AWS inspector , Shield and WAF

AWS inspector :

Checks the vulnerability and potential security threats of your ec2 machine

An AWS service to test the network accessibility if your amazon ec2 instances and security state of your application that run on that instances

Example: if you have created an ec2 machine and you leave port 81 which is ftp port open …then the inspector will tell you that this machine the port is enabled via which the hacker might get inside your system

- AWS inspector performs an assessment on the target ec2 instances and check for vulnerabilities and security threats
- Install an agent on target ec2 instances
- Amazon inspect will collect the information of the network and tell you the vulnerabilities which can be improvised

WAF :

Web application firewall .

Lets you monitor http and https request that are forwarded to an Amazon API gateway , cloudfront (CDN service) or an application load balancer

Shield :

Aws shield is managed DDOS protection service provided by aws to protect applications and services hosted on aws.

It provides scalable , automatic protection against DDos attacks that target web applications , Api and network infrastructure

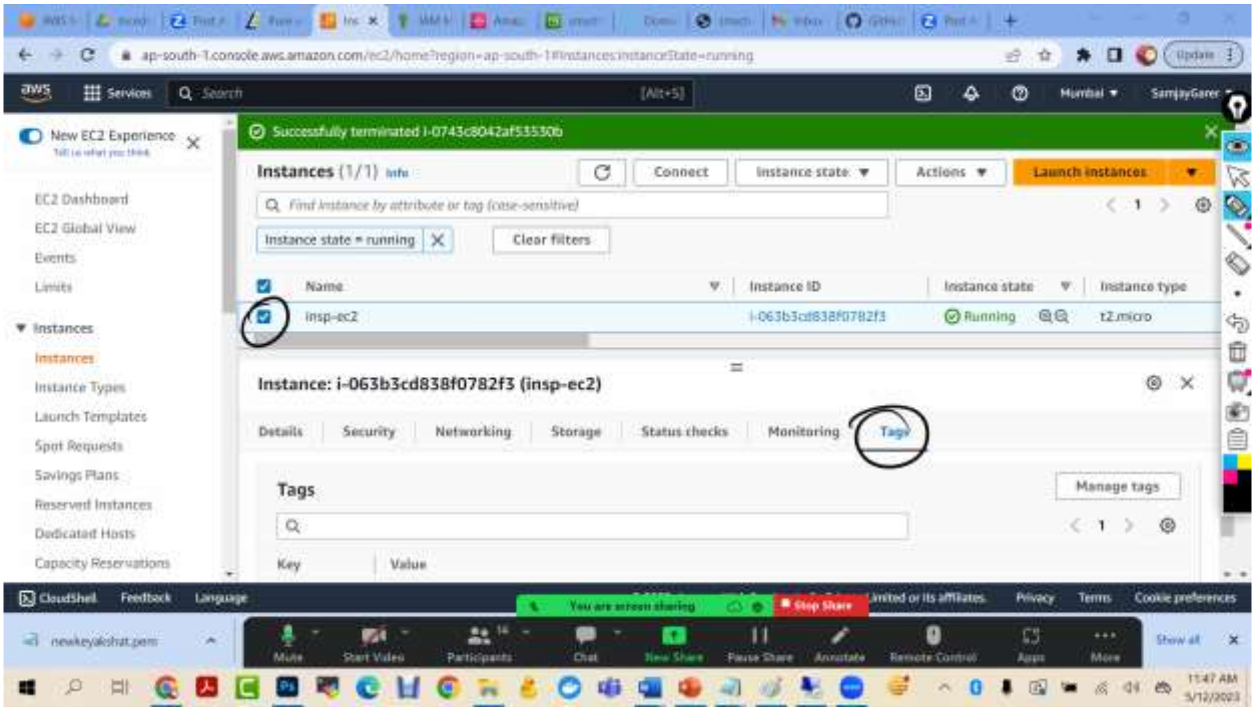
Shield is automatically enabled for Aws customer without any charge .

Lab:

We have a production ec2 instance for which we need to perform a network accessibility check . We will leverage the amazon inspector to perfrom this n/w accessibility check .,

To induce security threat we will open port 21 on our ec2 instance . Port 21 is associated with FTP and it is generally not recommended to keep it open on your production instances.

1) Launch amazon linux ec2 machine and keep port 21 open (inbound rules)



ap-south-1.console.aws.amazon.com/ec2/home?region=ap-south-1#Instances:instanceState=running

