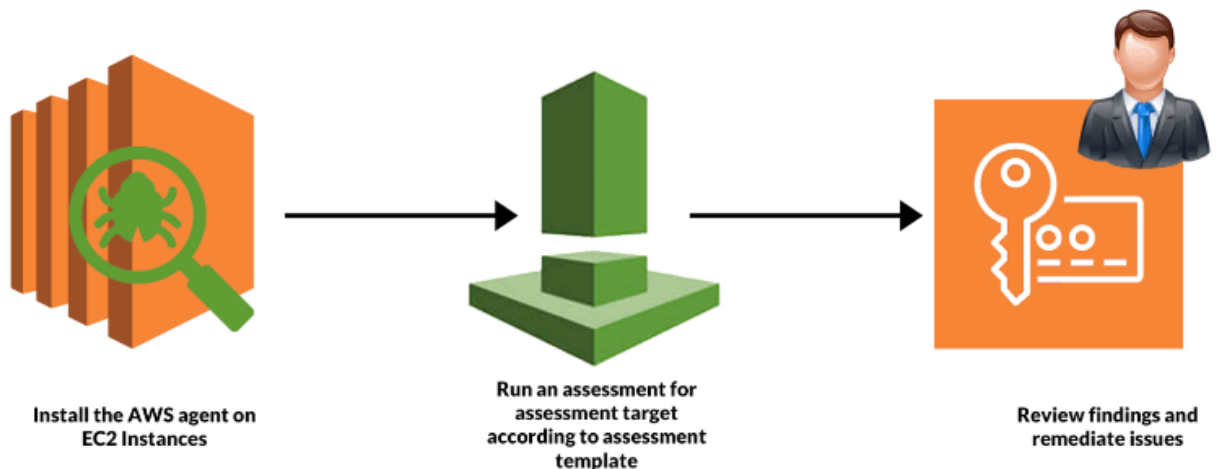


AWS INSPECTOR

Amazon Inspector is an automated security assessment service to test the network accessibility of EC2 instances. It helps you to identify vulnerabilities within your EC2 instances and applications. And allows you to make security testing more regular occurrence as part of the development and IT operations.

Amazon Inspector provides a clear list of security and compliance findings assigned a priority by the severity level. Moreover, these findings can be analyzed directly or as part of comprehensive assessment records available via the API or AWS Inspector console. AWS Inspector security assessments help you check for unintended network accessibility of EC2 instances and vulnerabilities on those EC2 instances.

How Amazon Inspector Works?

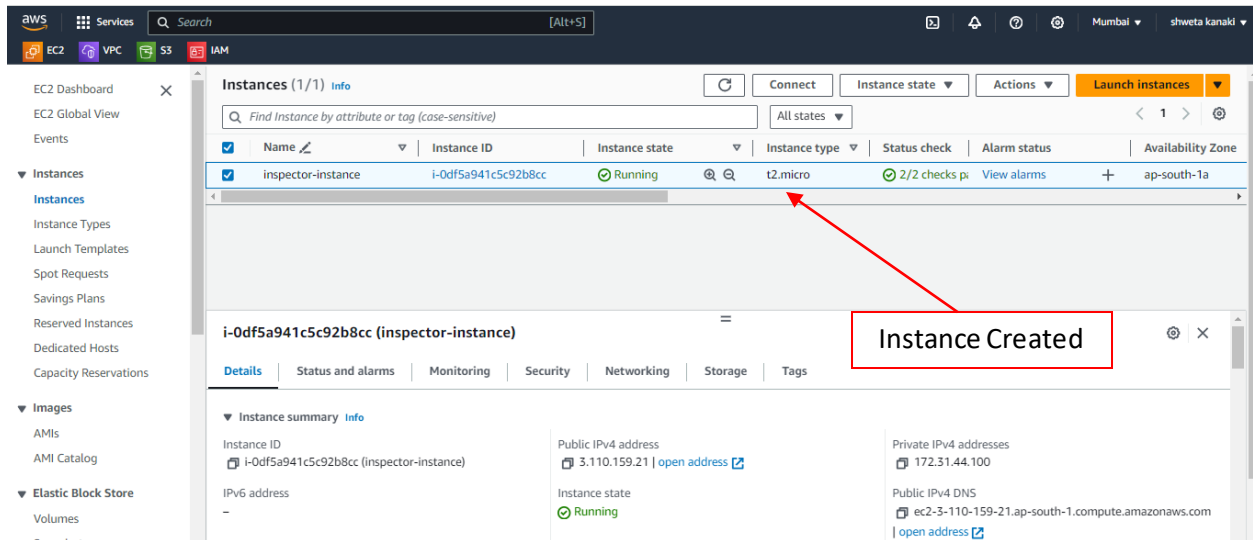


Amazon Inspector performs an automatic assessment and generates a findings report containing steps to keep the environment safe. To use this service, you need to define the collection of AWS and all the resources that complete the application to proceed and tested. It is followed by adding and performing security practices. You can also set the duration of that assessment which can vary from 15 Min to 12 Hrs or last for one day.

