

PHASE 1: Create a Custom VPC

The screenshot shows the AWS VPC Dashboard. At the top, there are buttons for 'Create VPC' and 'Launch EC2 Instances'. A note says: 'Note: Your Instances will launch in the Asia Pacific region.' Below this is a section titled 'Resources by Region' with a note: 'You are using the following Amazon VPC resources.' It lists various resources with counts for the Mumbai region:

- VPCs: Mumbai 1 (with a 'See all regions' link)
- NAT Gateways: Mumbai 0 (with a 'See all regions' link)
- Subnets: Mumbai 3 (with a 'See all regions' link)
- VPC Peering Connections: Mumbai 0 (with a 'See all regions' link)
- Route Tables: Mumbai 1 (with a 'See all regions' link)
- Network ACLs: Mumbai 1 (with a 'See all regions' link)
- Internet Gateways: Mumbai 1 (with a 'See all regions' link)
- Security Groups: Mumbai 1 (with a 'See all regions' link)
- Customer Gateways: Mumbai 0 (with a 'See all regions' link)

On the left sidebar, under 'Virtual private cloud', there are sections for 'Your VPCs', 'Subnets', 'Route tables', 'Internet gateways', 'Egress-only internet gateways', 'DHCP option sets', 'Elastic IPs', 'Managed prefix lists', 'NAT gateways', and 'Peering connections'. Under 'Security', there are sections for 'Network ACLs' and 'Security groups'. On the right side, there are boxes for 'Service Health', 'Settings', and 'Additional Information'.

The screenshot shows the 'Create VPC' wizard. The current step is 'VPC settings'. The 'Resources to create' section has 'VPC only' selected. The 'Name tag - optional' field contains 'cspm-vpc'. The 'IPv4 CIDR block' section has 'IPv4 CIDR manual input' selected, and the 'IPv4 CIDR' field contains '10.0.0.0/16'. The 'IPv6 CIDR block' section has 'No IPv6 CIDR block' selected. The bottom of the page includes standard AWS navigation links like CloudShell, Feedback, and a footer with copyright information and date.

The screenshot shows the AWS VPC Dashboard. A green success message at the top says "You successfully created vpc-0782c9f0f1adc2877 / cspm-vpc". The main card displays details for the VPC "vpc-0782c9f0f1adc2877 / cspm-vpc". Key information includes:

VPC ID	State	Block Public Access	DNS hostnames
vpc-0782c9f0f1adc2877	Available	Off	Disabled
DNS resolution	Tenancy	DHCP option set	Main route table
Enabled	default	dopt-042a3de05f8e65071	rtb-04578b762f4c68ef1
Main network ACL	Default VPC	IPv4 CIDR	IPv6 pool
acl-07381381a569f5f20	No	10.0.0.0/16	-
IPv6 CIDR (Network border group)	Network Address Usage metrics	Route 53 Resolver DNS Firewall rule groups	Owner ID
-	Disabled	-	982081056098

Below the details, there are tabs for Resource map, CIDRs, Flow logs, Tags, and Integrations. The Resource map tab is selected.

PHASE 2: Add Subnet

The screenshot shows the "Create subnet" wizard. The first step, "Subnet settings", is displayed. It asks to specify CIDR blocks and Availability Zone for the subnet.

Subnet 1 of 1

Subnet name
Create a tag with a key of 'Name' and a value that you specify.
public-subnet

The name can be up to 256 characters long.

Availability Zone Asia Pacific (Mumbai) / ap-south-1a
Choose the zone in which your subnet will reside, or let Amazon choose one for you.

IPv4 VPC CIDR block 10.0.0.0/16
Choose the VPC's IPv4 CIDR block for the subnet. The subnet's IPv4 CIDR must lie within this block.

IPv4 subnet CIDR block
10.0.0.0/24
256 IPs

Tags - optional

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

The screenshot shows the AWS VPC Subnets page. A green success message at the top states: "You have successfully created 1 subnet: subnet-0edfcfd1ff27a043c". Below this, the "Subnets (1) Info" section displays a single subnet named "public-subnet" with the ID "subnet-0edfcfd1ff27a043c". The subnet is listed as "Available" and is associated with the VPC "vpc-0782c9f0f1adc2877 | cspm...". The left sidebar shows navigation options for VPC dashboard, EC2 Global View, 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), and Security (Network ACLs, Security groups). The bottom status bar indicates it's 20:23 on 15-07-2025.

Enable auto-assign public IP:

The screenshot shows the "Edit subnet settings" page for the subnet "subnet-0edfcfd1ff27a043c". In the "Auto-assign IP settings" section, the checkbox "Enable auto-assign public IPv4 address" is checked. Other options like "Enable auto-assign customer-owned IPv4 address" are disabled. The "Resource-based name (RBN) settings" section is also visible. The bottom status bar indicates it's 20:34 on 15-07-2025.

The screenshot shows the "Subnet Details" page for the subnet "subnet-0edfcfd1ff27a043c". A green success message states: "You have successfully changed subnet settings: Enable auto-assign public IPv4 address". The left sidebar shows navigation options for VPC dashboard, EC2 Global View, Subnets (NAT gateways, Peering connections), and Security. The bottom status bar indicates it's 20:34 on 15-07-2025.

PHASE 3: Add Internet Gateway & Routing

The screenshot shows the AWS VPC console interface. On the left, there's a sidebar with navigation links like 'Virtual private cloud' (selected), 'Internet gateways' (selected), and 'Security'. The main area displays a message: 'The following internet gateway was created: igw-09a495dada364be3d - cspm-igw. You can now attach to a VPC to enable the VPC to communicate with the internet.' Below this, the 'igw-09a495dada364be3d / cspm-igw' card shows details: Internet gateway ID (igw-09a495dada364be3d), State (Detached), VPC ID (-), and Owner (982081056098). A 'Tags' section lists 'Name: cspm-igw'. At the bottom right of the card is a 'Manage tags' button.

This screenshot shows the 'Attach to VPC' dialog box. It has a 'VPC' section with a note: 'Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.' Below it is an 'Available VPCs' section with a note: 'Attach the internet gateway to this VPC.' A search bar contains the text 'vpc-0782c9f0f1adc2877'. At the bottom right are 'Cancel' and 'Attach internet gateway' buttons.