Successfully terminated i-0743c8042af53530b

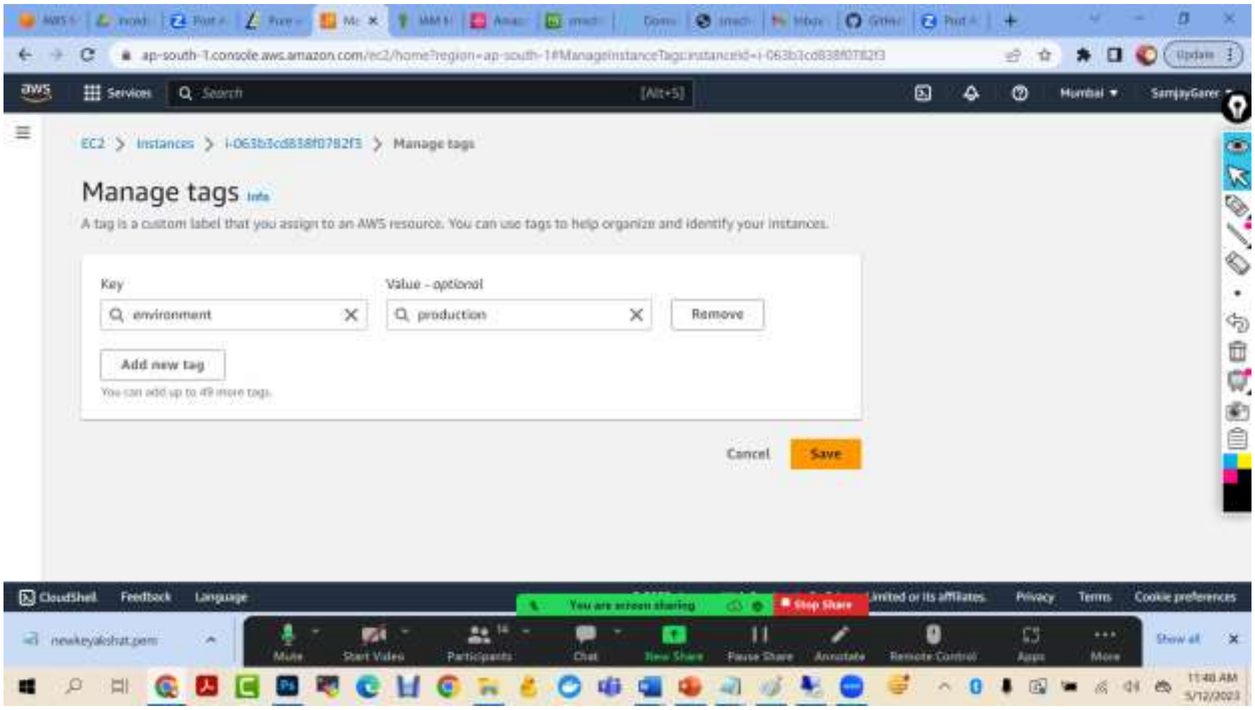
Instances (1/1)

Instance state = running

Name	Instance ID	Instance state	Instance type
insp-ec2	i-063b3cd838f0782f3	Running	t2.micro

Instance: i-063b3cd838f0782f3 (insp-ec2)

Add tags to the taget group ….key : environment and value: production



EC2 > Instances > i-063b3cd838f0782f3 > Manage tags

Manage tags Info

A tag is a custom label that you assign to an AWS resource. You can use tags to help organize and identify your instances.

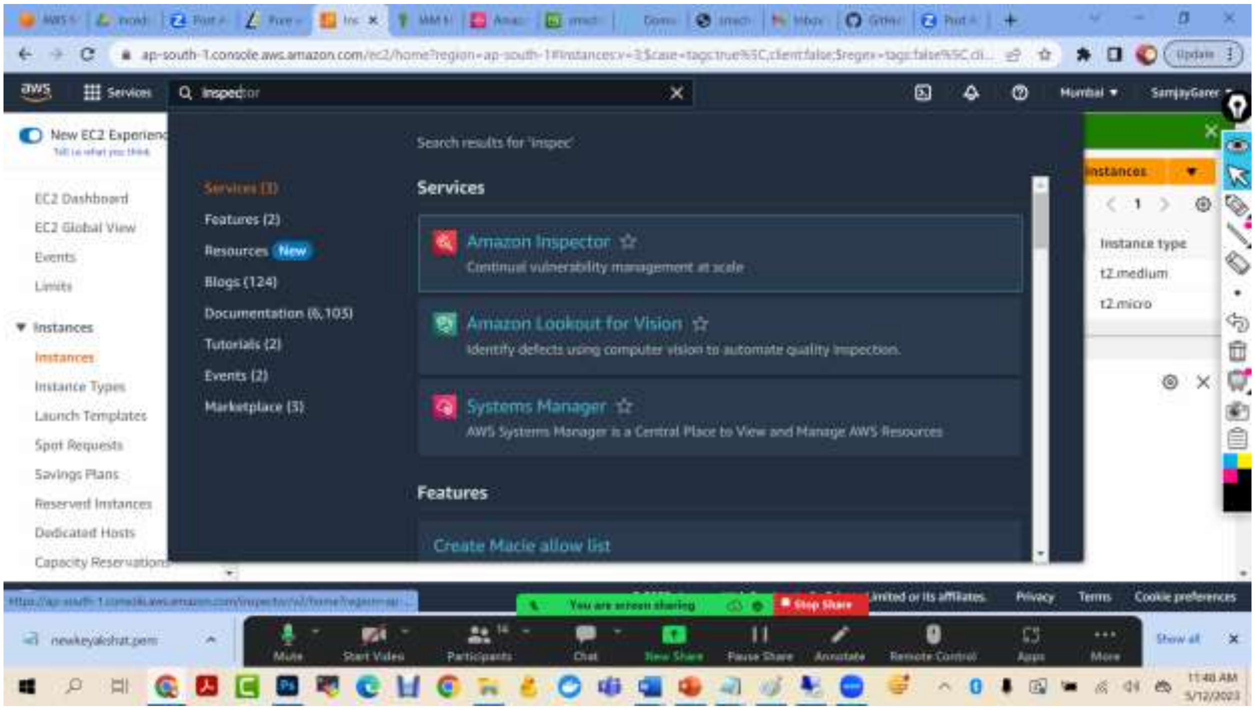
Key	Value - optional
environment	production

Remove

Add new tag

You can add up to 49 more tags.