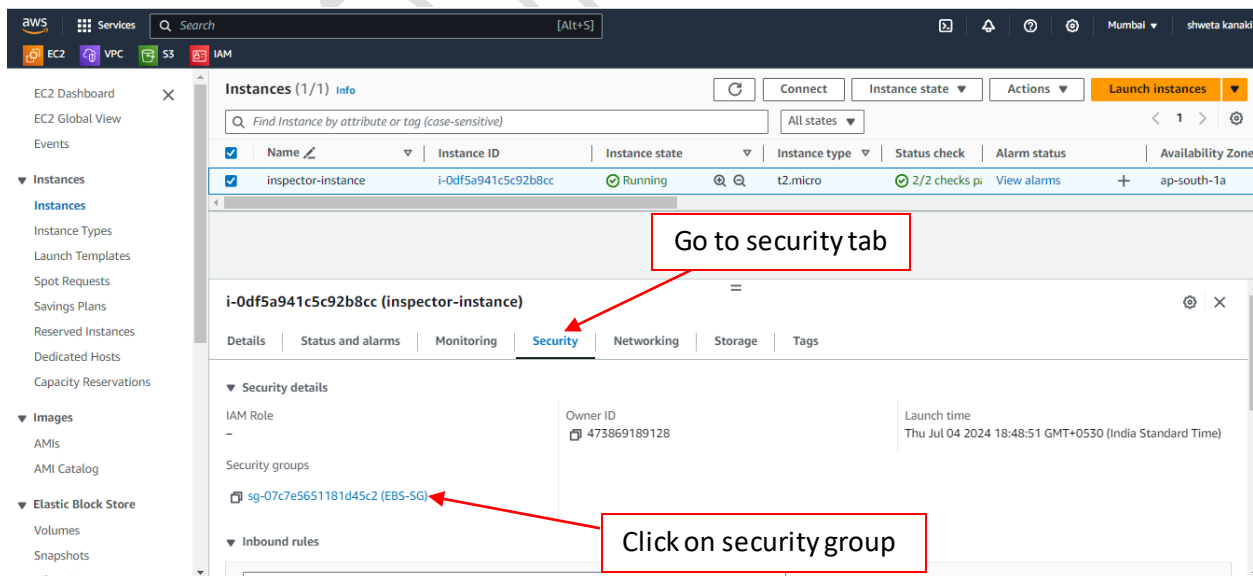
An Inspector Agent runs on the EC2 machines hosting the application that monitors the network, file system, and process activity. After collecting all the required data, it is compared with the built-in security rules to identify security or compliance issues.

