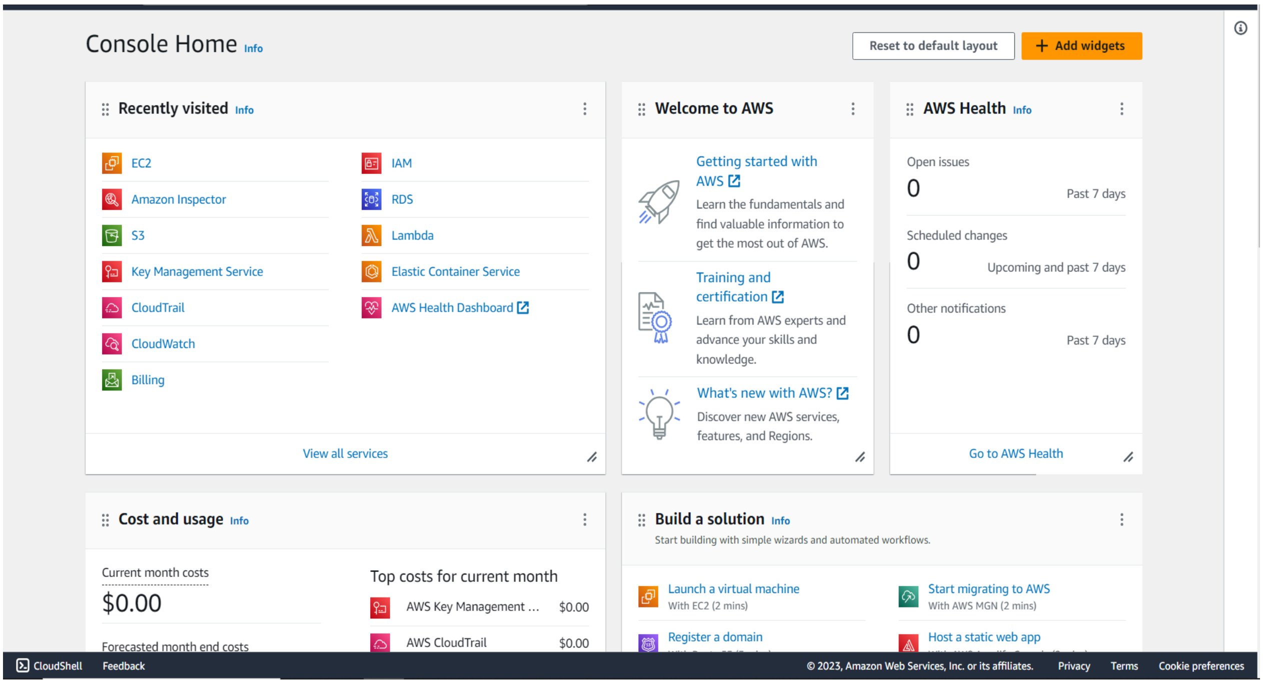
Finding vulnerabilities on EC2 instance using Amazon Inspector

1. Sign in to AWS Console.



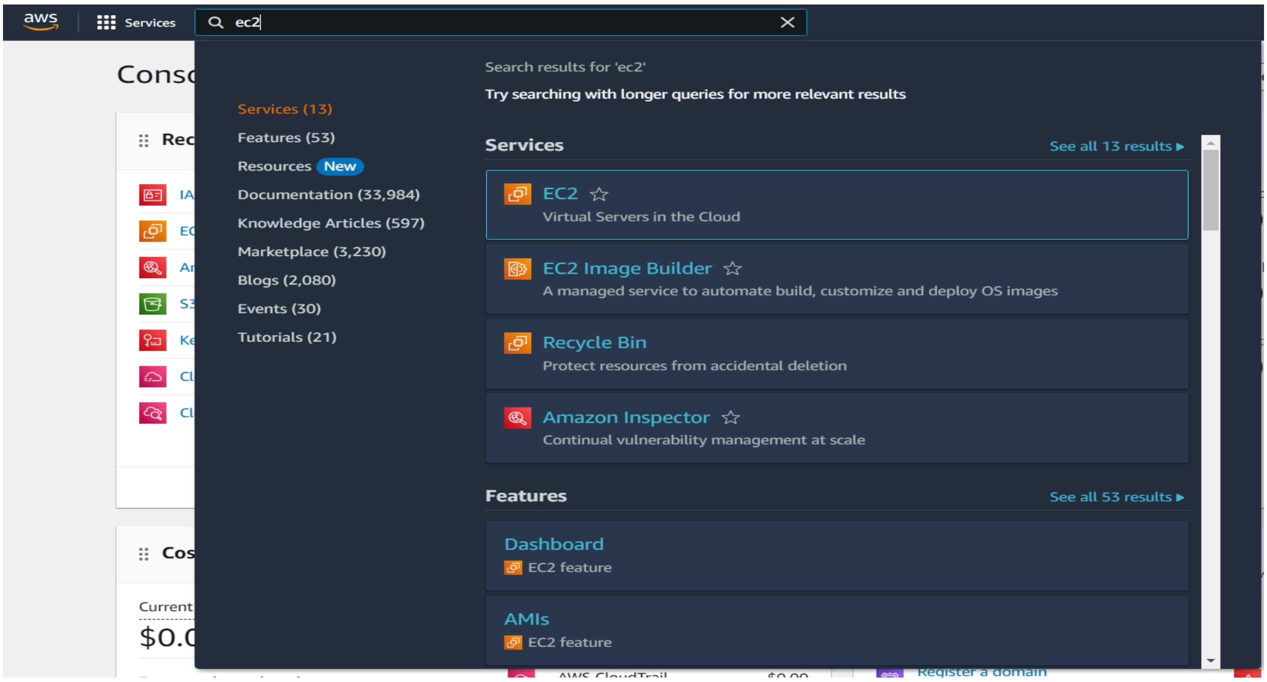
Learn the fundamentals and find valuable information to get the most out of AWS.