← → ⌂ ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#InternetGateway:internetGatewayId=igw-09a495dada364be3d...

aws Search [Alt+S] Asia Pacific (Mumbai) Kallola

VPC > Internet gateways > igw-09a495dada364be3d

Internet gateway igw-09a495dada364be3d successfully attached to vpc-0782c9f0f1adc2877

igw-09a495dada364be3d / cspm-igw

Details Info

Internet gateway ID igw-09a495dada364be3d	State Attached	VPC ID vpc-0782c9f0f1adc2877 cspm-vpc	Owner 982081056098
--	-------------------	--	-----------------------

Tags

Key	Value
Name	cspm-igw

Actions

CloudShell Feedback © 2025, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences 24°C Mostly clear 20:42 15-07-2025 ENG IN

← → ⌂ ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#CreateRouteTable:

aws 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

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 20:42 15-07-2025 ENG IN

← → ⌂ ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#RouteTableDetails:RouteTableId=rtb-0f4e7ca6586f7b... ☆ 🗃 🔍 New Chrome available ⚙

VPC > Route tables > rtb-0f4e7ca6586f7bb3a

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

CloudShell Feedback

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

24°C Mostly clear

Search

Route table rtb-0f4e7ca6586f7bb3a | public-route-table was created successfully.

rtb-0f4e7ca6586f7bb3a / public-route-table

Actions ▾

Details Info

Route table ID rtb-0f4e7ca6586f7bb3a	Main No	Explicit subnet associations -	Edge associations -
VPC vpc-0782c9f0f1adc2877 cspm-vpc	Owner ID 982081056098		

Routes Subnet associations Edge associations Route propagation Tags

Routes (1)

Filter routes				Both ▾	Edit routes
Destination	Target	Status	Propagated		
10.0.0.0/16	local	Active	No		

← → ⌂ ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#RouteTableDetails:RouteTableId=rtb-0f4e7ca6586f7b... ☆ 🗃 🔍 New Chrome available ⚙

v route 53

VPC > Route tables > rtb-0f4e7ca6586f7bb3a

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

CloudShell Feedback

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

24°C Mostly clear

Search

Updated routes for rtb-0f4e7ca6586f7bb3a / public-route-table successfully

▶ Details

Details Info

Route table ID rtb-0f4e7ca6586f7bb3a	Main No	Explicit subnet associations -	Edge associations -
VPC vpc-0782c9f0f1adc2877 cspm-vpc	Owner ID 982081056098		

Routes Subnet associations Edge associations Route propagation Tags

Routes (2)

Filter routes				Both ▾	Edit routes
Destination	Target	Status	Propagated		
0.0.0.0/0	igw-09a495dada364be3d	Active	No		
10.0.0.0/16	local	Active	No		

Associate the route table with public-subnet:

VPC dashboard

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

Details

Route table ID: rtb-Of4e7ca6586f7bb3a

Main: No

VPC: vpc-0782c9f0f1adc2877 | cspm-vpc

Owner ID: 982081056098

Explicit subnet associations: subnet-0edffcf1ff27a043c / public-subnet

Edge associations: -

Routes (2)

Destination	Target	Status	Propagated
0.0.0.0/0	igw-09a495dada364be3d	Active	No
10.0.0.0/16	local	Active	No

PHASE 4: Create Security Group

Create security group

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

Security group name: cspm-sg

Description: Allows SSH access to developers

VPC: vpc-0782c9f0f1adc2877 (cspm-vpc)

Inbound rules

This security group has no inbound rules.

Add rule

Outbound rules

ap-south-1.console.aws.amazon.com/vpcconsole/home?region=ap-south-1#CreateSecurityGroup:

Inbound rules

Type	Protocol	Port range	Source	Description - optional
HTTP	TCP	80	An... 0.0.0.0/0	
SSH	TCP	22	My IP 0.0.0.0/0	
				106.51.219.48/32

Add rule

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

Outbound rules

Type	Protocol	Port range	Destination	Description - optional
CloudShell	Feedback			

sg-099f3912b756a0ead - cspm-sg

Details

Security group name	Security group ID	Description	VPC ID
cspm-sg	sg-099f3912b756a0ead	Security Group for CSPM	vpc-0782c9f0f1adc2877
Owner	982081056098	Inbound rules count	Outbound rules count
		2 Permission entries	1 Permission entry

Inbound rules | Outbound rules | Sharing - new | VPC associations - new | Tags

Inbound rules (2)

Name	Security group rule ID	IP version	Type	Protocol
-	sgr-00eb10d6e8a5cc557	IPv4	HTTP	TCP
-	sgr-0336f0ae1b6d73d7d	IPv4	SSH	TCP

PHASE 5: Launch EC2 Instance

← → ⌂ ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#Overview:

aws | 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

© 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:

aws | 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 **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.

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 [X](#)

Cancel **Launch instance** **Preview code**

© 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 ⋮

aws Search [Alt+S] Asia Pacific (Mumbai) Kallola

EC2 Instances Launch an instance

Amazon Machine Image (AMI)

Amazon Linux 2023 kernel-6.1 AMI
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 64-bit (...) **Boot mode** uefi-preferred **AMI ID** ami-0a1235697f4afa8a4 **Publish Date** 2025-07-08 **Username** ec2-user

Verified provider

Instance type Info | Get advice

Instance type t2.micro

Additional costs apply for AMIs with pre-installed software

Summary

Number of instances 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 X

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 ⋮

aws Search [Alt+S] Asia Pacific (Mumbai) Kallola

EC2 Instances Launch an instance

Instance type

t2.micro Free tier eligible

All generations Compare instance types

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 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 X

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 :

aws 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

Select security groups
cspm-sg sg-099f3912b756a0ead X
VPC: vpc-0782c9f0f1adc2877

Common security groups | Info
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

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

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

← → ⌂ ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#LaunchInstances: ☆ ⌂ ↴ ↵ New Chrome available :

aws 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.