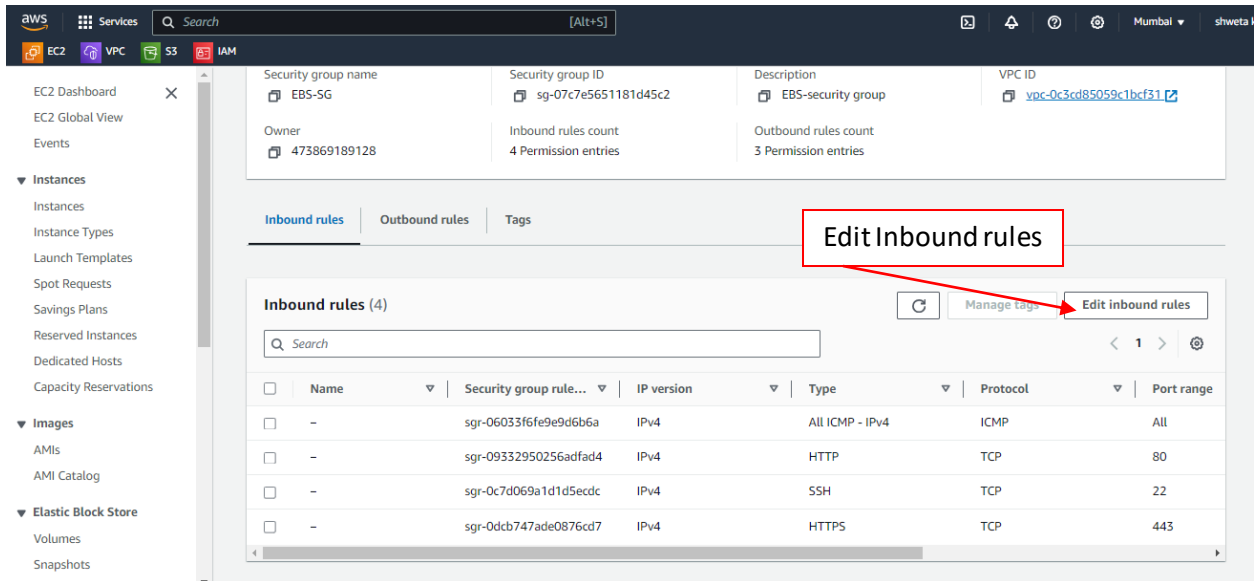
GETTING STARTED WITH AMAZON INSPECTOR

Step 1: Create a EC2 instance



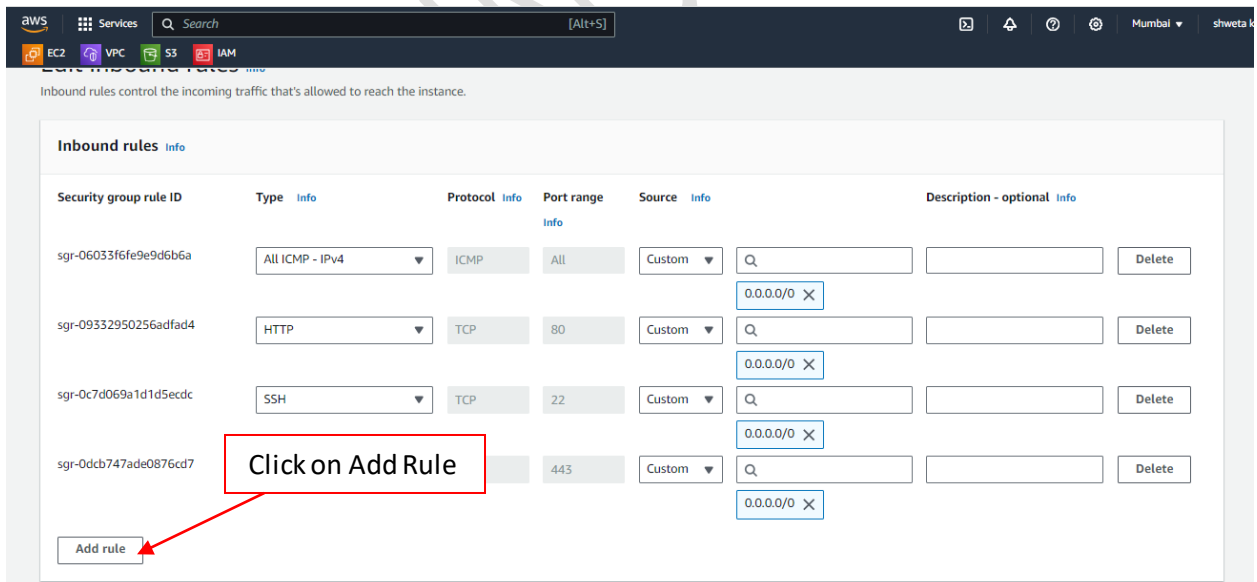
Step 2: Modify Security Group





Edit Inbound rules

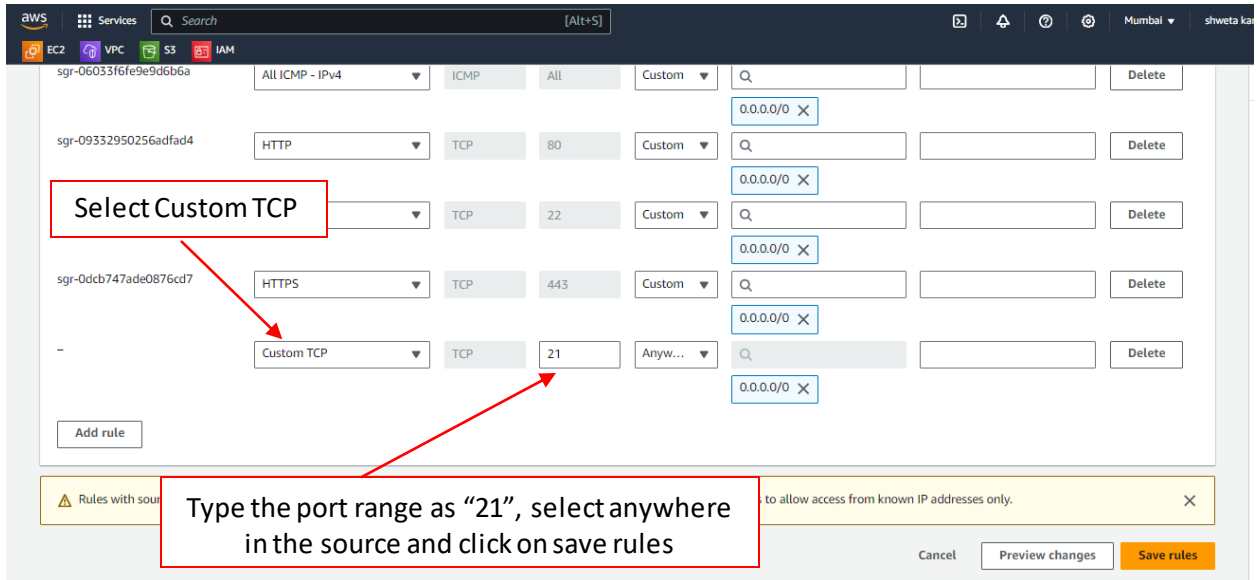
Name	Security group rule...	IP version	Type	Protocol	Port range
-	sgr-06033f6fe9e9d6b6a	IPv4	All ICMP - IPv4	ICMP	All
-	sgr-09332950256adfad4	IPv4	HTTP	TCP	80
-	sgr-0c7d069a1d1d5ecdc	IPv4	SSH	TCP	22
-	sgr-0dcb747ade0876cd7	IPv4	HTTPS	TCP	443



Click on Add Rule

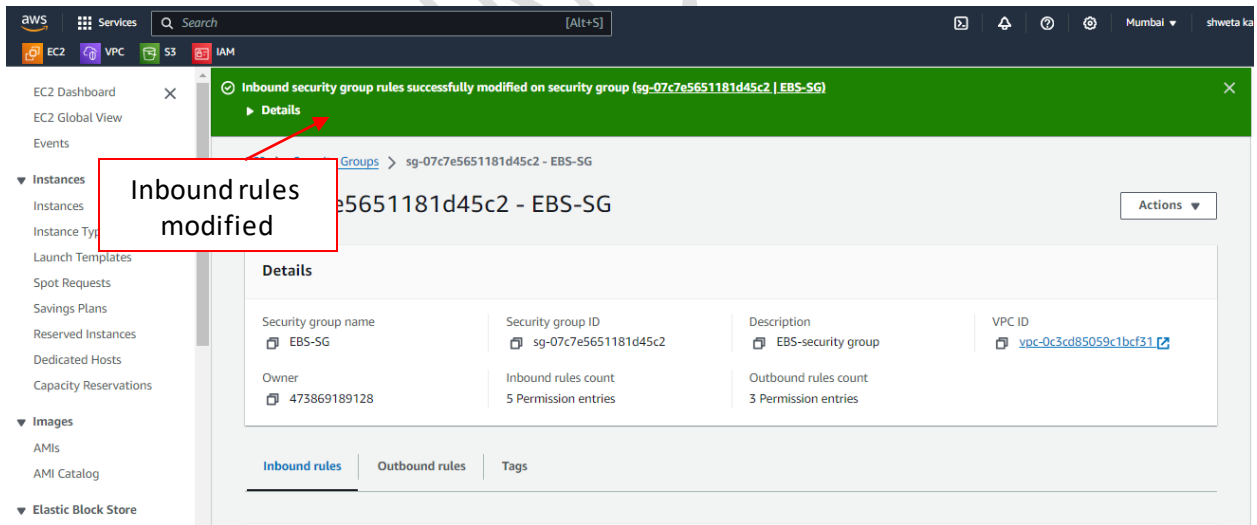
Security group rule ID	Type	Protocol	Port range	Source	Description - optional	Actions
sgr-06033f6fe9e9d6b6a	All ICMP - IPv4	ICMP	All	Custom		Delete
sgr-09332950256adfad4	HTTP	TCP	80	Custom		Delete
sgr-0c7d069a1d1d5ecdc	SSH	TCP	22	Custom		Delete
sgr-0dcb747ade0876cd7			443	Custom		Delete

Add rule



Select Custom TCP

Type the port range as "21", select anywhere in the source and click on save rules



Inbound rules modified

Inbound security group rules successfully modified on security group (sg-07c7e5651181d45c2 | EBS-SG)