Learn from AWS experts and advance your skills and knowledge.

Discover new AWS services, features, and Regions.

Start building with simple wizards and automated workflows.

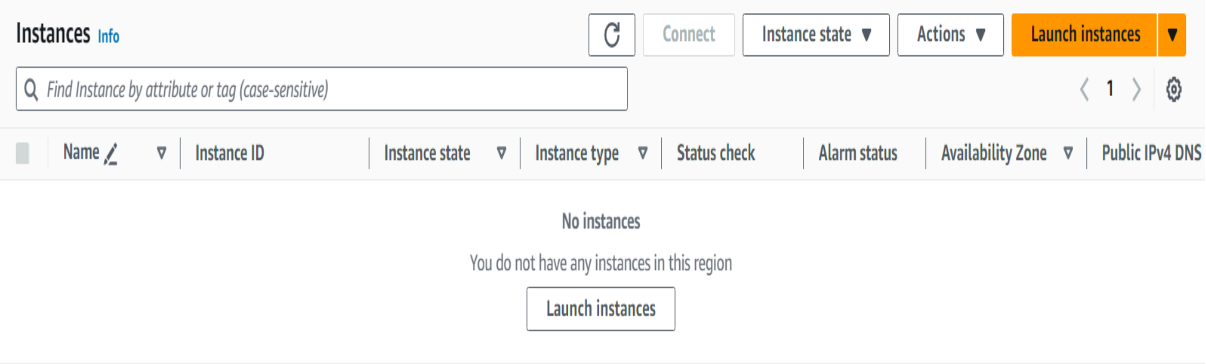
2. Search and click on Ec2.



Search results for 'ec2'

Try searching with longer queries for more relevant results

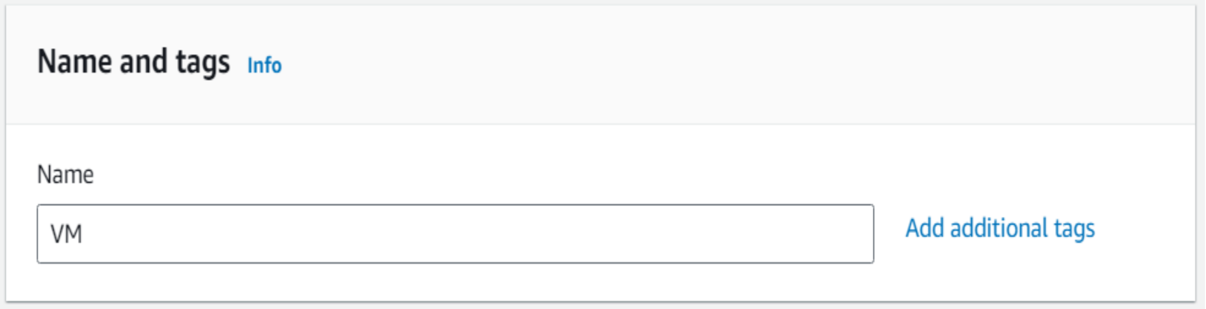
3. Click on “Launch instances”.



No instances

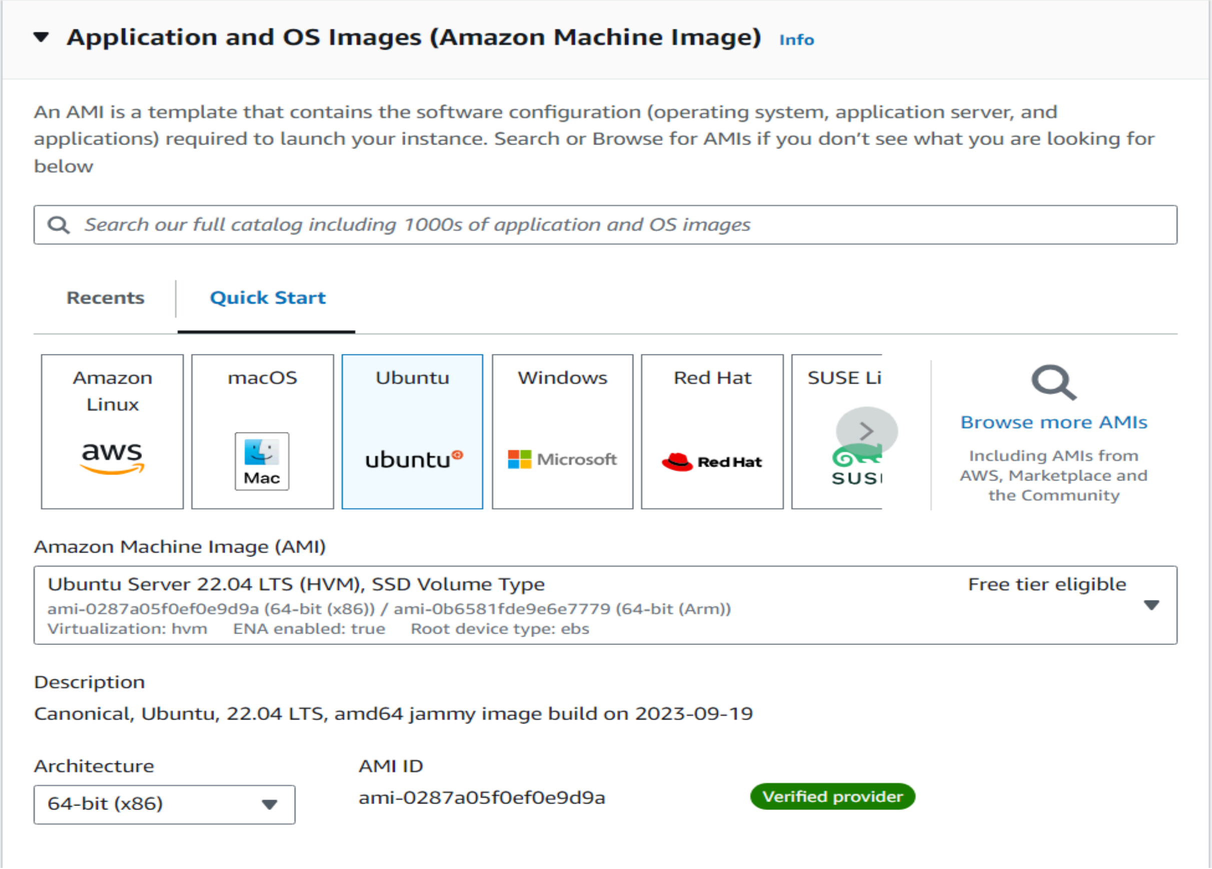
You do not have any instances in this region