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

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

← → ⌂ ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#LaunchInstances: ☆ 🔍 New Chrome available :

aws | 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.

```
#!/bin/bash
yum update -y
amazon-linux-extras install nginx1-1
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 X

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 :

aws | 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.

Launch log

Request	Status
Initializing requests	<input checked="" type="radio"/> Succeeded
Launch initiation	<input checked="" type="radio"/> Failed

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

Credit specification | Info

Select

ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#LaunchInstances

Success Successfully initiated launch of instance (i-0b59a723a52616832)

Launch log

Next Steps

What would you like to do next with this instance, for example "create alarm" or "create backup"

Create billing and free tier usage alerts

To manage costs and avoid surprise bills, set up email notifications for billing and free tier usage thresholds.

Create billing alerts

Connect to your instance

Once your instance is running, log into it from your local computer.

Connect to instance

Learn more

Connect an RDS database

Configure the connection between an EC2 instance and a database to allow traffic flow between them.

Connect an RDS database

Create a new RDS database

Learn more

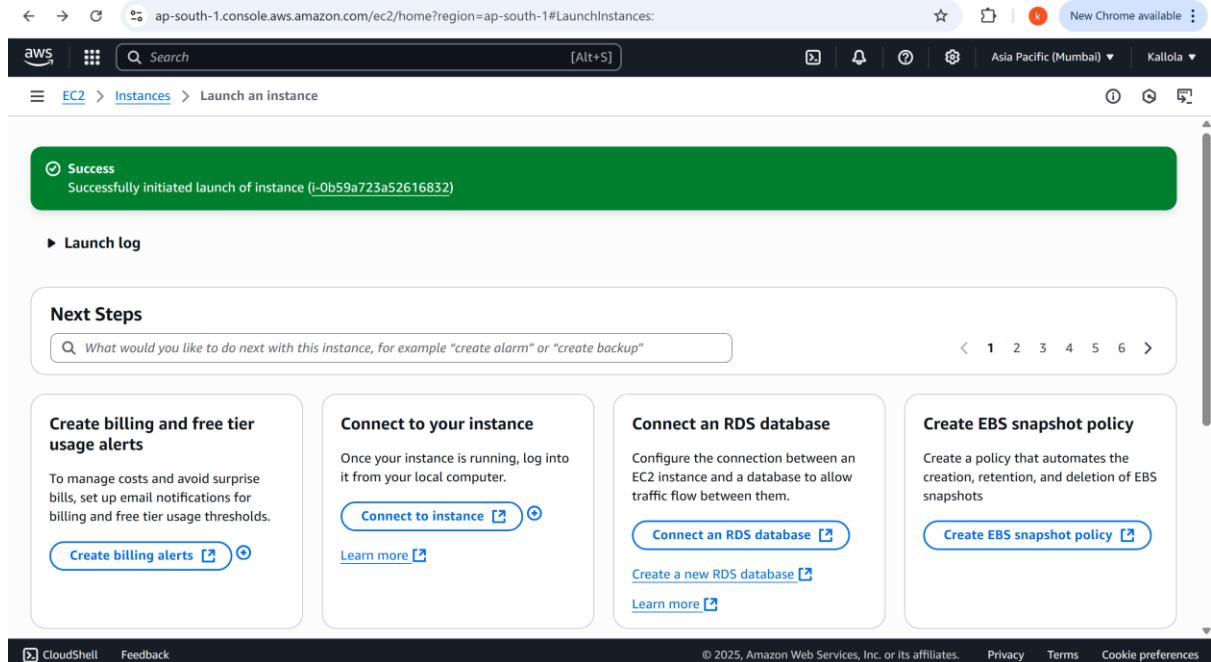
Create EBS snapshot policy

Create a policy that automates the creation, retention, and deletion of EBS snapshots.

Create EBS snapshot policy

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#Instances

Successfully initiated starting of i-0b59a723a52616832

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

CloudShell Feedback

Instances (1/1) Info Last updated less than a minute ago

Find Instance by attribute or tag (case-sensitive)

All states

Name Instance ID Instance state Instance type Status check Alarm status

<input checked="" type="checkbox"/> nginx-cspm	i-0b59a723a52616832	Running	t2.micro	Initializing	View alarms +
--	---------------------	---------	----------	--------------	-------------------------------

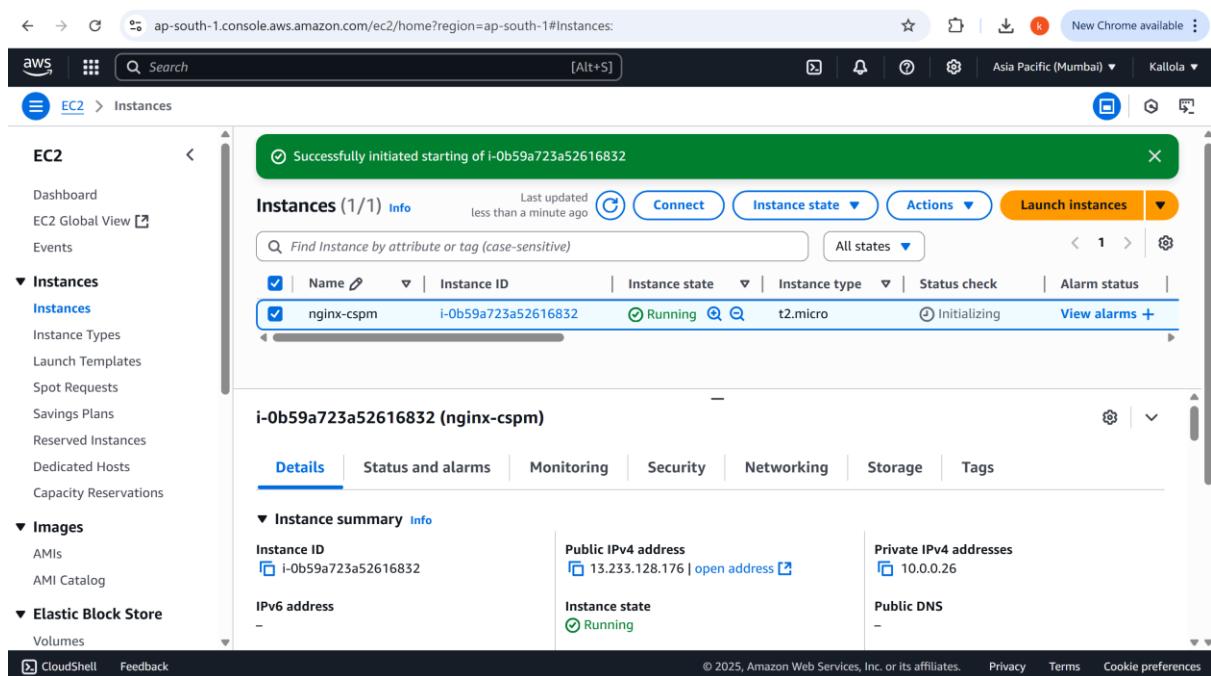
i-0b59a723a52616832 (nginx-cspm)

Details Status and alarms Monitoring Security Networking Storage Tags

Instance summary

Instance ID i-0b59a723a52616832	Public IPv4 address 13.233.128.176 open address	Private IPv4 addresses 10.0.0.26
IPv6 address -	Instance state Running	Public DNS -

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



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-10-0-26 ~]$ 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-httdp 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
=====

[ec2-user@ip-10-0-0-26 ~]$ curl 13.233.128.176 (ec2-user) () 
Running transaction
Preparing :
Running scriptlet: nginx-filesystem-1:1.28.0-1.amzn2023.0.1.noarch
Installing : nginx-filesystem-1:1.28.0-1.amzn2023.0.1.noarch
Installing : nginx-mimetypes-2.1.49-3.amzn2023.0.3.noarch
Installing : libunwind-1.4.0-5.amzn2023.0.2.x86_64
Installing : gperftools-libs-2.9.1-1.amzn2023.0.3.x86_64
Installing : nginx-core-1:1.28.0-1.amzn2023.0.1.x86_64
Installing : generic-logos-httdp-18.0.0-12.amzn2023.0.3.noarch
Installing : nginx-1:1.28.0-1.amzn2023.0.1.x86_64
Running scriptlet: nginx-1:1.28.0-1.amzn2023.0.1.x86_64
Verifying  : generic-logos-httdp-18.0.0-12.amzn2023.0.3.noarch
Verifying  : gperftools-libs-2.9.1-1.amzn2023.0.3.x86_64
Verifying  : libunwind-1.4.0-5.amzn2023.0.2.x86_64
Verifying  : nginx-1:1.28.0-1.amzn2023.0.1.x86_64
Verifying  : nginx-core-1:1.28.0-1.amzn2023.0.1.x86_64
Verifying  : nginx-filesystem-1:1.28.0-1.amzn2023.0.1.noarch
Verifying  : nginx-mimetypes-2.1.49-3.amzn2023.0.3.noarch
=====
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-httdp-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 ~]$ 
```