Details

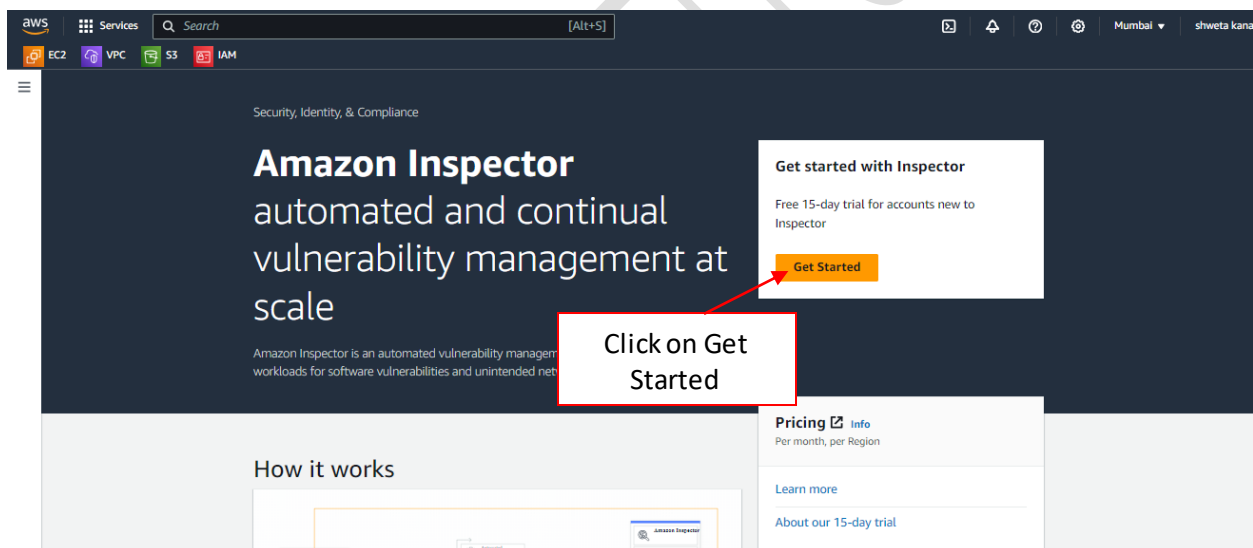
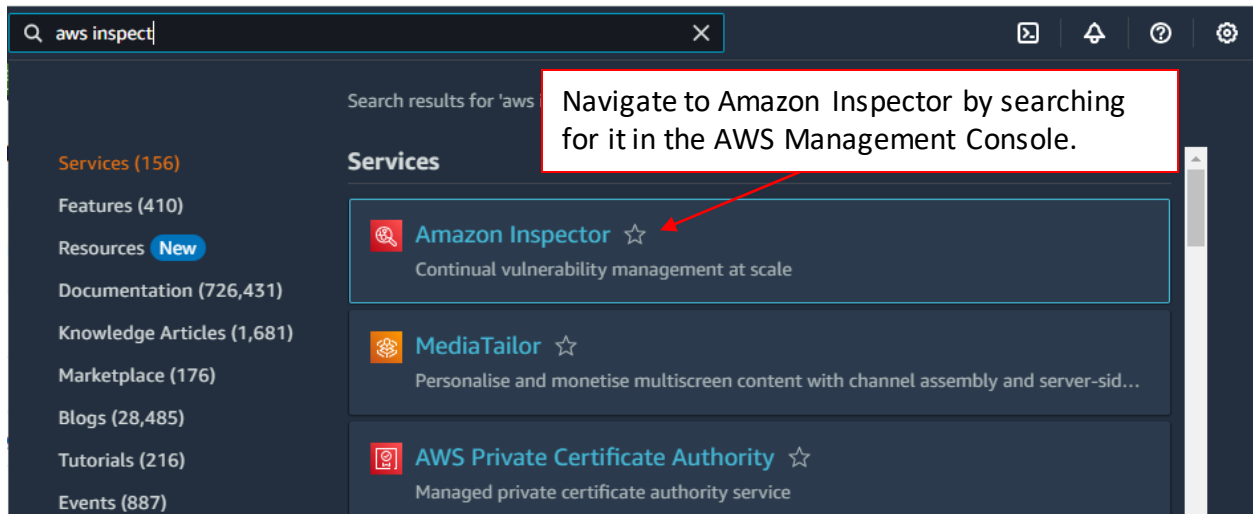
Groups > sg-07c7e5651181d45c2 - EBS-SG