4. Give a name to the instance.



Name: VM

5. Select Ubuntu as the OS Image.


Application and OS Images (Amazon Machine Image) Info
Search our full catalog including 1000s of application and OS images
Recents
Quick Start
Amazon Linux
aws
macOS
Mac
Ubuntu
ubuntu
Windows
Microsoft
Red Hat
Red Hat
SUSE Li
SUSI
Browse more AMIs
Including AMIs from AWS, Marketplace and the Community
Verified provider

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

Amazon Machine Image (AMI)

Ubuntu Server 22.04 LTS (HVM), SSD Volume Type — Free tier eligible
ami-0287a05f0ef0e9d9a (64-bit (x86)) / ami-0b6581fde9e6e7779 (64-bit (Arm))
Virtualization: hvm ENA enabled: true Root device type: ebs

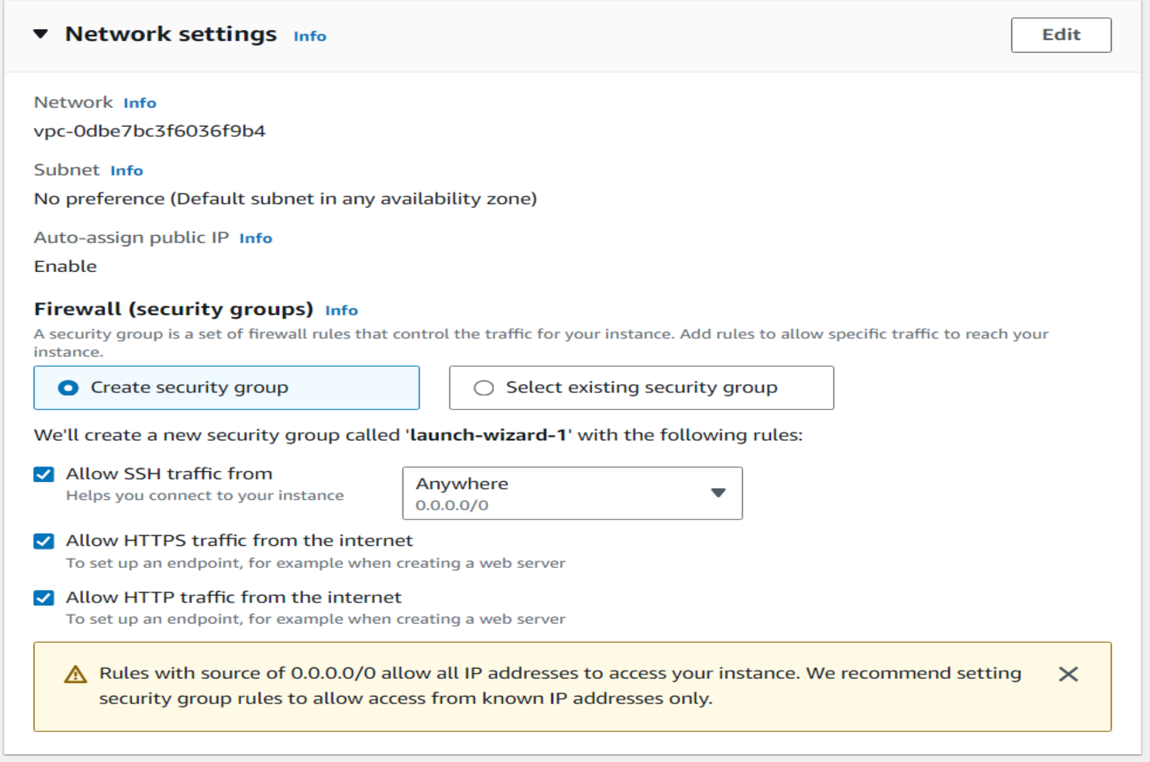
Description

Canonical, Ubuntu, 22.04 LTS, amd64 jammy image build on 2023-09-19

Architecture: 64-bit (x86)

AMI ID: ami-0287a05f0ef0e9d9a

6. Create a security group or select an existing one.



▼ **Network settings** Info

Network Info
vpc-0dbe7bc3f6036f9b4

Subnet Info
No preference (Default subnet in any availability zone)

Auto-assign public IP Info
Enable

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

We'll create a new security group called '**launch-wizard-1**' with the following rules:

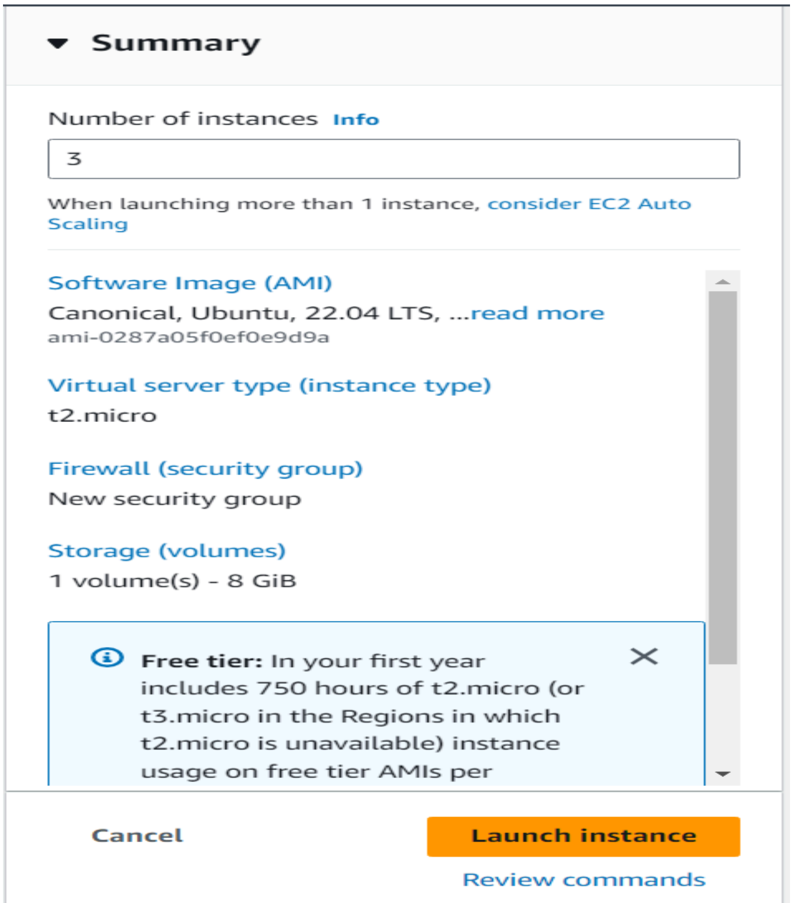
☑ Allow SSH traffic from — Anywhere 0.0.0.0/0
Helps you connect to your instance

☑ Allow HTTPS traffic from the internet
To set up an endpoint, for example when creating a web server

☑ Allow HTTP traffic from the internet
To set up an endpoint, for example when creating a web server

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

7. Set the number of instances to 3 and click on “Launch instance”.



▼ **Summary**

Number of instances Info
3

When launching more than 1 instance, consider EC2 Auto Scaling

Software Image (AMI)
Canonical, Ubuntu, 22.04 LTS, ...read more
ami-0287a05f0ef0e9d9a

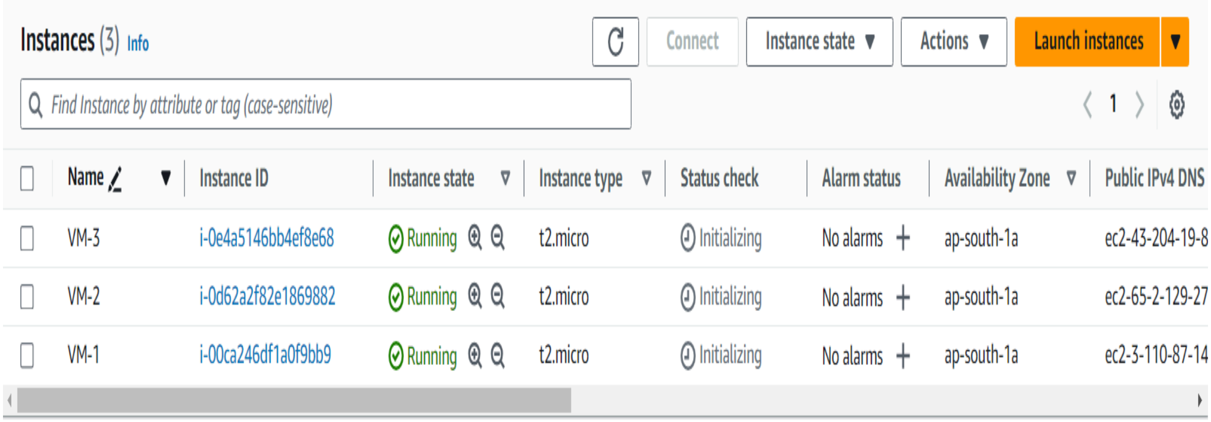
Virtual server type (instance type)
t2.micro