Cancel Save



Search: inspector

Search results for 'inspec'

Services (3)
Features (2)
Resources New
Blogs (124)
Documentation (6,103)
Tutorials (2)
Events (2)
Marketplace (3)

Services

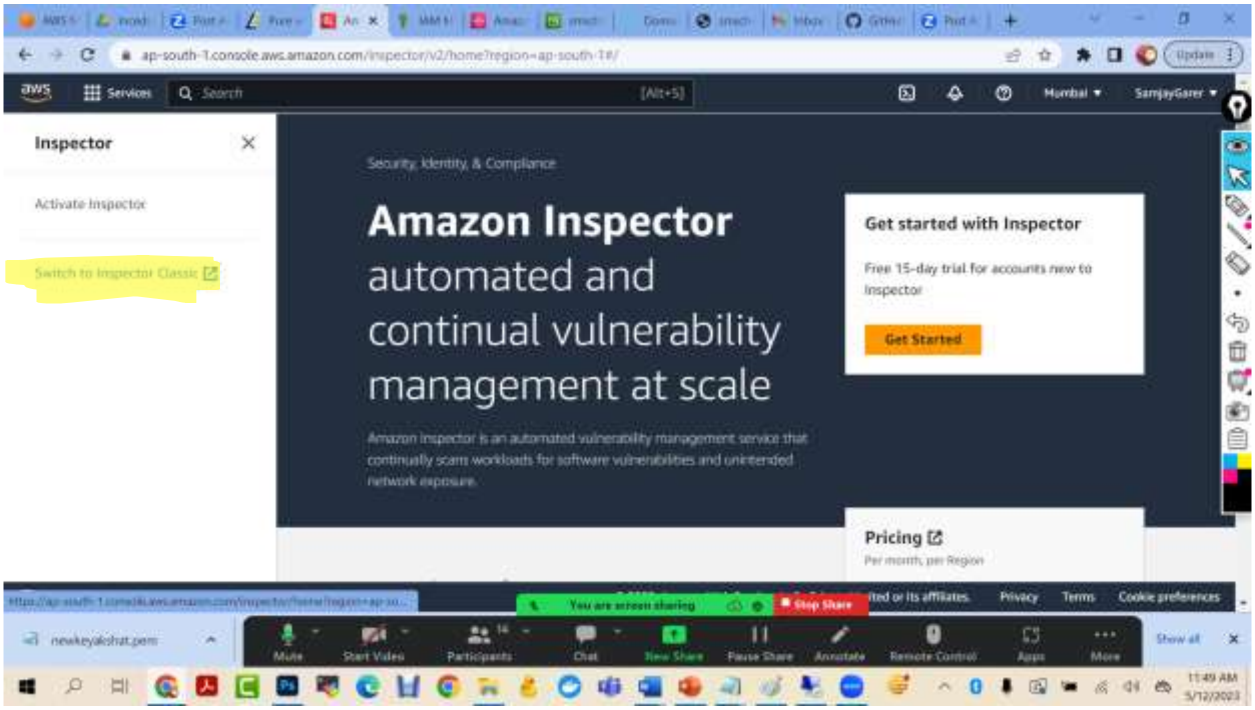
Amazon Inspector ☆
Continual vulnerability management at scale

Amazon Lookout for Vision ☆
Identify defects using computer vision to automate quality inspection.

Systems Manager ☆
AWS Systems Manager is a Central Place to View and Manage AWS Resources

