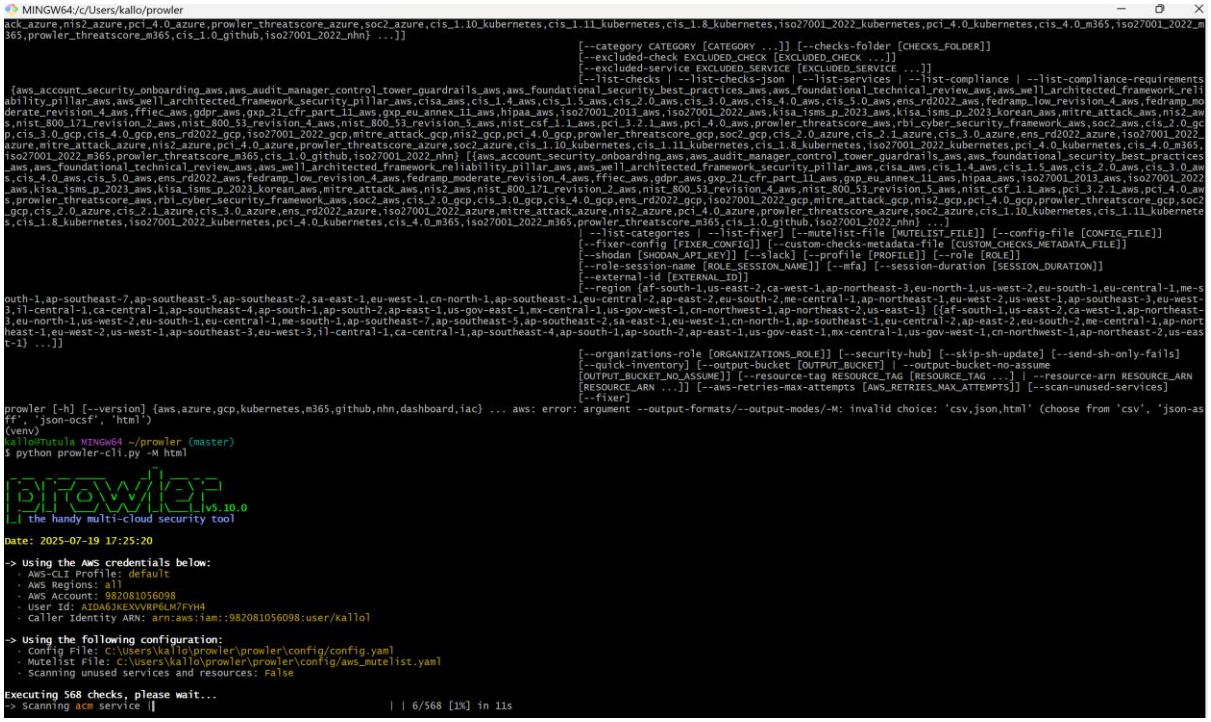
Prowler does not yet support Python 3.13 — it currently supports versions **above 3.9.1 but *below* 3.13**, such as **Python 3.10 or 3.11**, which are stable and widely used.