Firewall (security group)
New security group

Storage (volumes)
1 volume(s) - 8 GiB

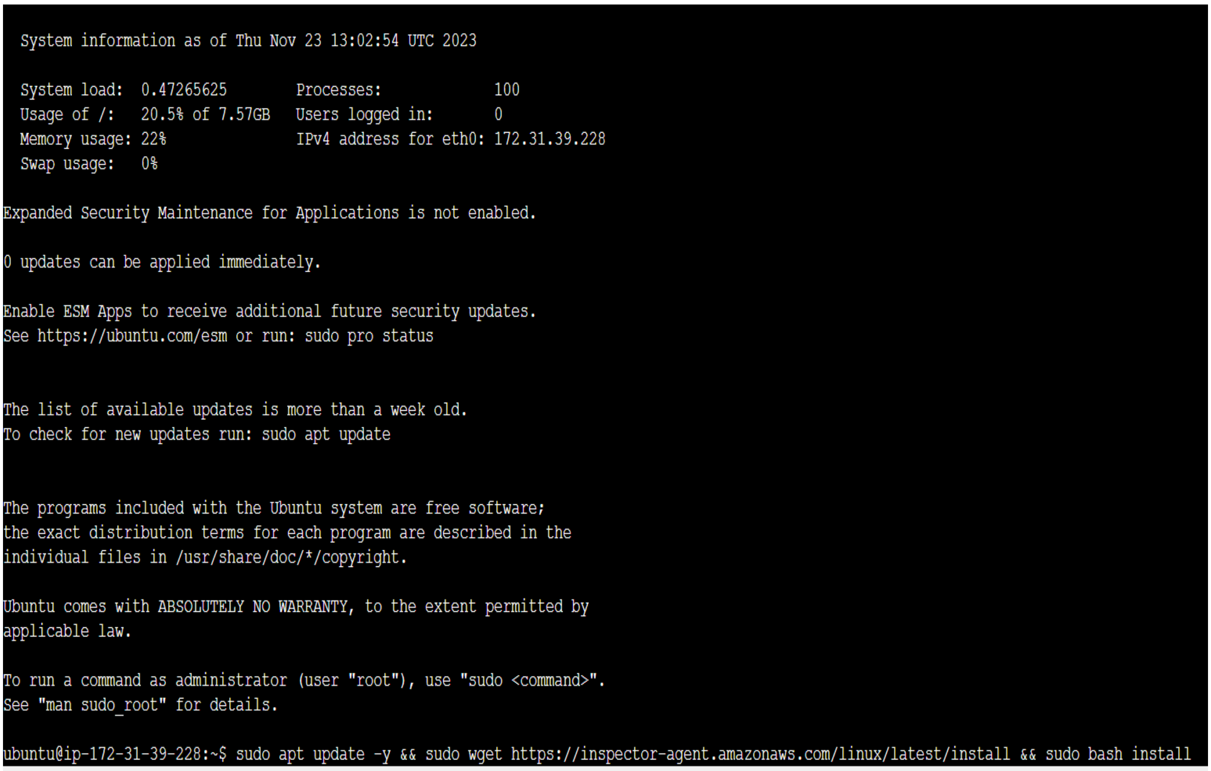
Free tier: In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per

8. Rename the 3 instances to identify them uniquely.



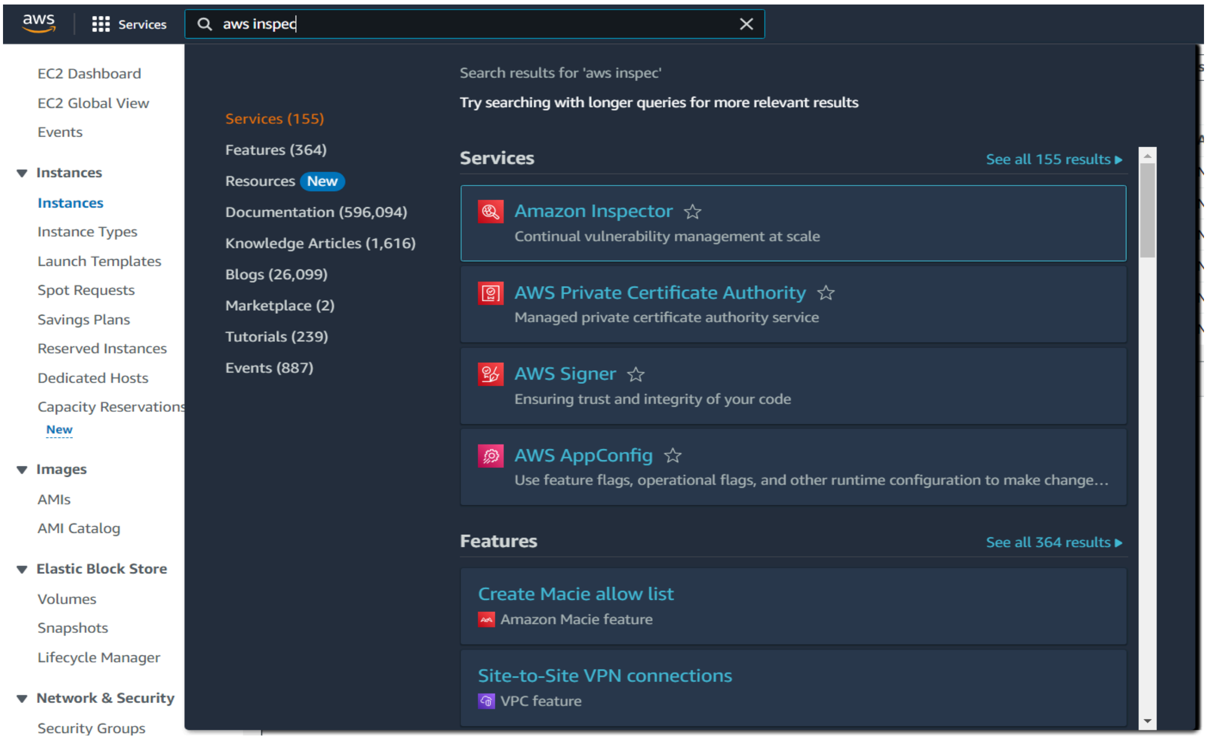
□	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
□	VM-3	i-0e4a5146bb4ef8e68	✓ Running	t2.micro	Initializing	No alarms +	ap-south-1a	ec2-43-204-19-8
□	VM-2	i-0d62a2f82e1869882	✓ Running	t2.micro	Initializing	No alarms +	ap-south-1a	ec2-65-2-129-27
□	VM-1	i-00ca246df1a0f9bb9	✓ Running	t2.micro	Initializing	No alarms +	ap-south-1a	ec2-3-110-87-14