Features

Create Macie allow list



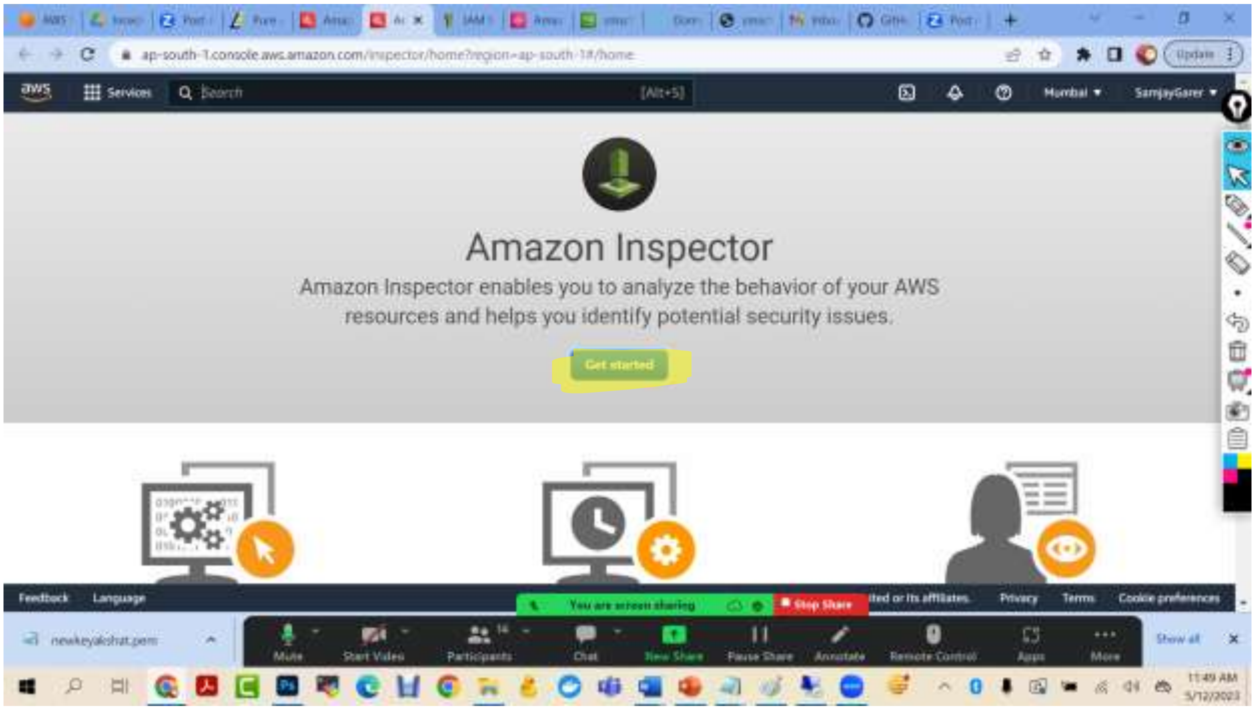
Security, Identity, & Compliance

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.

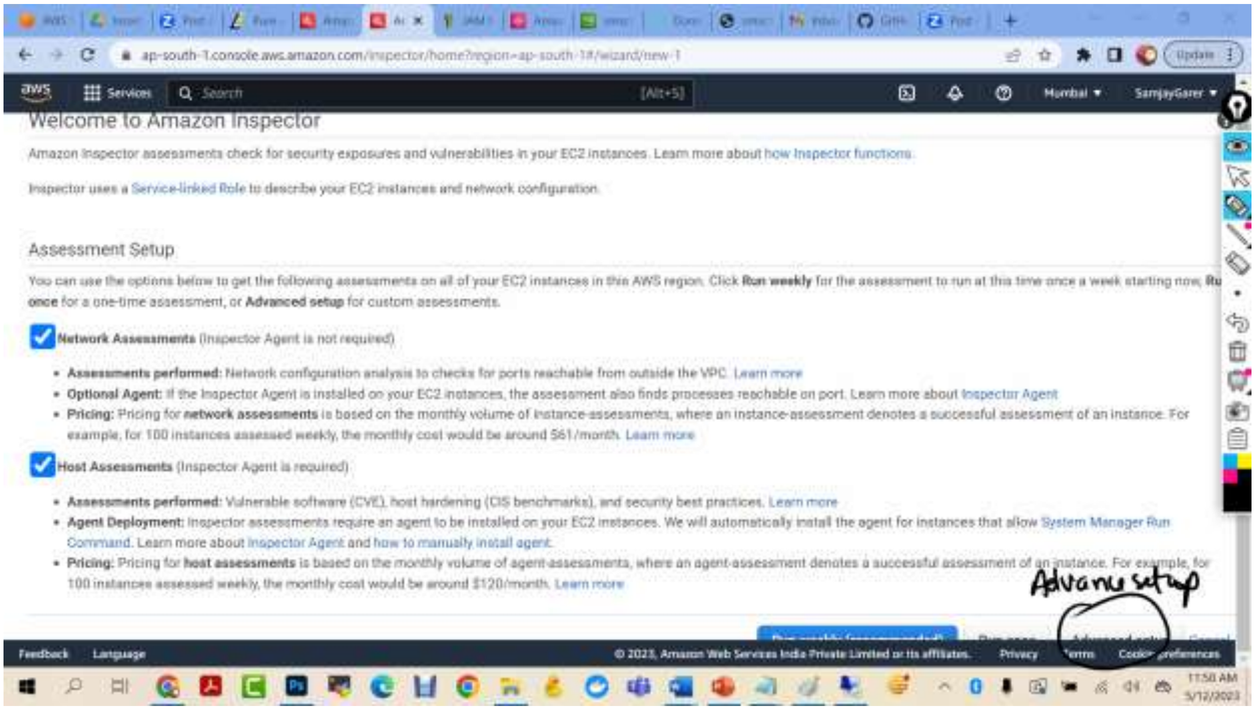
Get started with Inspector

Free 15-day trial for accounts new to Inspector



Amazon Inspector

Amazon Inspector enables you to analyze the behavior of your AWS resources and helps you identify potential security issues.



ap-south-1.console.aws.amazon.com/inspector/home?region=ap-south-1#/wizard/new-1

Welcome to Amazon Inspector

Amazon Inspector assessments check for security exposures and vulnerabilities in your EC2 instances. Learn more about how Inspector functions.