If you see this page, the nginx web server is successfully installed and working. Further configuration is required.

For online documentation and support please refer to [nginx.org](#). Commercial support is available at [nginx.com](#).

Thank you for using nginx.

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.

User created successfully

You can view and download the user's password and email instructions for signing in to the AWS Management Console.

Users (1)

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

User name	Path	Group	Last activity	MFA	Password age
Kallola	/	0	-	-	-

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

Kallool Info

Delete

Summary

ARN arn:aws:iam::982081056098:user/Kallool	Console access Disabled	Access key 1 Create access key
Created July 18, 2025, 22:57 (UTC+05:30)	Last console sign-in -	

Permissions Groups Tags Security credentials Last Accessed

Permissions policies (2)

Permissions are defined by policies attached to the user directly or through groups.

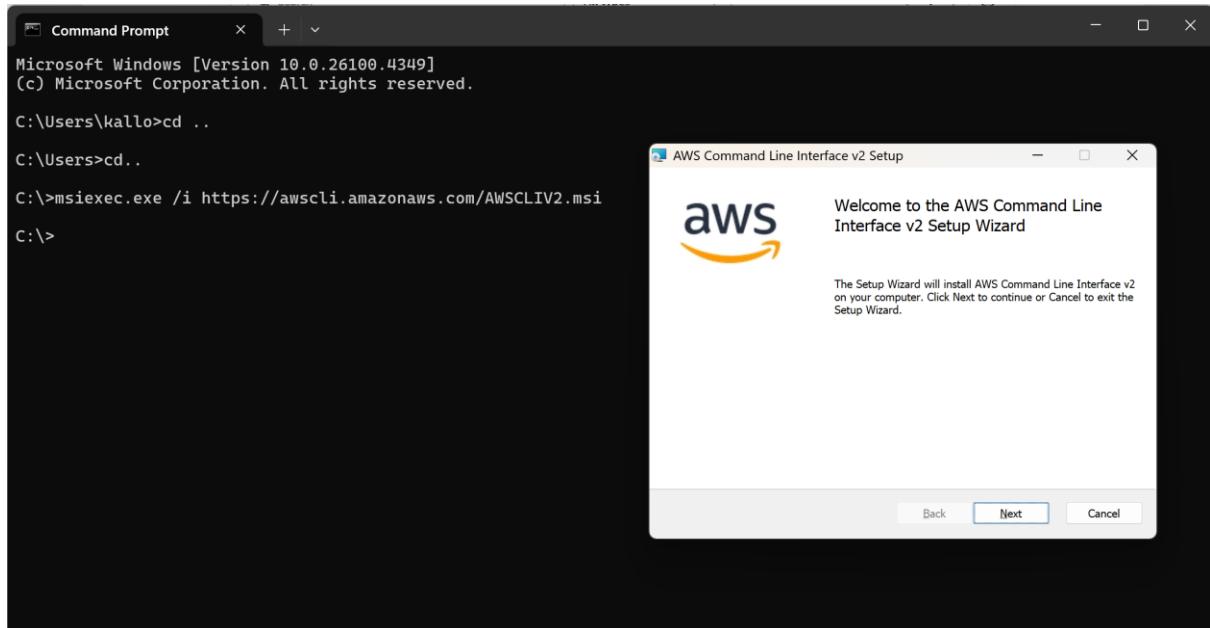
Filter by Type

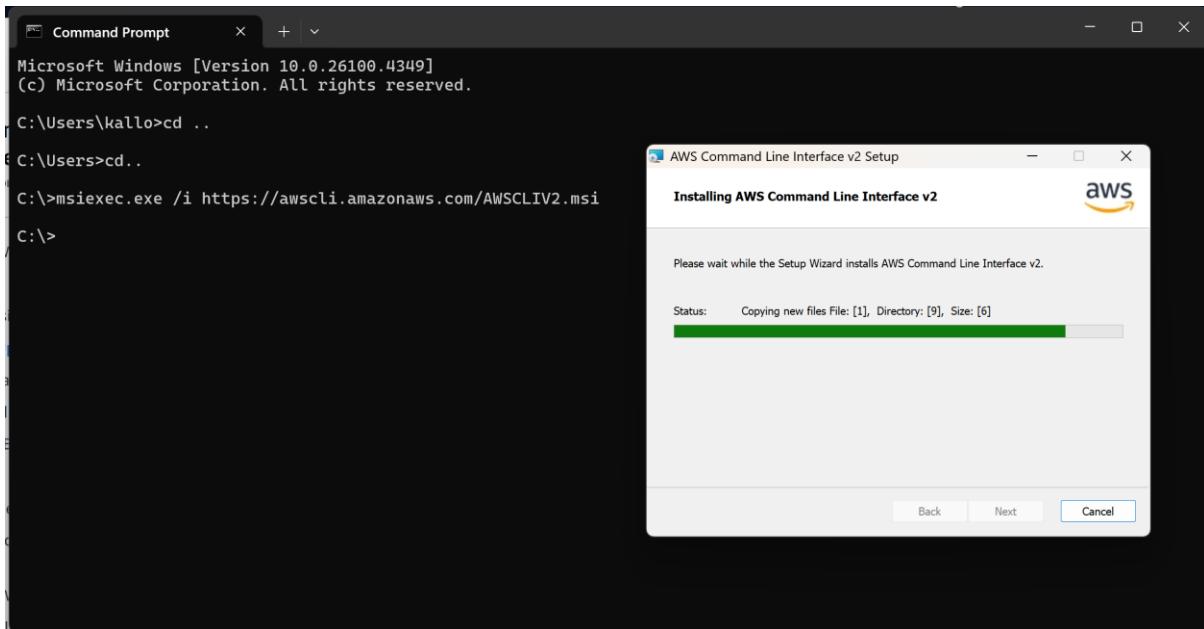
Policy name	Type	Attached via
AIOpsReadOnlyAccess	AWS managed	Directly
SecurityAudit	AWS managed - job function	Directly

Add permissions ▾

Create access key & download access key & secret key.

2. Install & configure AWS CLI on your laptop.





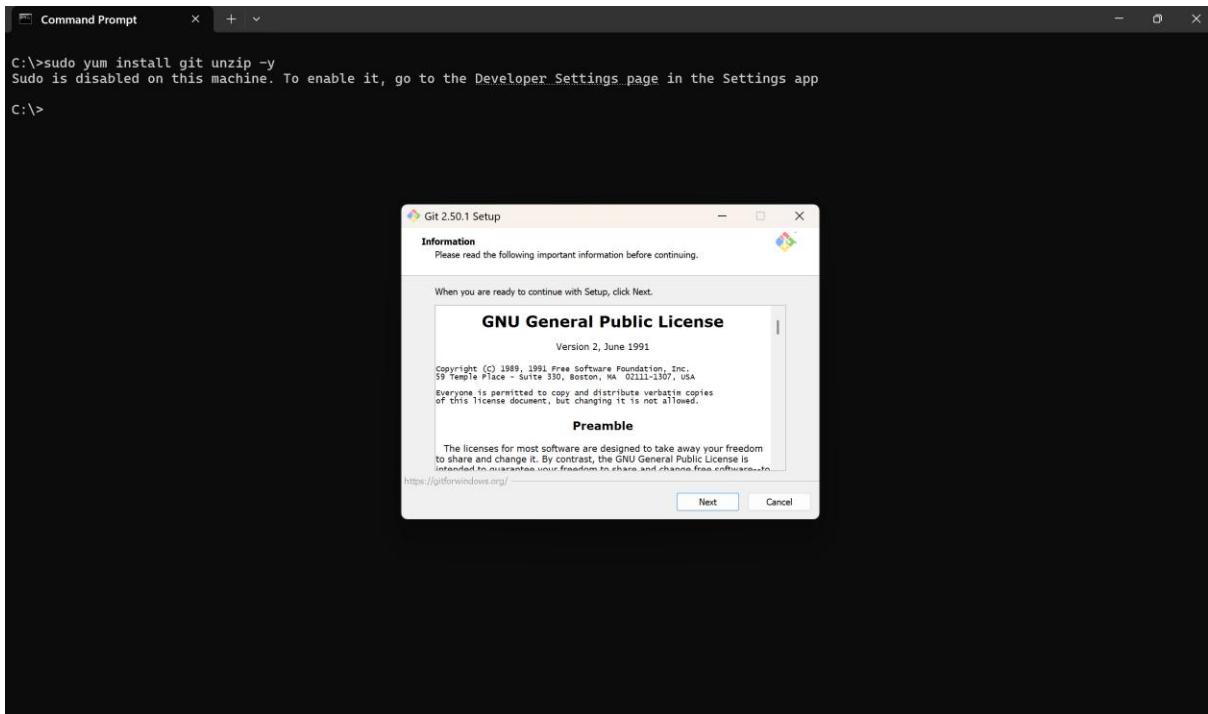
```
C:\>aws --version
aws-cli/2.27.54 Python/3.13.4 Windows/11 exe/AMD64
```

Once finished, you have to configure it.