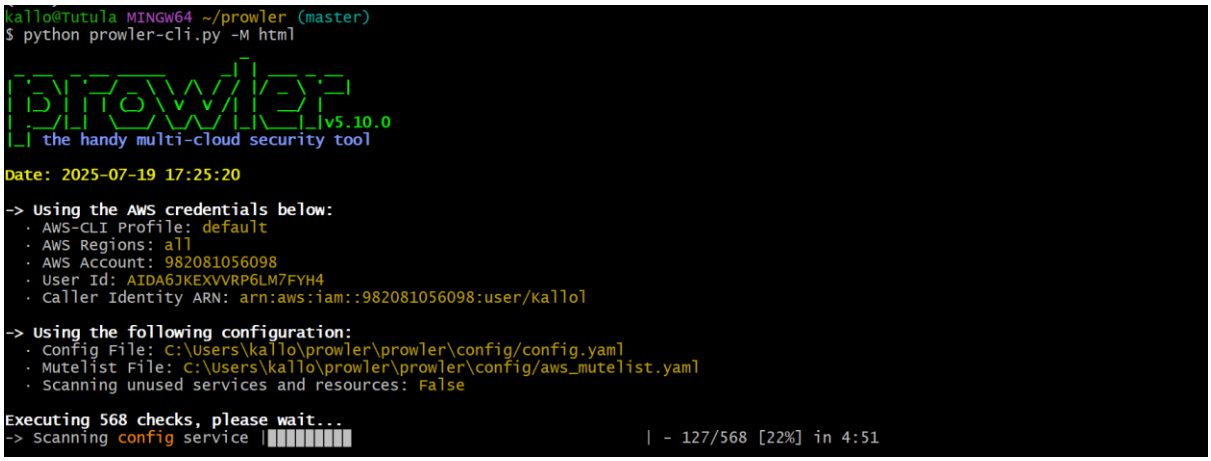
So now we have to install python 3.11.5

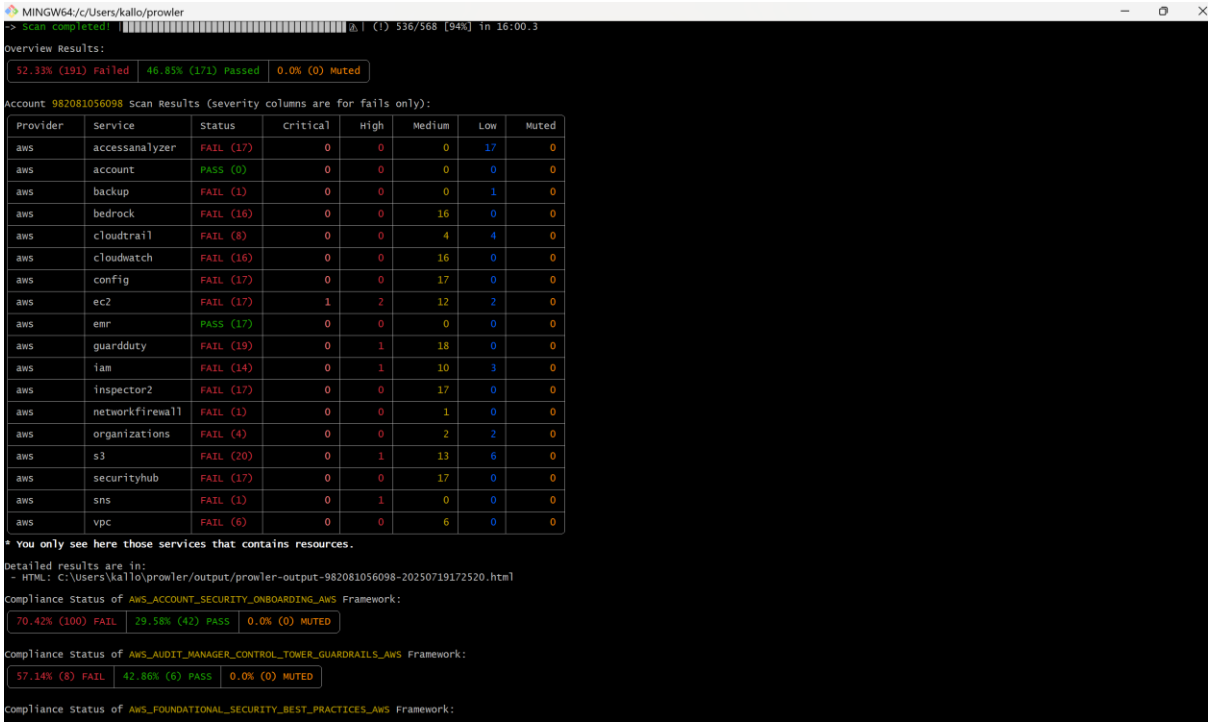


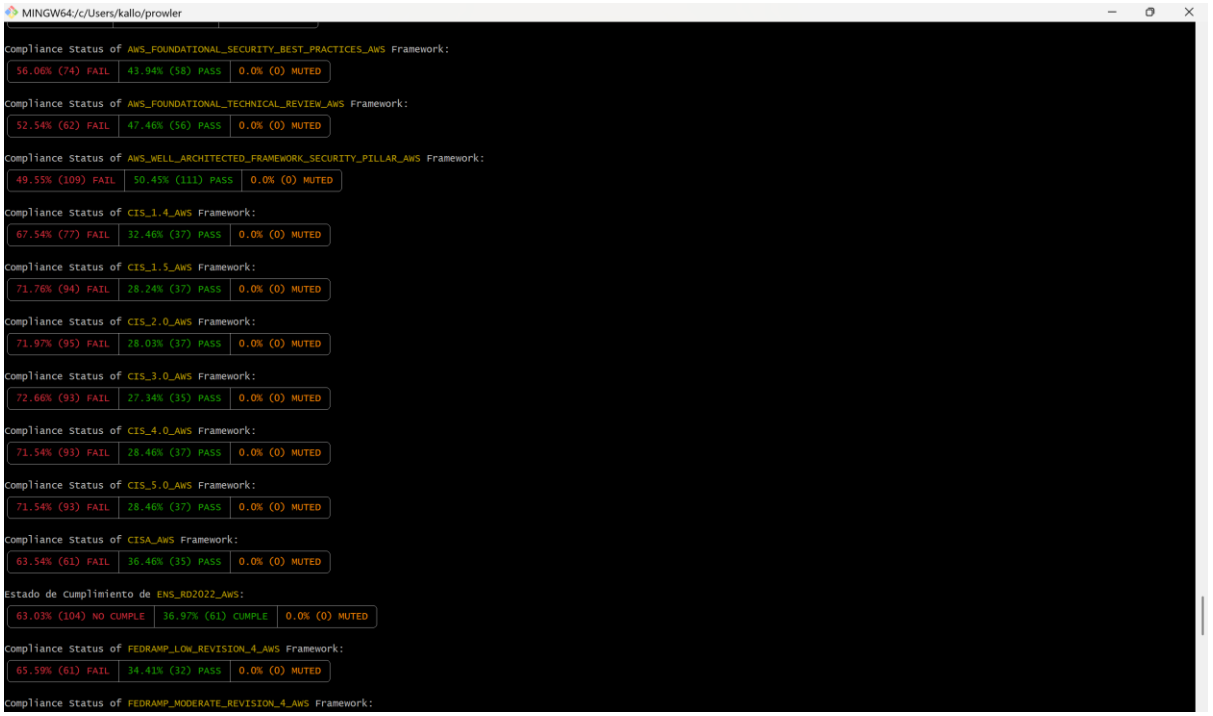


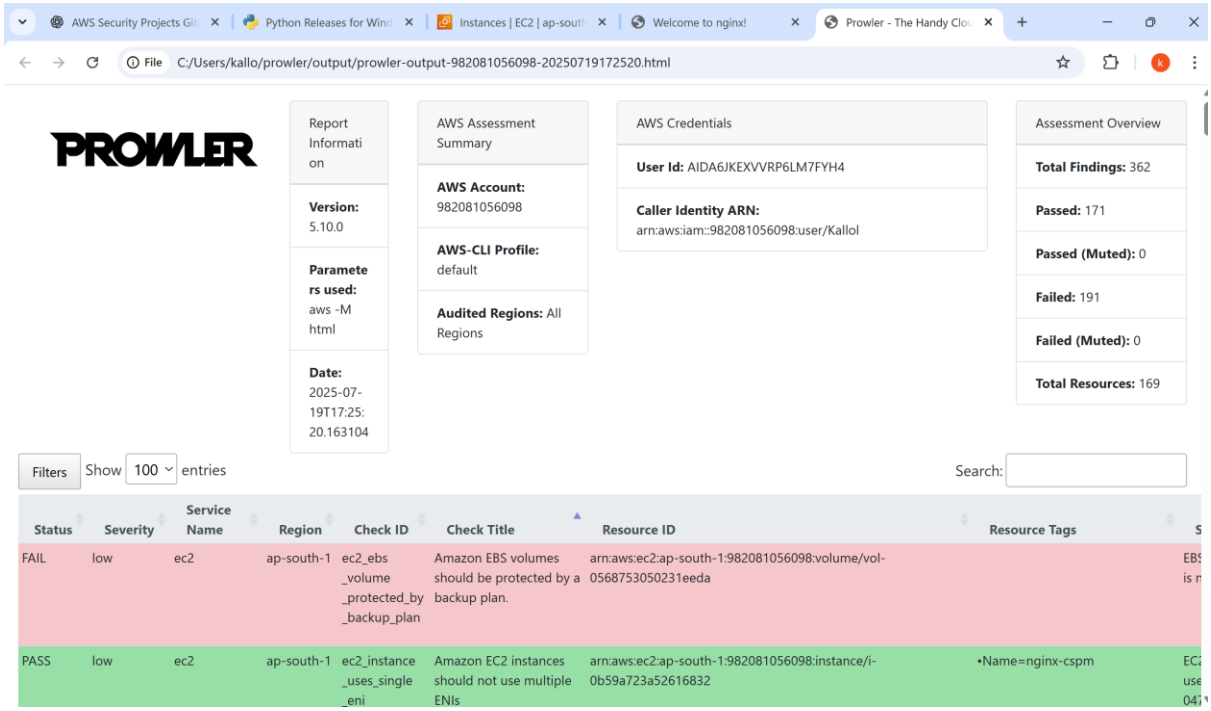



MINGW64:/c/Users/kallo/prowler
kallo@Tutula MINGW64 ~/prowler (master)
$ python prowler-cli.py -M html
v5.10.0
the handy multi-cloud security tool
Date: 2025-07-19 17:25:20
-> Using the AWS credentials below:
· AWS-CLI Profile: default
· AWS Regions: all
· AWS Account: 982081056098
· User Id: AIDA6JKEXVVRP6LM7FYH4
· Caller Identity ARN: arn:aws:iam::982081056098:user/kallol
-> Using the following configuration:
· Config File: C:\Users\kallo\prowler\prowler\config/config.yaml
· Mutelist File: C:\Users\kallo\prowler\prowler\config/aws_mutelist.yaml
· Scanning unused services and resources: False
Executing 568 checks, please wait...
-> Scanning acm service


kallo@Tutula MINGW64 ~/prowler (master)
$ python prowler-cli.py -M html
v5.10.0