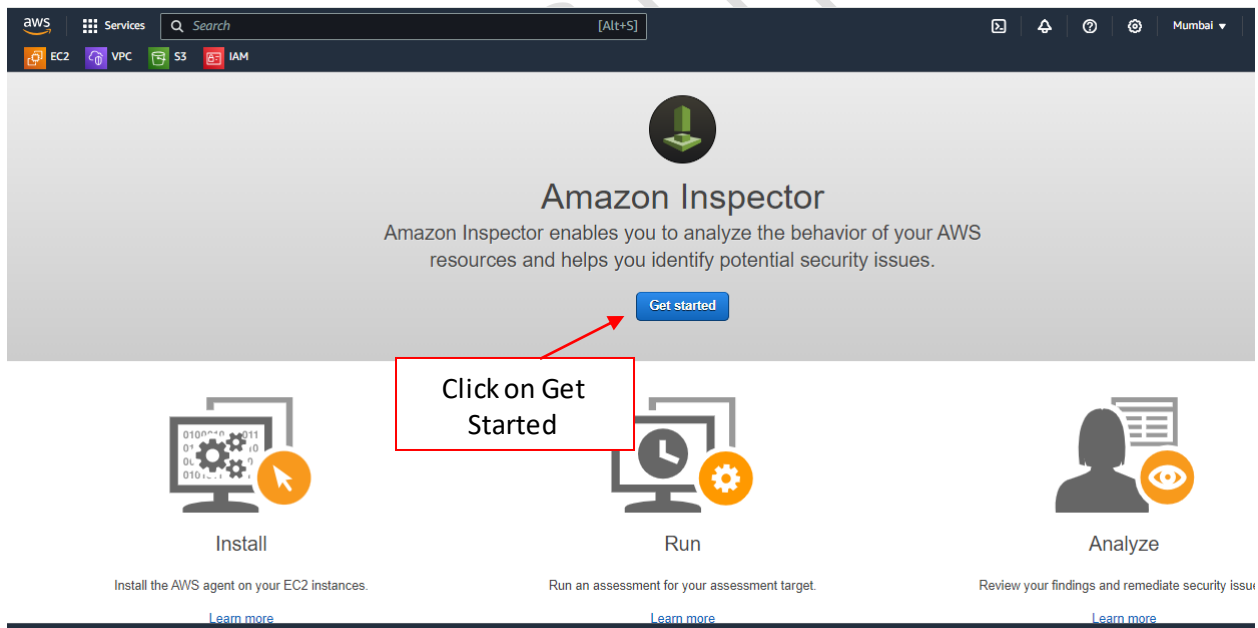
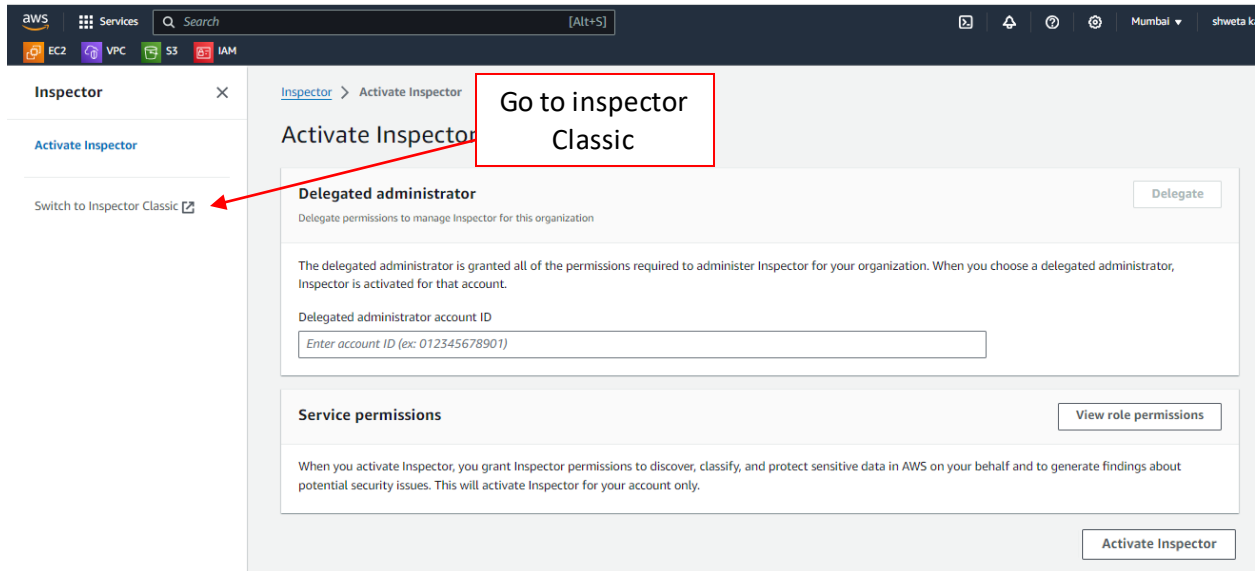
Details

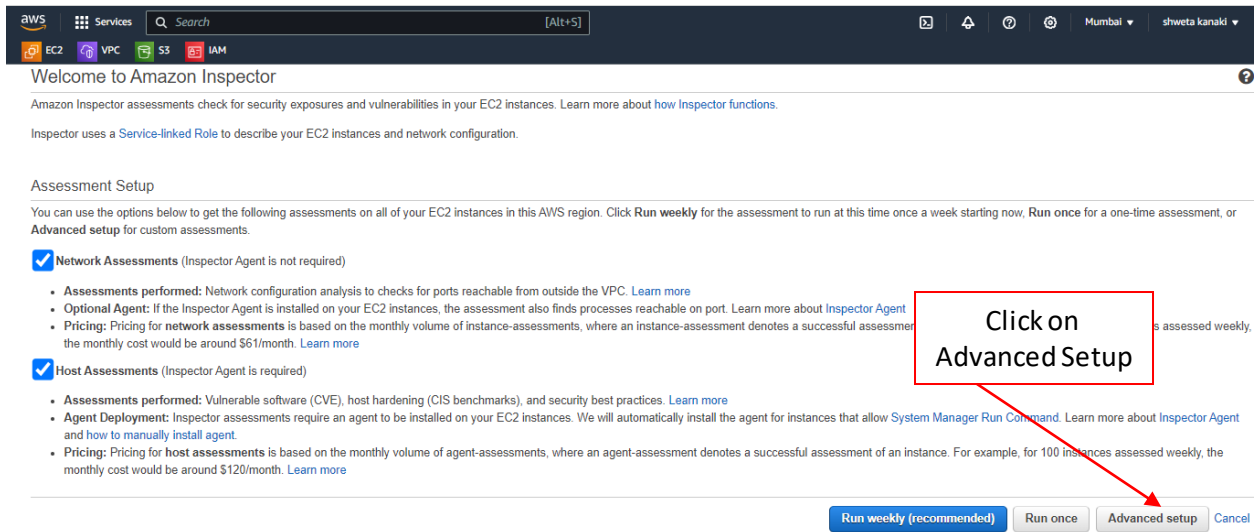
Security group name EBS-SG	Security group ID sg-07c7e5651181d45c2	Description EBS-security group	VPC ID vpc-0c3cd85059c1bcf31
Owner 473869189128	Inbound rules count 5 Permission entries	Outbound rules count 3 Permission entries	

Inbound rules | Outbound rules | Tags

Step 3: Setting up AWS Inspector







Welcome to Amazon Inspector

Amazon Inspector assessments check for security exposures and vulnerabilities in your EC2 instances. Learn more about [how Inspector functions](#).