Inspector uses a Service-linked Role to describe your EC2 instances and network configuration.

Assessment Setup

You can use the options below to get the following assessments on all of your EC2 instances in this AWS region. Click **Run weekly** for the assessment to run at this time once a week starting now, **Run once** for a one-time assessment, or **Advanced setup** for custom assessments.

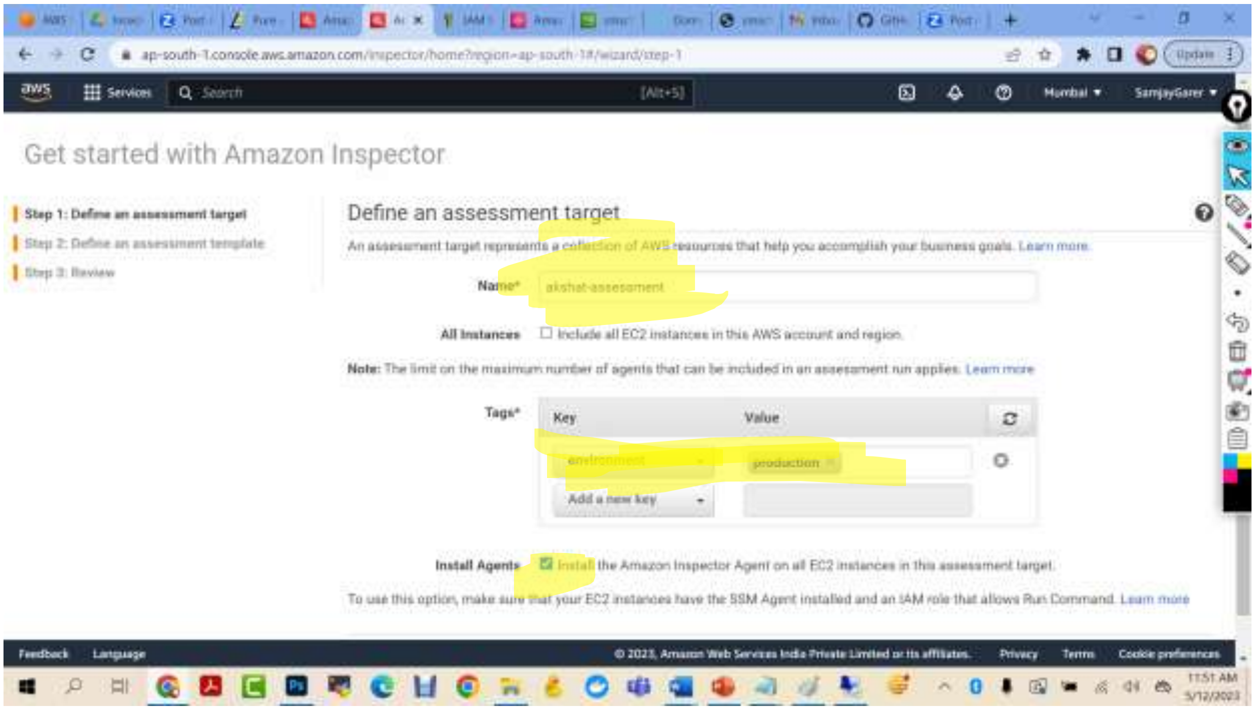
☑ **Network Assessments** (Inspector Agent is not required)

- **Assessments performed:** Network configuration analysis to checks for ports reachable from outside the VPC. Learn more
- **Optional Agent:** If the Inspector Agent is installed on your EC2 instances, the assesment also finds processes reachable on port. Learn more about Inspector Agent
- **Pricing:** Pricing for **network assessments** is based on the monthly volume of instance-assessments, where an instance-assessment denotes a successful assessment of an instance. For example, for 100 instances assessed weekly, the monthly cost would be around $61/month. Learn more

☑ **Host Assessments** (Inspector Agent is required)

- **Assessments performed:** Vulnerable software (CVE), host hardening (CIS benchmarks), and security best practices. Learn more
- **Agent Deployment:** Inspector assessments require an agent to be installed on your EC2 instances. We will automatically install the agent for instances that allow System Manager Run Command. Learn more about Inspector Agent and how to manually install agent.
- **Pricing:** Pricing for **host assessments** is based on the monthly volume of agent-assessments, where an agent-assessment denotes a successful assessment of an instance. For example, for 100 instances assessed weekly, the monthly cost would be around $120/month. Learn more

Advance setup



ap-south-1.console.aws.amazon.com/inspector/home?region=ap-south-1#/wizard/step-1