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

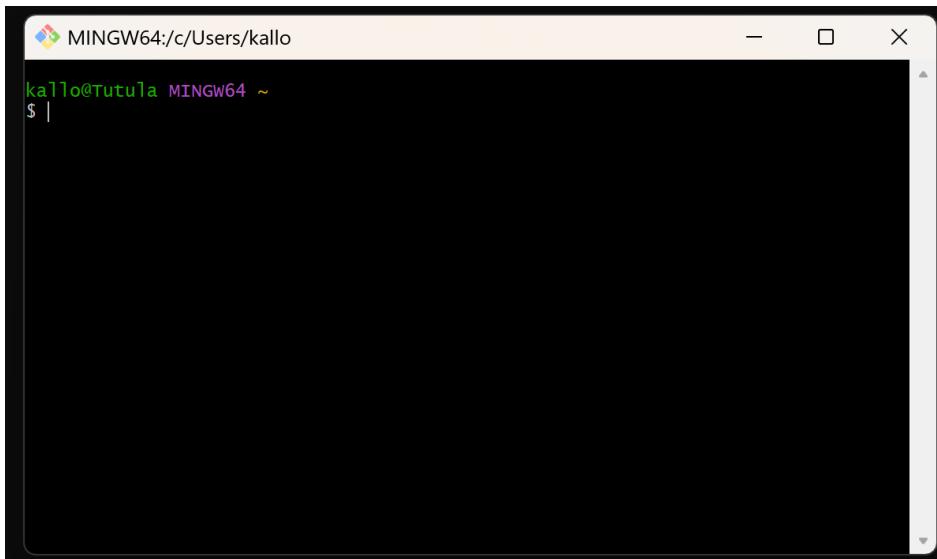
```
C:\>
```

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

```
MINGW64:/c/Users/kallo
kallo@Tutula MINGW64 ~
$ git clone https://github.com/prowler-cloud/prowler.git
Cloning into 'prowler'...
remote: Enumerating objects: 120060, done.
remote: Counting objects: 100% (1901/1901), done.
remote: Compressing objects: 100% (902/902), done.
remote: Total 120060 (delta 1564), reused 1031 (delta 995), pack-reused 118159 (from 3)
Receiving objects: 100% (120060/120060), 151.48 MiB | 6.20 MiB/s, done.
Resolving deltas: 100% (85668/85668), done.
Updating files: 100% (6181/6181), done.

kallo@Tutula MINGW64 ~
$ |
```

```
MINGW64:/c/Users/kallo/prowler
kallo@Tutula MINGW64 ~
$ git clone https://github.com/prowler-cloud/prowler.git
Cloning into 'prowler'...
remote: Enumerating objects: 120060, done.
remote: Counting objects: 100% (1901/1901), done.
remote: Compressing objects: 100% (902/902), done.
remote: Total 120060 (delta 1564), reused 1031 (delta 995), pack-reused 118159 (from 3)
Receiving objects: 100% (120060/120060), 151.48 MiB | 6.20 MiB/s, done.
Resolving deltas: 100% (85668/85668), done.
Updating files: 100% (6181/6181), done.

kallo@Tutula MINGW64 ~
$ cd prowler

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

Step 2: Run basic audit

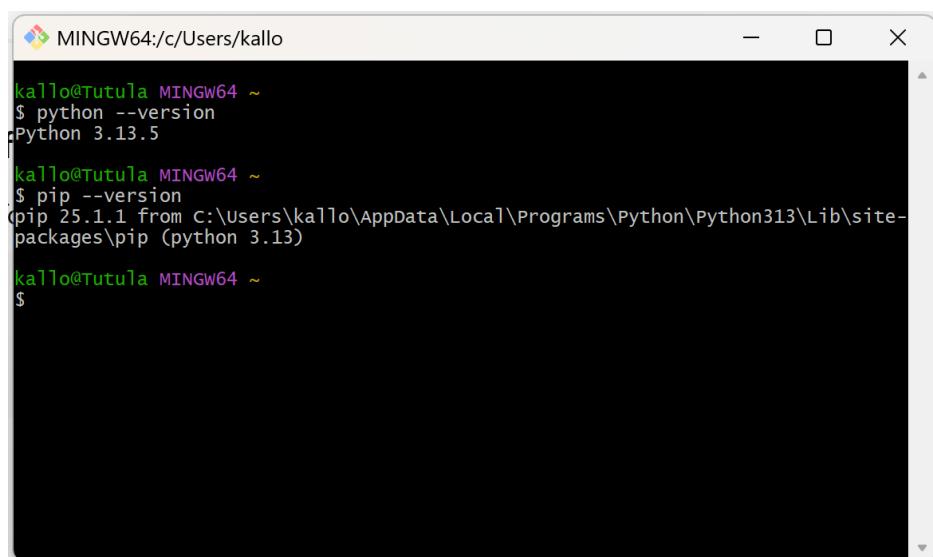
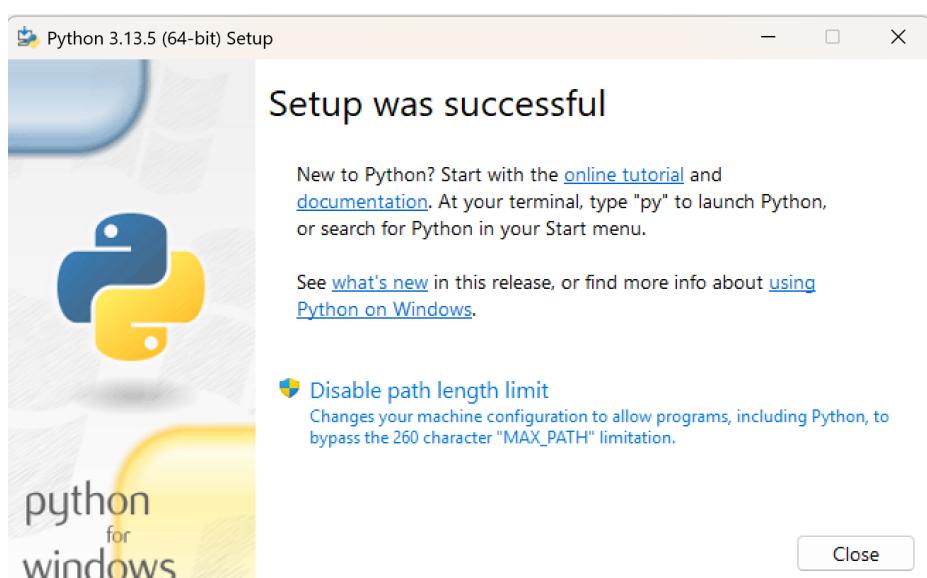
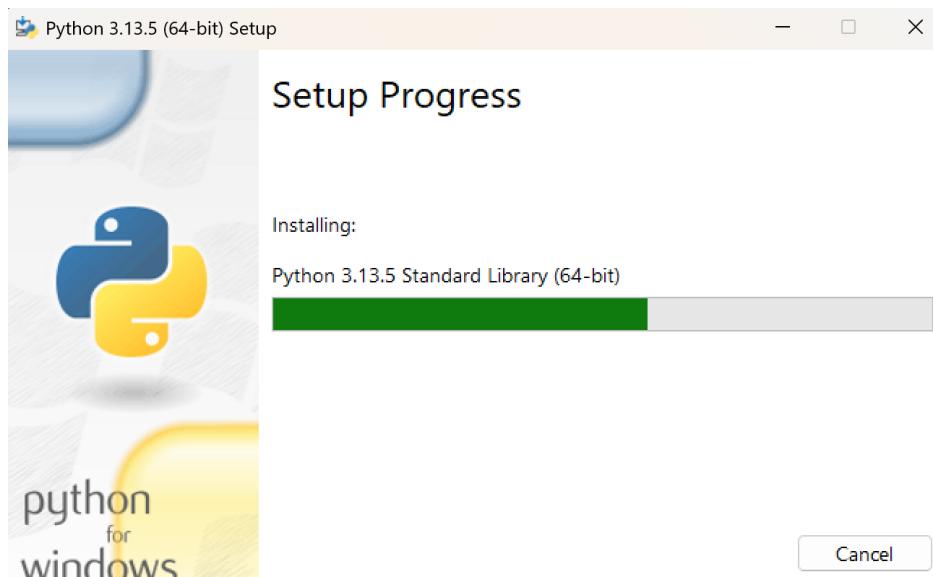
Run the CIS benchmark scan:

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)