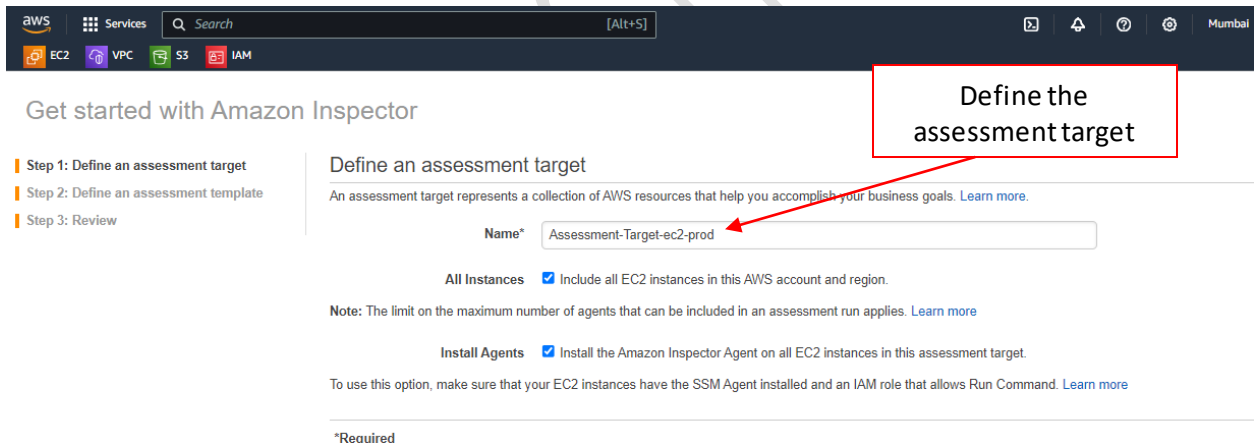
Inspector uses a [Service-linked Role](#) to describe your EC2 instances and network configuration.

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 assessment 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. 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](#)

[Run weekly \(recommended\)](#) [Run once](#) [Advanced setup](#) [Cancel](#)



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*

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](#)

*Required

aws Services Search [Alt+S]

EC2 VPC S3 IAM

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* Assessment-Target-ec2-prod

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
Add a new key	
Name	

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](#)

*Required

Uncheck all instances

Select the Name

aws Services Search [Alt+S]

EC2 VPC S3 IAM

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* Assessment-Target-ec2-prod

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
Name	Add a new value
Add a new key	[None]
	inspector-instance
	kiran

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](#)

*Required

Select the created instance



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* Assessment-Target-ec2-prod

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](#)

Key	Value
Name	inspector-instance
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](#)

*Required

Click Next

Cancel Preview 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

Rules packages* Common Vulnerabilities and Exposures-1.1 x
CIS Operating System Security Configuration Benchmarks-1.0 x
Network Reachability-1.1 x
Security Best Practices-1.0 x

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

Duration* 1 Hour (Recommended)

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](#)

Define the
assessment template

Get started with Amazon Inspector

Step 1: Define an assessment target
Step 2: Define an assessment template

Define an assessment template

An assessment template allows you to specify various properties for an assessment run, including the rules packages to use, the duration of the assessment, and the assessment schedule. [Learn more](#)

Name* Assessment-Template-Default

Rules packages* Network Reachability-1.1

Duration 15 Minutes

Assessment Schedule ☐ Set up recurring assessment runs once every 7 days. The first run starts on create. [Learn more](#)

*Required

Cancel Previous Next

Change the duration as 15 mins

Select only network reachability

Uncheck assessment Schedule and click next

Step 3: Review

Review the details of your target and template, and then choose Create.

Define an assessment target

Name Assessment-Target-ec2-prod

Tags

Key	Value
Name	inspector-instance

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](#)

Define an assessment template

Name Assessment-Template-Default

Rules packages Network Reachability-1.1

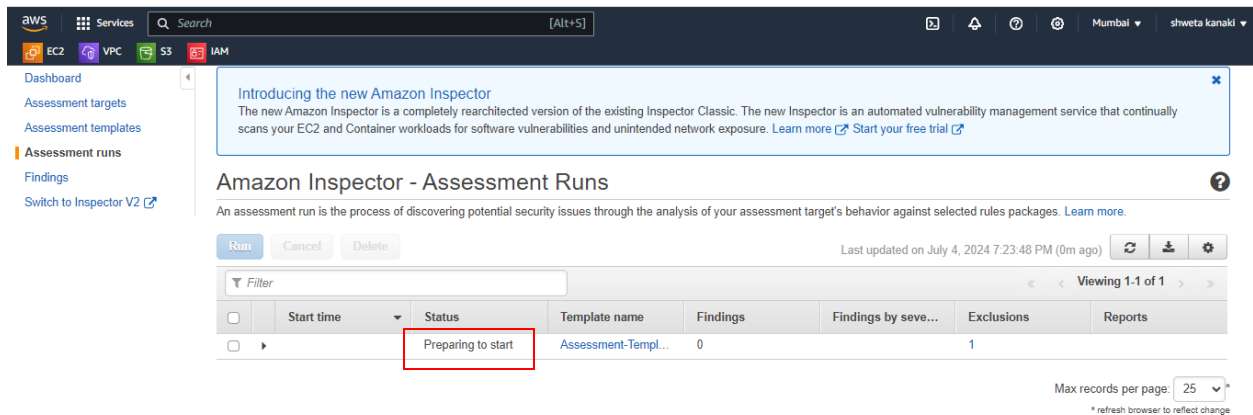
An assessment run requires the AWS agent to run on all EC2 instances that comprise your assessment target. If you have not yet deployed the AWS agent, you can create the assessment template, but remember to install AWS agents before you run the assessment.

Cancel Preview Previous Create

Review and Create

Assessment Run will start automatically.

Step 4: Findings



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](#).

Run Cancel Delete

Last updated on July 4, 2024 7:23:48 PM (0m ago)