9. Connect one instance and fire the command "sudo apt update -y && sudo wget https://inspector-agent.amazonaws.com/linux/latest/install && sudo bash install". Repeat the same for the other 2 instances.



```
  System information as of Thu Nov 23 13:02:54 UTC 2023

  System load:  0.47265625        Processes:             100
  Usage of /:   20.5% of 7.57GB   Users logged in:       0
  Memory usage: 22%               IPv4 address for eth0: 172.31.39.228
  Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

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


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


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ip-172-31-39-228:~$ sudo apt update -y && sudo wget https://inspector-agent.amazonaws.com/linux/latest/install && sudo bash install
```

10. Now search for Amazon Inspector and click on it.



Search results for 'aws inspec'

Try searching with longer queries for more relevant results

Amazon Inspector ☆
Continual vulnerability management at scale

AWS Private Certificate Authority ☆
Managed private certificate authority service

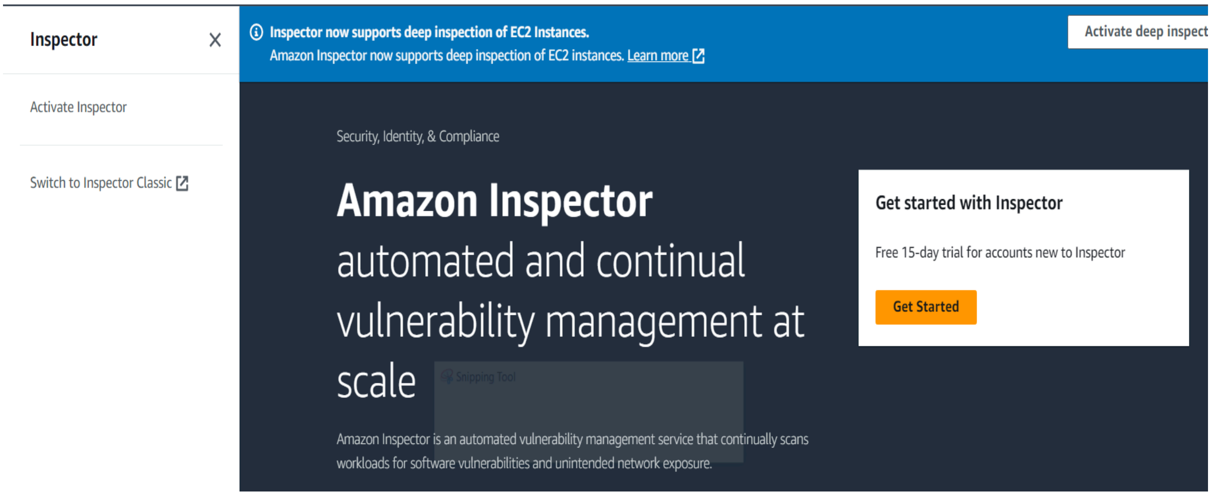
AWS Signer ☆
Ensuring trust and integrity of your code

AWS AppConfig ☆
Use feature flags, operational flags, and other runtime configuration to make change…

Create Macie allow list
Amazon Macie feature

Site-to-Site VPN connections
VPC feature

11. Click on the side menu icon and click on “Switch to Inspector Classic”.



Inspector now supports deep inspection of EC2 Instances.
Amazon Inspector now supports deep inspection of EC2 instances. Learn more

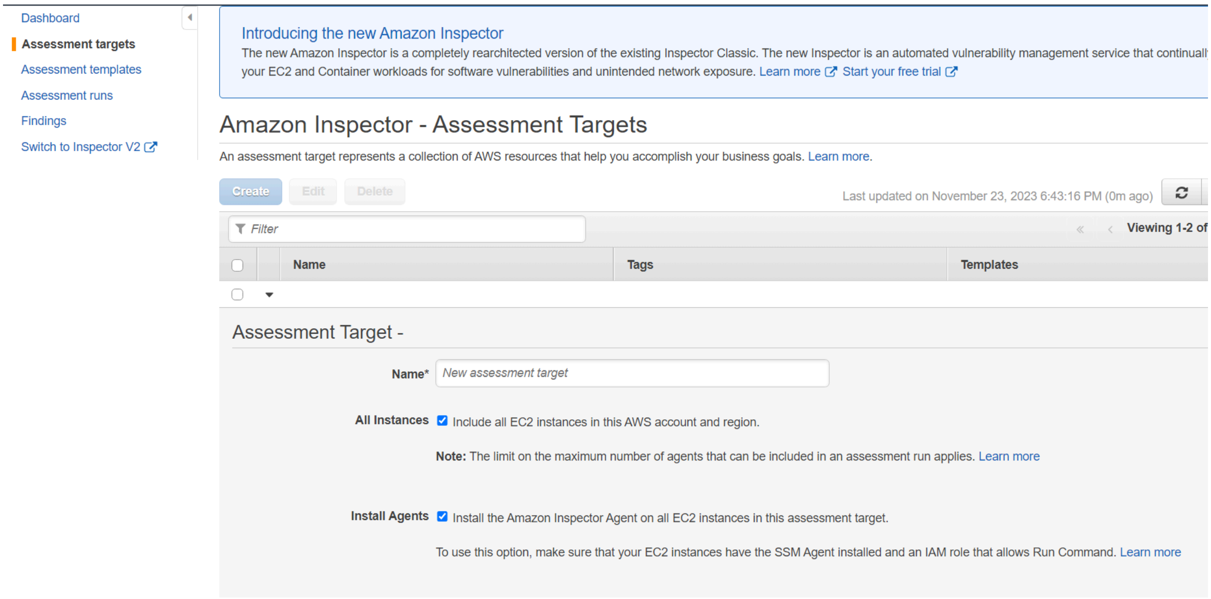
Amazon Inspector
automated and continual vulnerability management at scale

Amazon Inspector is an automated vulnerability management service that continually scans workloads for software vulnerabilities and unintended network exposure.