```
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/
-rwrxr-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`.
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`.

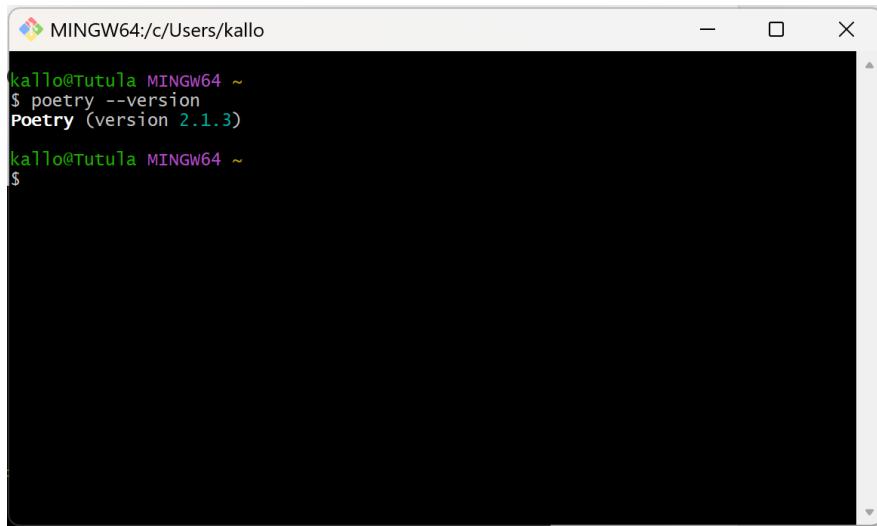
You can test that everything is set up by executing:
poetry --version

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

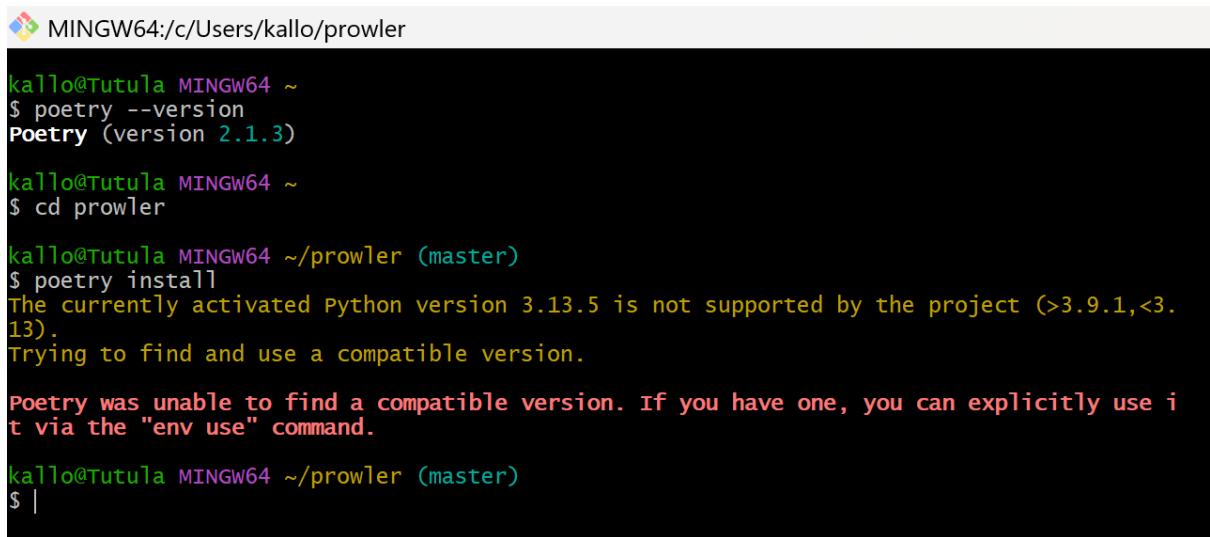
Append the bin directory to your user environment variable `PATH`