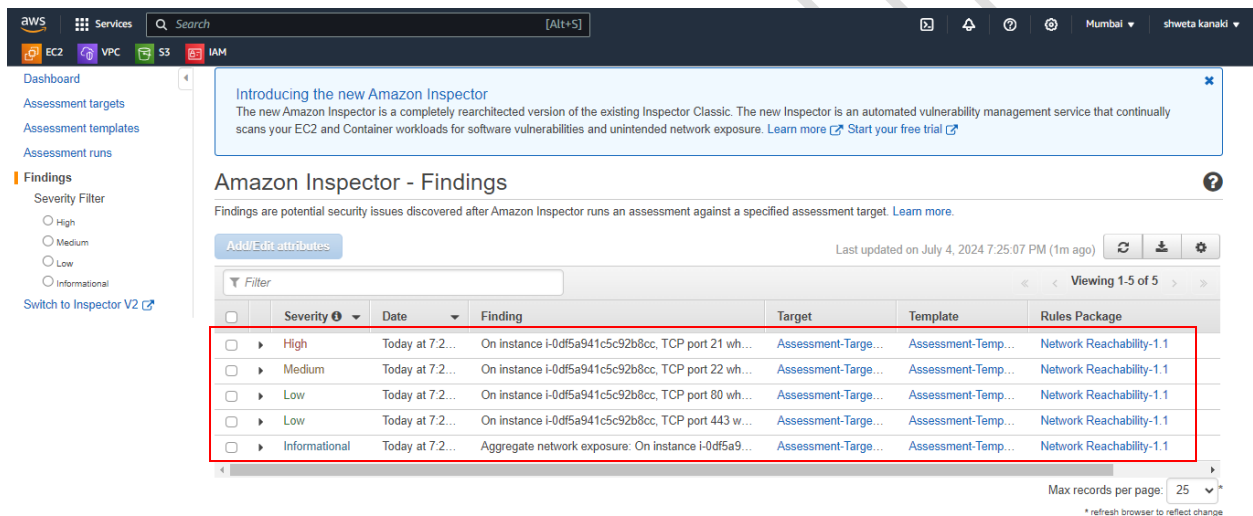
Filter

	Start time	Status	Template name	Findings	Findings by seve...	Exclusions	Reports
<input type="checkbox"/>		Preparing to start	Assessment-Templ...	0		1	

Max records per page: 25

* refresh browser to reflect change

Now go to the findings and check for the risk.



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](#).

Add/Edit attributes

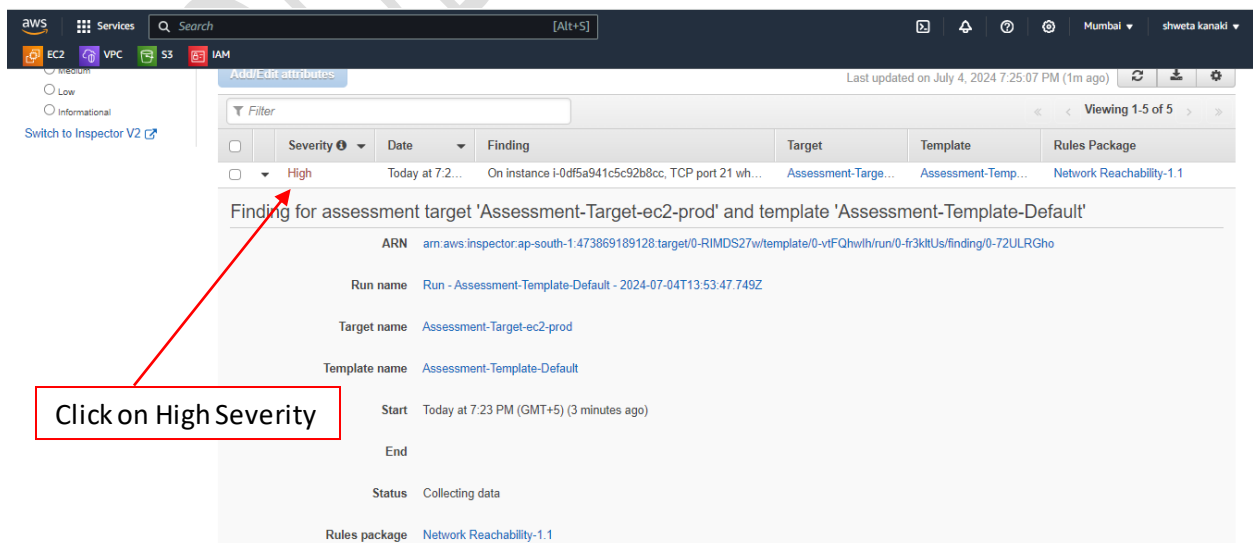
Last updated on July 4, 2024 7:25:07 PM (1m ago)

Filter

	Severity	Date	Finding	Target	Template	Rules Package
<input type="checkbox"/>	High	Today at 7:2...	On instance i-0df5a941c5c92b8cc, TCP port 21 wh...	Assessment-Targe...	Assessment-Temp...	Network Reachability-1.1
<input type="checkbox"/>	Medium	Today at 7:2...	On instance i-0df5a941c5c92b8cc, TCP port 22 wh...	Assessment-Targe...	Assessment-Temp...	Network Reachability-1.1
<input type="checkbox"/>	Low	Today at 7:2...	On instance i-0df5a941c5c92b8cc, TCP port 80 wh...	Assessment-Targe...	Assessment-Temp...	Network Reachability-1.1
<input type="checkbox"/>	Low	Today at 7:2...	On instance i-0df5a941c5c92b8cc, TCP port 443 w...	Assessment-Targe...	Assessment-Temp...	Network Reachability-1.1
<input type="checkbox"/>	Informational	Today at 7:2...	Aggregate network exposure: On instance i-0df5a9...	Assessment-Targe...	Assessment-Temp...	Network Reachability-1.1

Max records per page: 25

* refresh browser to reflect change



Add/Edit attributes

Last updated on July 4, 2024 7:25:07 PM (1m ago)

Filter

	Severity	Date	Finding	Target	Template	Rules Package
<input type="checkbox"/>	High	Today at 7:2...	On instance i-0df5a941c5c92b8cc, TCP port 21 wh...	Assessment-Targe...	Assessment-Temp...	Network Reachability-1.1

Finding for assessment target 'Assessment-Target-ec2-prod' and template 'Assessment-Template-Default'

ARN am:aws:inspector:ap-south-1:473869189128:target/0-RIMDS27w/template/0-vfQhwh/run/0-fr3kdtUs/finding/0-72ULRGho