Get started with Amazon Inspector

Step 1: Define an assessment target

Step 2: Define an assessment template

Step 3: Review

Define an assessment target

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

Name* akshat-assessment

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

Tags*

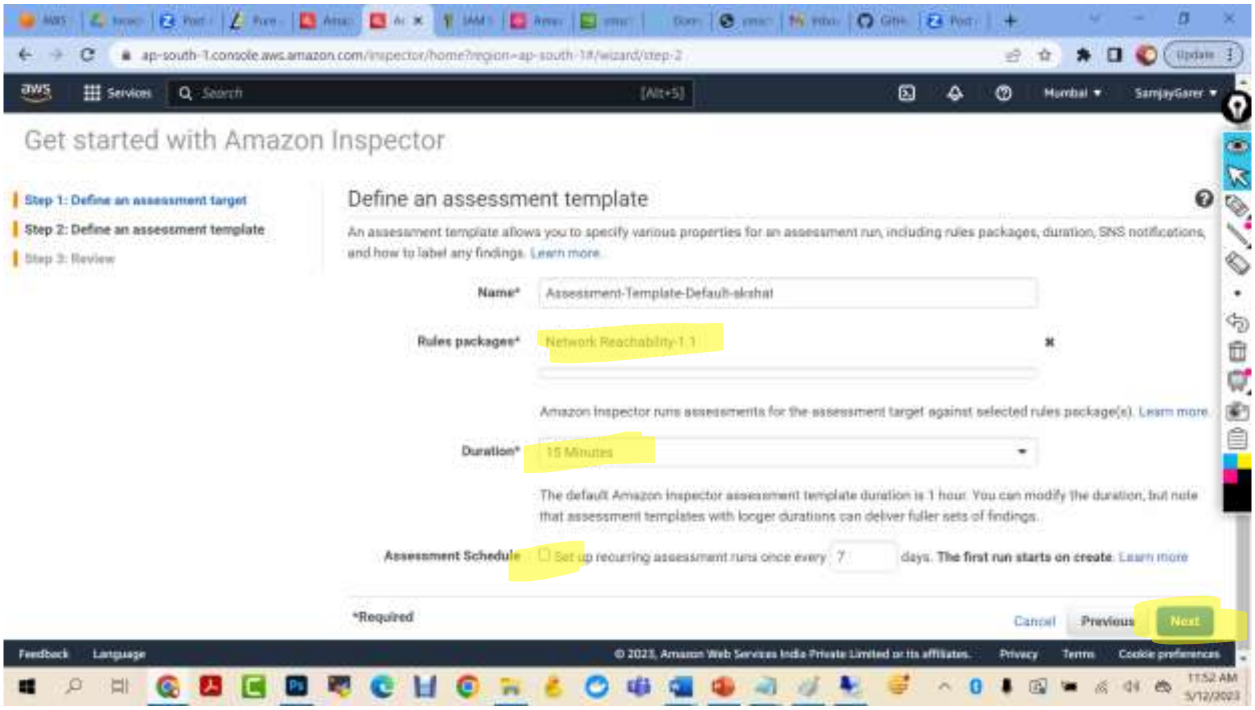
Key	Value
environment	production
Add a new key	

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

Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
11:51 AM
5/12/2023

Next



Get started with Amazon Inspector

- Step 1: Define an assessment target
- Step 2: Define an assessment template
- Step 3: Review

Define an assessment template

An assessment template allows you to specify various properties for an assessment run, including rules packages, duration, SNS notifications, and how to label any findings. Learn more

Name* Assessment-Template-Default-akshat

Rules packages* Network Reachability-1.1

Amazon Inspector runs assessments for the assessment target against selected rules package(s). Learn more

Duration* 15 Minutes

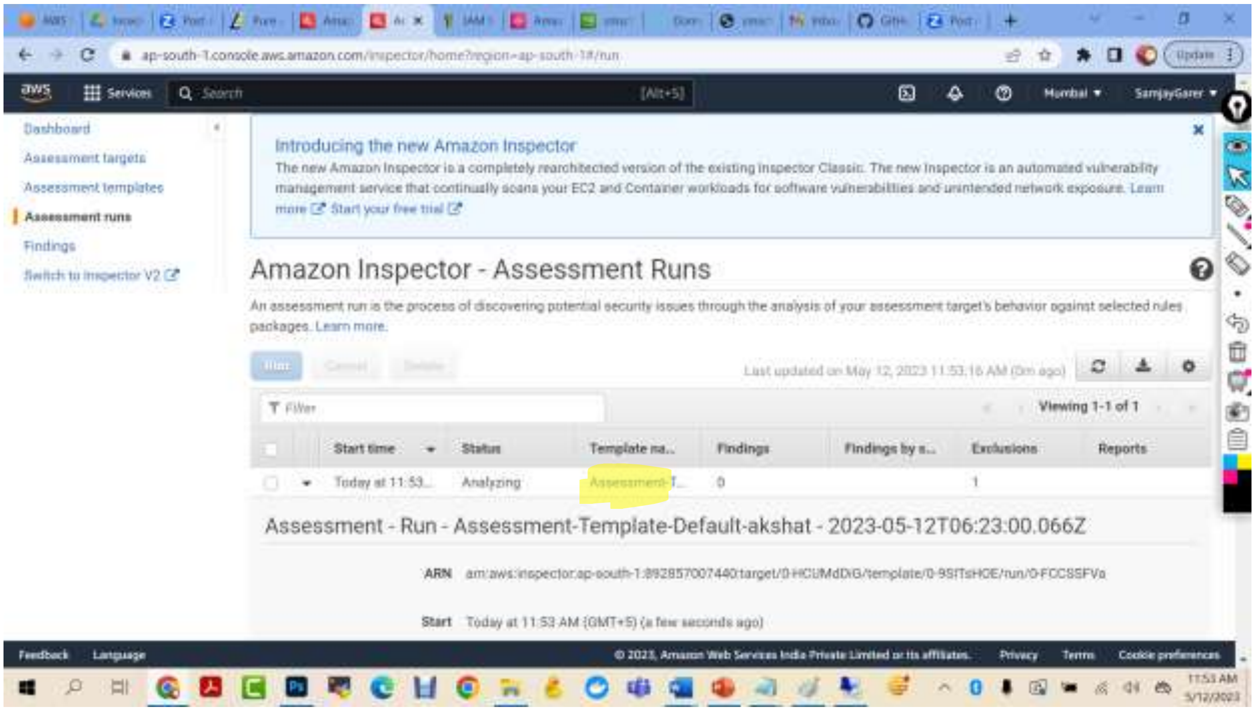
The default Amazon Inspector assessment template duration is 1 hour. You can modify the duration, but note that assessment templates with longer durations can deliver fuller sets of findings.