Get started with Inspector

Free 15-day trial for accounts new to Inspector

12. Create an assessment target, give a name to it, Check to “include all EC2 instances in this AWS account and region” and then click “Save” below.



Introducing the new Amazon Inspector

The new Amazon Inspector is a completely rearchitected version of the existing Inspector Classic. The new Inspector is an automated vulnerability management service that continuall your EC2 and Container workloads for software vulnerabilities and unintended network exposure. Learn more Start your free trial

Amazon Inspector - Assessment Targets

An assessment target represents a collection of AWS resources that help you accomplish your business goals. Learn more.

Last updated on November 23, 2023 6:43:16 PM (0m ago)

□	Name	Tags	Templates

Assessment Target -

Name* New assessment target

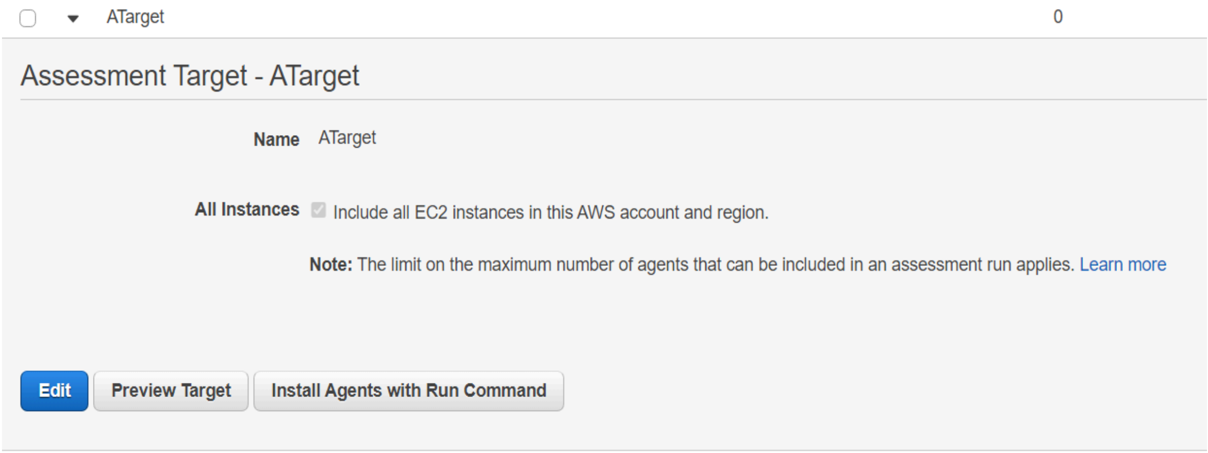
All Instances ☑ Include all EC2 instances in this AWS account and region.

Note: The limit on the maximum number of agents that can be included in an assessment run applies. Learn more

Install Agents ☑ Install the Amazon Inspector Agent on all EC2 instances in this assessment target.

To use this option, make sure that your EC2 instances have the SSM Agent installed and an IAM role that allows Run Command. Learn more

13. Then open the target by clicking on dropdown and click on “Install Agents with Run Command”.



□ ATarget 0

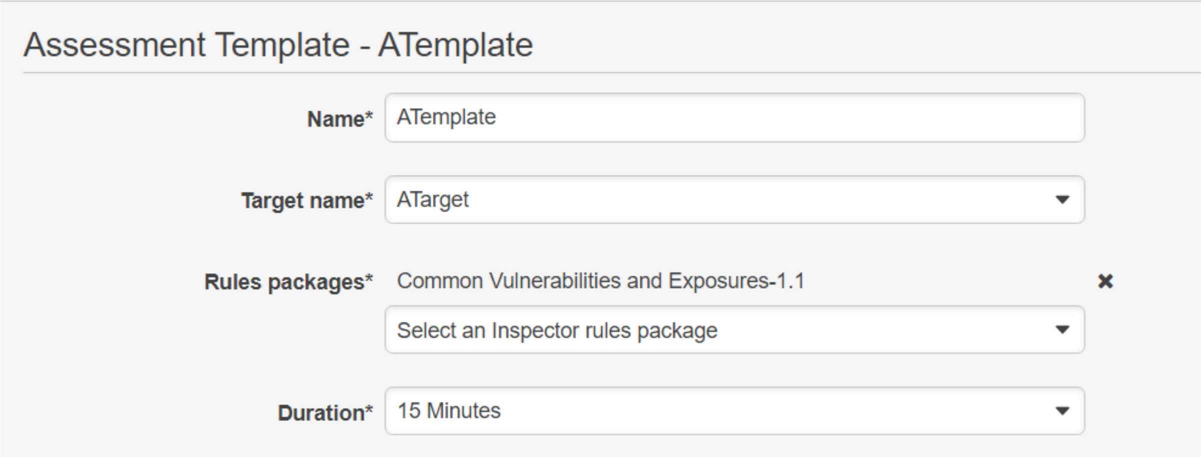
Assessment Target - ATarget

Name ATarget

All Instances ☑ Include all EC2 instances in this AWS account and region.

Note: The limit on the maximum number of agents that can be included in an assessment run applies. Learn more

14. Create an Assessment Template, give a name, select the target, select rules packages as “Common Vulnerabilities and Exposures-1.1”, set the Duration to 15 Minutes and then click on save.