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

Exit & reconnect Git Bash & run poetry –version



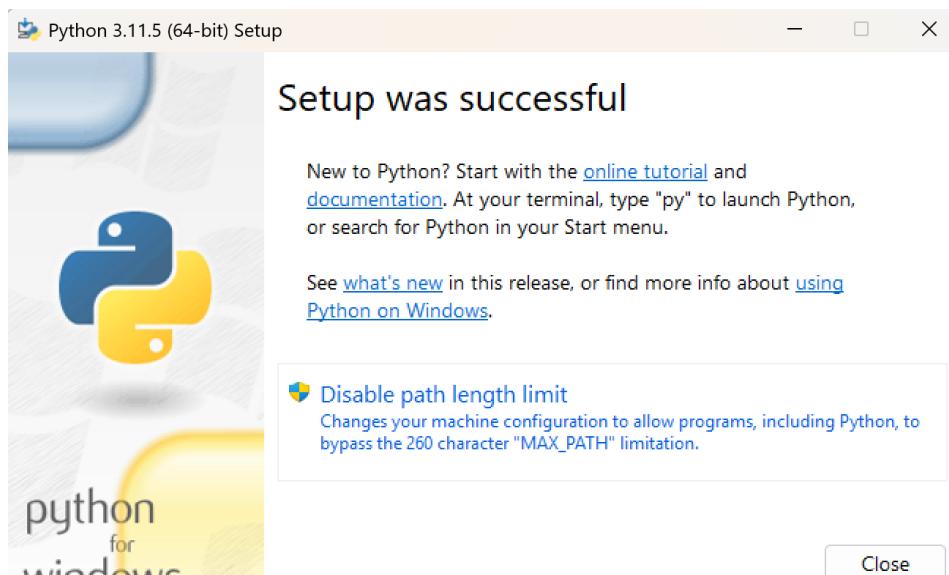
```
MINGW64:/c/Users/kallo
kallo@Tutula MINGW64 ~
$ poetry --version
Poetry (version 2.1.3)
kallo@Tutula MINGW64 ~
$
```



```
MINGW64:/c/Users/kallo/prowler
kallo@Tutula MINGW64 ~
$ poetry --version
Poetry (version 2.1.3)
kallo@Tutula MINGW64 ~
$ cd prowler
kallo@Tutula MINGW64 ~/prowler (master)
$ poetry install
The currently activated Python version 3.13.5 is not supported by the project (>3.9.1,<3.13).
Trying to find and use a compatible version.
Poetry was unable to find a compatible version. If you have one, you can explicitly use it via the "env use" command.
kallo@Tutula MINGW64 ~/prowler (master)
$ |
```

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 ~
$ python --version
Python 3.11.5
```

```
kallo@Tutula MINGW64 ~/prowler (master)
$ pip --version
pip 23.2.1 from c:\users\kallo\appdata\local\programs\python\python311\lib\site-packages\pip (python 3.11)
kallo@Tutula MINGW64 ~/prowler (master)
$ |
```



```

MINGW64:/c/Users/kallo/prowler
--> Scan completed [██████████] 0 | () 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_GARDRAILS_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:

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:		
---	--	--

```

MINGW64:/c/Users/kallo/prowler
 50.9% (169) FAIL | 49.1% (163) PASS | 0.0% (0) MUTED
Compliance status of MITRE_ATTACK_AWS Framework:
 75.62% (116) FAIL | 24.18% (37) PASS | 0.0% (0) MUTED
Compliance status of NIS2_AWS Framework:
 60.42% (87) FAIL | 39.58% (57) PASS | 0.0% (0) MUTED
Compliance status of NIST_800_171_REVISION_2_AWS Framework:
 69.7% (69) FAIL | 30.3% (30) PASS | 0.0% (0) MUTED
Compliance status of NIST_800_53_REVISION_4_AWS Framework:
 66.32% (63) FAIL | 33.68% (32) PASS | 0.0% (0) MUTED
Compliance status of NIST_800_53_REVISION_5_AWS Framework:
 66.67% (64) FAIL | 33.33% (32) PASS | 0.0% (0) MUTED
Compliance status of NIST_CSF_1_1_AWS Framework:
 73.73% (87) FAIL | 26.27% (31) PASS | 0.0% (0) MUTED
Compliance status of PCI_3.2.1_AWS Framework:
 69.57% (64) FAIL | 30.43% (28) PASS | 0.0% (0) MUTED
Compliance status of PCI_4.0_AWS Framework:
 57.6% (72) FAIL | 42.4% (53) PASS | 0.0% (0) MUTED
Compliance status of PROWLER_THREATSCORE_AWS Framework:
 53.89% (97) FAIL | 46.11% (83) PASS | 0.0% (0) MUTED
Compliance status of RBI_CYBER_SECURITY_FRAMEWORK_AWS Framework:
 64.71% (44) FAIL | 35.29% (24) PASS | 0.0% (0) MUTED
Compliance status of SOC2_AWS Framework:
 65.41% (104) FAIL | 34.59% (55) PASS | 0.0% (0) MUTED
Detailed compliance results are in C:\users\kallo\prowler\output\compliance/
(venv)
callto:putula MINGW64 ~/prowler (master)

```

Status	Severity	Service Name	Region	Check ID	Check Title	Resource ID	Resource Tags
FAIL	low	ec2	ap-south-1	ap_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	EBS is not
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 EC2 use 047

`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	*Name=nginx-cspm
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 paravirtualization 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, Amazon read more...	Ensure that all in-use Amazon read more... <input checked="" type="checkbox"/>	•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... <input checked="" type="checkbox"/>	•AWS-Foundational-Security-Be read more...
EC2 Instance i-0b59a723a52616832 virtualization type is set to HVM.	Using paravirtual instances can read more...	To update an EC2 instance to a read more... <input checked="" type="checkbox"/>	•AWS-Foundational-Security-Be read more...
VPC vpc-0782c9f0f1adc2877 has no EC2 endpoint.	Without VPC endpoints, network read more...	To improve the security posture read more... <input checked="" type="checkbox"/>	•AWS-Foundational-Security-Be read more...
Root user in the account was last accessed 0 days ago.	The root account has unrestricted read more...	Follow the remediation instructions read more... <input checked="" type="checkbox"/>	•AWS-Account-Security-Onboard read more...
EC2 Instance i-0b59a723a52616832 is Having old software installed.	Having old software installed.	Check if software is up-to-date. read more... <input checked="" type="checkbox"/>	•AWS-