Assessment Schedule □ Set up recurring assessment runs once every 7 days. The first run starts on create. Learn more

*Required

Uncheck the assessment schedule

Create



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 continually scans your EC2 and Container workloads for software vulnerabilities and unintended network exposure. Learn more Start your free trial

Amazon Inspector - Assessment Runs

An assessment run is the process of discovering potential security issues through the analysis of your assessment target's behavior against selected rules packages. Learn more.

Last updated on May 12, 2023 11:53:16 AM (0m ago)

Viewing 1-1 of 1

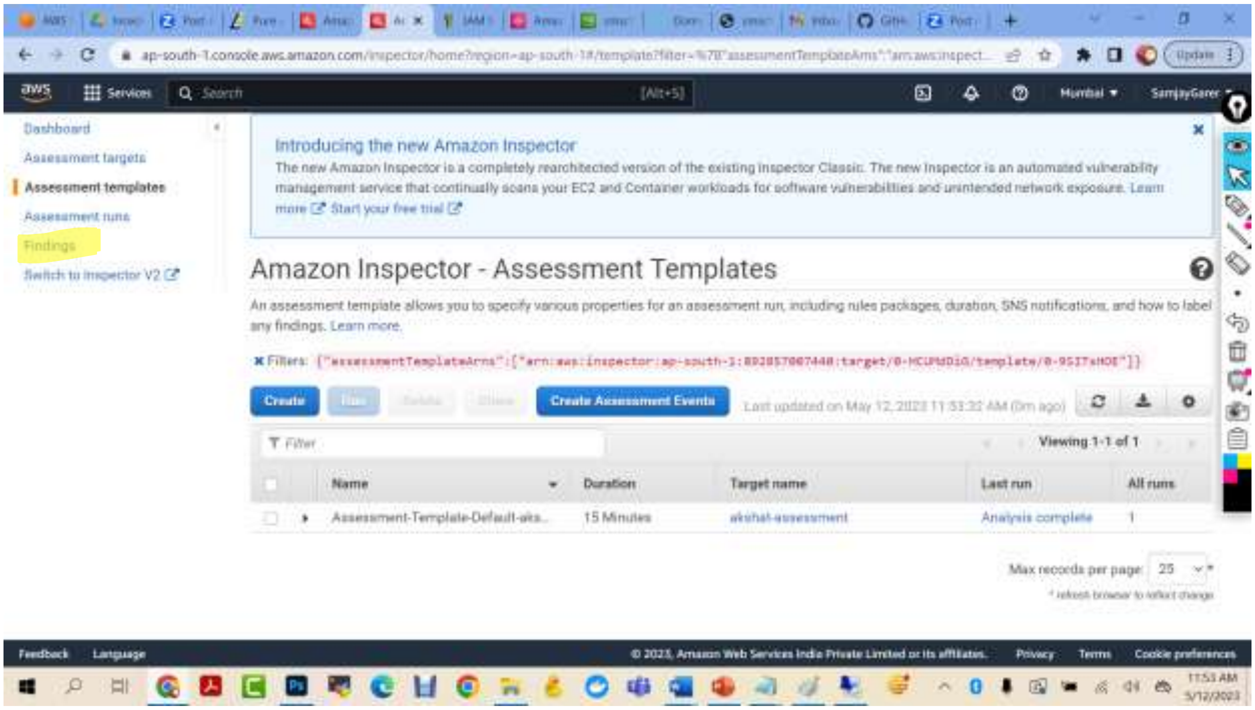
	Start time	Status	Template na...	Findings	Findings by s...	Exclusions	Reports
□	Today at 11:53...	Analyzing	Assessment-T...	0		1	

Assessment - Run - Assessment-Template-Default-akshat - 2023-05-12T06:23:00.066Z

ARN arn:aws:inspector:ap-south-1:892857007440:target/0-HCUMdDiG/template/0-9SITsHOE/run/0-FCCSSFVa

Start Today at 11:53 AM (GMT+5) (a few seconds ago)

Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
11:53 AM
5/12/2023



ap-south-1.console.aws.amazon.com/inspector/home?region=ap-south-1#/template?filter=%7B"assessmentTemplateArns":"arn:aws:inspect...