Assessment Template - ATemplate

Name* ATemplate

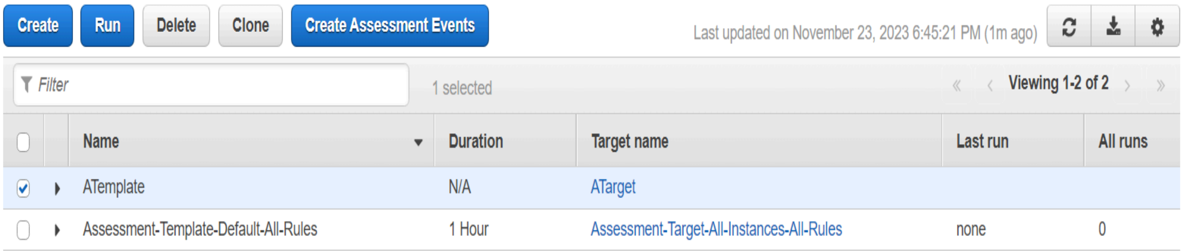
Target name* ATarget

Rules packages* Common Vulnerabilities and Exposures-1.1 ✖

Select an Inspector rules package

Duration* 15 Minutes

15. Now select the template and click on run and then wait for 15 minutes.



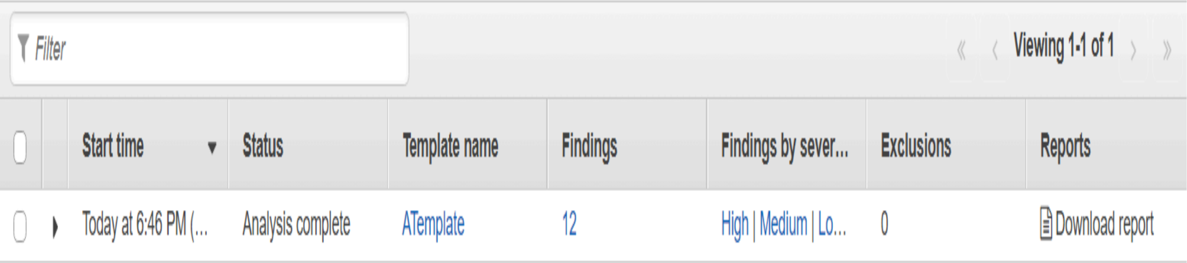
Last updated on November 23, 2023 6:45:21 PM (1m ago)

1 selected

Viewing 1-2 of 2

		Name	Duration	Target name	Last run	All runs
☑	▸	ATemplate	N/A	ATarget		
□	▸	Assessment-Template-Default-All-Rules	1 Hour	Assessment-Target-All-Instances-All-Rules	none	0

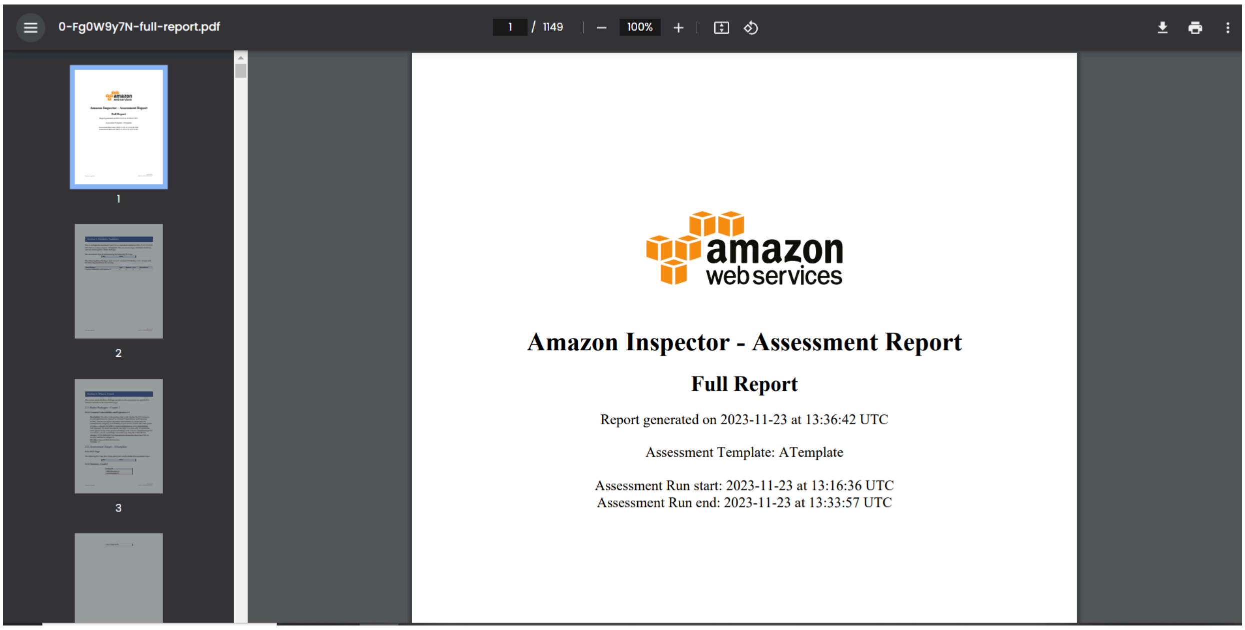
16. After the set duration, in the Assessment runs, the report gets ready. Click on Download report



Viewing 1-1 of 1

		Start time	Status	Template name	Findings	Findings by sever...	Exclusions	Reports
□	▸	Today at 6:46 PM (...	Analysis complete	ATemplate	12	High | Medium | Lo...	0	Download report

17. The pdf report will be opened in a new tab



amazon web services

Amazon Inspector - Assessment Report

Full Report

Report generated on 2023-11-23 at 13:36:42 UTC

Assessment Template: ATemplate

Assessment Run start: 2023-11-23 at 13:16:36 UTC
Assessment Run end: 2023-11-23 at 13:33:57 UTC