the handy multi-cloud security tool
Date: 2025-07-19 17:25:20
-> Using the AWS credentials below:
· AWS-CLI Profile: default
· AWS Regions: all
· AWS Account: 982081056098
· User Id: AIDA6JKEXVVRP6LM7FYH4
· Caller Identity ARN: arn:aws:iam::982081056098:user/Kallol
-> Using the following configuration:
· Config File: C:\Users\kallo\prowler\prowler\config/config.yaml
· Mutelist File: C:\Users\kallo\prowler\prowler\config/aws_mutelist.yaml
· Scanning unused services and resources: False
Executing 568 checks, please wait...
-> Scanning config service


MINGW64:/c/Users/kallo/prowler
-> Scan completed! | (!) 536/568 [94%] in 16:00.3
Overview Results:
52.33% (191) Failed
46.85% (171) Passed
0.0% (0) Muted
Account 982081056098 Scan Results (severity columns are for fails only):
Provider Service Status Critical High Medium Low Muted
aws accessanalyzer FAIL (17) 0 0 0 17 0
aws account PASS (0) 0 0 0 0 0
aws backup FAIL (1) 0 0 0 1 0
aws bedrock FAIL (16) 0 0 16 0 0
aws cloudtrail FAIL (8) 0 0 4 4 0
aws cloudwatch FAIL (16) 0 0 16 0 0
aws config FAIL (17) 0 0 17 0 0
aws ec2 FAIL (17) 1 2 12 2 0
aws emr PASS (17) 0 0 0 0 0
aws guardduty FAIL (19) 0 1 18 0 0
aws iam FAIL (14) 0 1 10 3 0
aws inspector2 FAIL (17) 0 0 17 0 0
aws networkfirewall FAIL (1) 0 0 1 0 0
aws organizations FAIL (4) 0 0 2 2 0
aws s3 FAIL (20) 0 1 13 6 0
aws securityhub FAIL (17) 0 0 17 0 0
aws sns FAIL (1) 0 1 0 0 0
aws vpc FAIL (6) 0 0 6 0 0
* You only see here those services that contains resources.
Detailed results are in:
- HTML: C:\Users\kallo\prowler/output/prowler-output-982081056098-20250719172520.html
Compliance Status of AWS_ACCOUNT_SECURITY_ONBOARDING_AWS Framework:
70.42% (100) FAIL
29.58% (42) PASS
0.0% (0) MUTED
Compliance Status of AWS_AUDIT_MANAGER_CONTROL_TOWER_GUARDRAILS_AWS Framework:
57.14% (8) FAIL
42.86% (6) PASS
0.0% (0) MUTED
Compliance Status of AWS_FOUNDATIONAL_SECURITY_BEST_PRACTICES_AWS Framework:


MINGW64:/c/Users/kallo/prowler
Compliance Status of AWS_FOUNDATIONAL_SECURITY_BEST_PRACTICES_AWS Framework:
56.06% (74) FAIL
43.94% (58) PASS
0.0% (0) MUTED
Compliance Status of AWS_FOUNDATIONAL_TECHNICAL_REVIEW_AWS Framework:
52.54% (62) FAIL
47.46% (56) PASS
0.0% (0) MUTED
Compliance Status of AWS_WELL_ARCHITECTED_FRAMEWORK_SECURITY_PILLAR_AWS Framework:
49.55% (109) FAIL
50.45% (111) PASS
0.0% (0) MUTED
Compliance Status of CIS_1.4_AWS Framework:
67.54% (77) FAIL
32.46% (37) PASS
0.0% (0) MUTED
Compliance Status of CIS_1.5_AWS Framework:
71.76% (94) FAIL
28.24% (37) PASS
0.0% (0) MUTED
Compliance Status of CIS_2.0_AWS Framework:
71.97% (95) FAIL
28.03% (37) PASS
0.0% (0) MUTED
Compliance Status of CIS_3.0_AWS Framework:
72.66% (93) FAIL
27.34% (35) PASS
0.0% (0) MUTED
Compliance Status of CIS_4.0_AWS Framework:
71.54% (93) FAIL
28.46% (37) PASS
0.0% (0) MUTED
Compliance Status of CIS_5.0_AWS Framework:
71.54% (93) FAIL
28.46% (37) PASS
0.0% (0) MUTED
Compliance Status of CISA_AWS Framework:
63.54% (61) FAIL
36.46% (35) PASS
0.0% (0) MUTED
Estado de Cumplimiento de ENS_RD2022_AWS:
63.03% (104) NO CUMPLE
36.97% (61) CUMPLE
0.0% (0) MUTED
Compliance Status of FEDRAMP_LOW_REVISION_4_AWS Framework:
65.59% (61) FAIL
34.41% (32) PASS
0.0% (0) MUTED
Compliance Status of FEDRAMP_MODERATE_REVISION_4_AWS Framework:



python prowler-cli.py -M html :

You're executing **Prowler**, a popular **Cloud Security Posture Management (CSPM)** tool for AWS, and generating an **HTML report** of security checks.

What This Command Does:

- It runs **security audits** on your AWS account.

- Checks your configurations **against AWS security best practices**, industry standards like:
    - **CIS Benchmarks**
    - **NIST 800-53**
    - **PCI-DSS**
    - **ISO 27001**, etc.
- It reviews services like:
    - IAM (Identity & Access Management)
    - S3 bucket policies
    - CloudTrail logging
    - MFA status
    - Security Groups
    - Key Management (KMS)
    - And many more

Status	Severity	Service Name	Region	Check ID	Check Title	Resource ID	Resource Tags
FAIL	low	ec2	ap-south-1	ec2_ebs_volume_protected_by_backup_plan	Amazon EBS volumes should be protected by a backup plan.	arn:aws:ec2:ap-south-1:982081056098:volume/vol-0568753050231eeda	
PASS	low	ec2	ap-south-1	ec2_instance_uses_single_eni	Amazon EC2 instances should not use multiple ENIs	arn:aws:ec2:ap-south-1:982081056098:instance/i-0b59a723a52616832	•Name=nginx-cspm
PASS	medium	ec2	ap-south-1	ec2_instance_paravirtual_type	Amazon EC2 paravirtual virtualization type should not be used.	arn:aws:ec2:ap-south-1:982081056098:instance/i-0b59a723a52616832	•Name=nginx-cspm
FAIL	medium	vpc	ap-south-1	vpc_endpoint_for_ec2_enabled	Amazon EC2 should be configured to use VPC endpoints that are created for the Amazon EC2 service.	arn:aws:ec2:ap-south-1:982081056098:vpc/vpc-0782c9f0f1adc2877	•Name=cspm-vpc
FAIL	high	iam	ap-south-1	iam_avoid_root_usage	Avoid the use of the root accounts	arn:aws:iam::982081056098:root	
PASS	medium	ec2	ap-south-1	ec2_instance	Check EC2 Instances	arn:aws:ec2:ap-south-1:982081056098:instance/i-	•Name=nginx-cspm

Status Extended	Risk	Recommendation	Compliance
EBS Volume vol-0568753050231eeda is not protected by a backup plan.	Without backup coverage, Amazo read more...	Ensure that all in-use Amazon read more...	•AWS-Foundational-Security-Be read more...
EC2 Instance i-0b59a723a52616832 uses only one ENI: (Interfaces: ['eni-047ea2f7857af4e2a']).	Multiple ENIs can cause dual-h read more...	To detach a network interface read more...	•AWS-Foundational-Security-Be read more...
EC2 Instance i-0b59a723a52616832 virtualization type is set to HVM.	Using paravirtual instances ca read more...	To update an EC2 instance to a read more...	•AWS-Foundational-Security-Be read more...
VPC vpc-0782c9f0f1adc2877 has no EC2 endpoint.	Without VPC endpoints, network read more...	To improve the security postur read more...	•AWS-Foundational-Security-Be read more...
Root user in the account was last accessed 0 days ago.	The root account has unrestric read more...	Follow the remediation instruc read more...	•AWS-Account-Security-Onboard read more...
EC2 Instance i-0b59a723a52616832 is	Having old	Check if software	•AWS-