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 continually scans your EC2 and Container workloads for software vulnerabilities and unintended network exposure. Learn more Start your free trial

Amazon Inspector - Assessment Templates

An assessment template allows you to specify various properties for an assessment run, including rules packages, duration, SNS notifications, and how to label any findings. Learn more.

Filters: {"assessmentTemplateArns":["arn:aws:inspector:ap-south-1:892857007448:target/0-HCUMdDiG/template/0-9SI7sHOE"]}

Last updated on May 12, 2023 11:53:32 AM (0m ago)

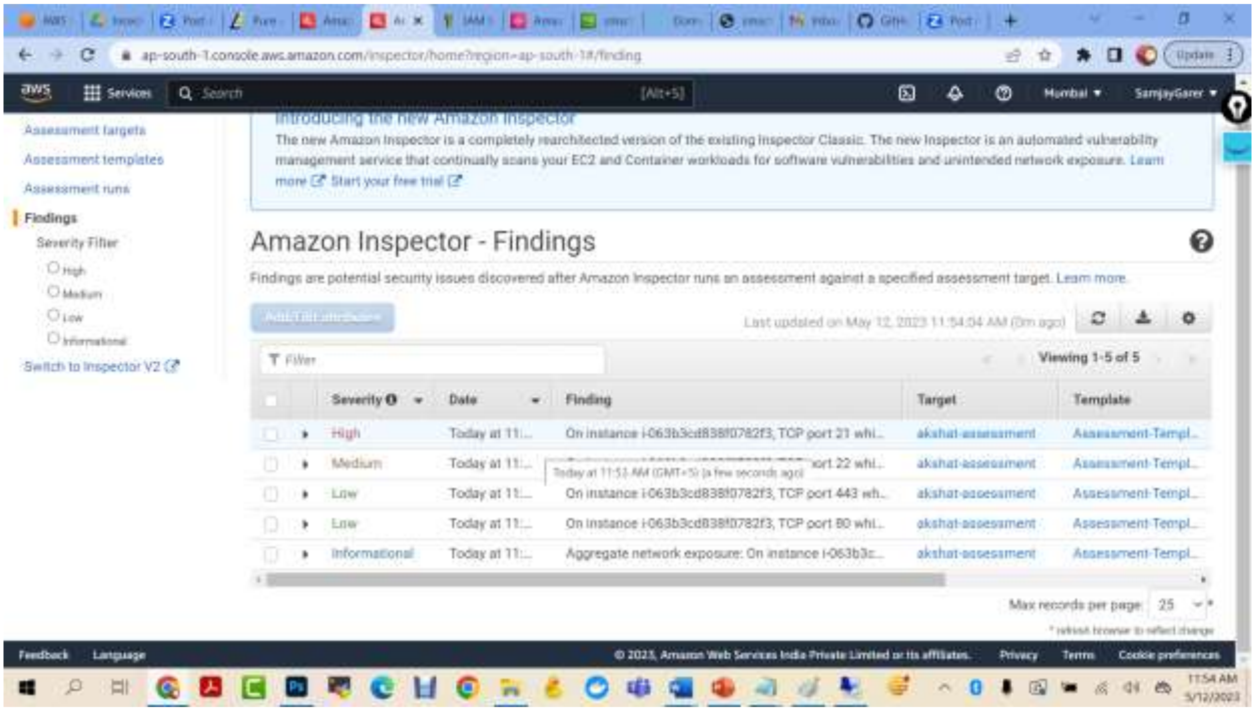
Viewing 1-1 of 1

Name	Duration	Target name	Last run	All runs
Assessment-Template-Default-aks...	15 Minutes	akshat-assessment	Analysis complete	1

Max records per page: 25

* refresh browser to reflect change

Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
11:53 AM
5/12/2023



ap-south-1.console.aws.amazon.com/inspector/home?region=ap-south-1#/finding

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 continually scans your EC2 and Container workloads for software vulnerabilities and unintended network exposure. Learn more Start your free trial

Amazon Inspector - Findings

Findings are potential security issues discovered after Amazon Inspector runs an assessment against a specified assessment target. Learn more.

Last updated on May 12, 2023 11:54:04 AM (0m ago)

Viewing 1-5 of 5

Severity	Date	Finding	Target	Template
High	Today at 11:...	On instance i-063b3cd838f0782f3, TCP port 21 whi...	akshat-assessment	Assessment-Templ...
Medium	Today at 11:...	...ort 22 whi...	akshat-assessment	Assessment-Templ...
Low	Today at 11:...	On instance i-063b3cd838f0782f3, TCP port 443 wh...	akshat-assessment	Assessment-Templ...
Low	Today at 11:...	On instance i-063b3cd838f0782f3, TCP port 80 whi...	akshat-assessment	Assessment-Templ...
Informational	Today at 11:...	Aggregate network exposure: On instance i-063b3c...	akshat-assessment	Assessment-Templ...

Today at 11:53 AM (GMT+5) (a few seconds ago)

Max records per page: 25

* refresh browser to reflect change

Feedback
Language
© 2023, Amazon Web Services India Private Limited or its affiliates.
Privacy
Terms
Cookie preferences
11:54 AM
5/12/2023

You can check the details of high medium low informational data via clicking on it