Run name Run - Assessment-Template-Default - 2024-07-04T13:53:47.749Z

Target name Assessment-Target-ec2-prod

Template name Assessment-Template-Default

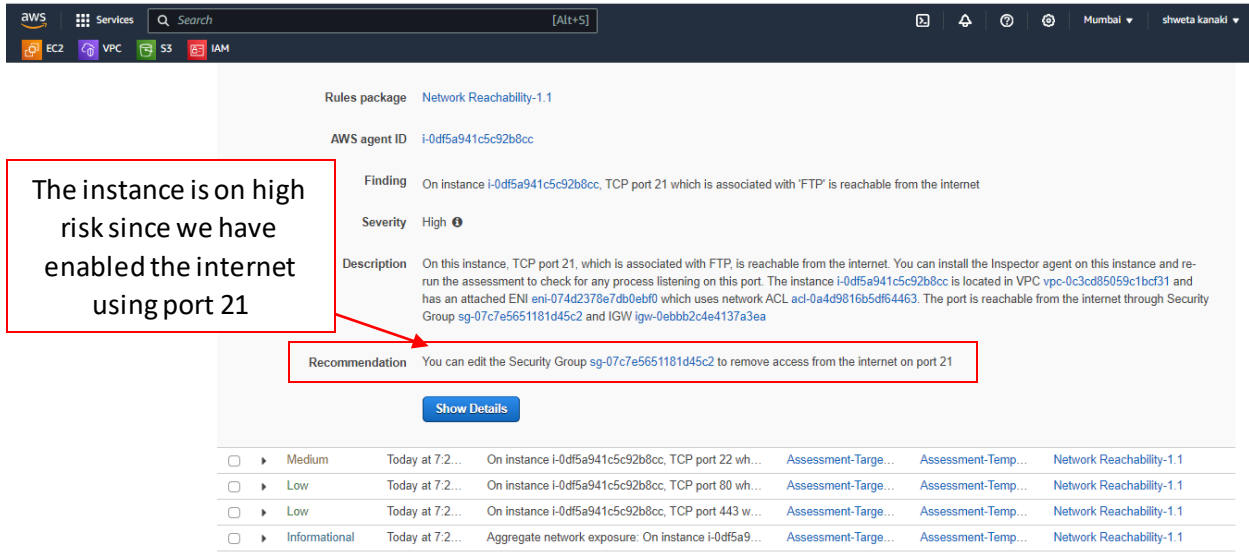
Start Today at 7:23 PM (GMT+5) (3 minutes ago)

End

Status Collecting data

Rules package Network Reachability-1.1

Click on High Severity



The instance is on high risk since we have enabled the internet using port 21

Rules package: [Network Reachability-1.1](#)

AWS agent ID: [i-0df5a941c5c92b8cc](#)

Finding On instance [i-0df5a941c5c92b8cc](#), TCP port 21 which is associated with 'FTP' is reachable from the internet

Severity High

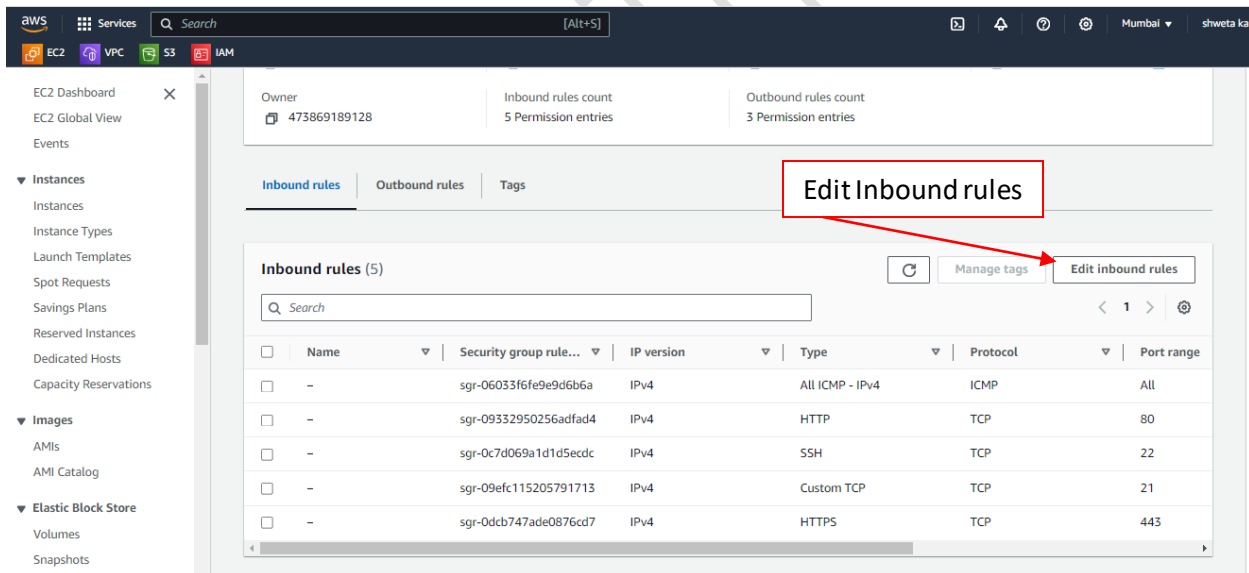
Description On this instance, TCP port 21, which is associated with FTP, is reachable from the internet. You can install the Inspector agent on this instance and re-run the assessment to check for any process listening on this port. The instance [i-0df5a941c5c92b8cc](#) is located in VPC [vpc-0c3cd85059c1bcf31](#) and has an attached ENI [eni-074d2378e7db0ebf0](#) which uses network ACL [acl-0a4d9816b5df64463](#). The port is reachable from the internet through Security Group [sg-07c7e5651181d45c2](#) and IGW [igw-0ebbb2c4e4137a3ea](#)

Recommendation You can edit the Security Group [sg-07c7e5651181d45c2](#) to remove access from the internet on port 21

[Show Details](#)

Severity	Time	Target	Assessment-Target...	Assessment-Temp...	Network Reachability-1.1
Medium	Today at 7:2...	On instance i-0df5a941c5c92b8cc , TCP port 22 wh...	Assessment-Target...	Assessment-Temp...	Network Reachability-1.1
Low	Today at 7:2...	On instance i-0df5a941c5c92b8cc , TCP port 80 wh...	Assessment-Target...	Assessment-Temp...	Network Reachability-1.1
Low	Today at 7:2...	On instance i-0df5a941c5c92b8cc , TCP port 443 w...	Assessment-Target...	Assessment-Temp...	Network Reachability-1.1
Informational	Today at 7:2...	Aggregate network exposure: On instance i-0df5a9...	Assessment-Target...	Assessment-Temp...	Network Reachability-1.1

To eliminate the risk go to instance's security group and remove the port 21.



Owner: [473869189128](#)

Inbound rules count: 5 Permission entries

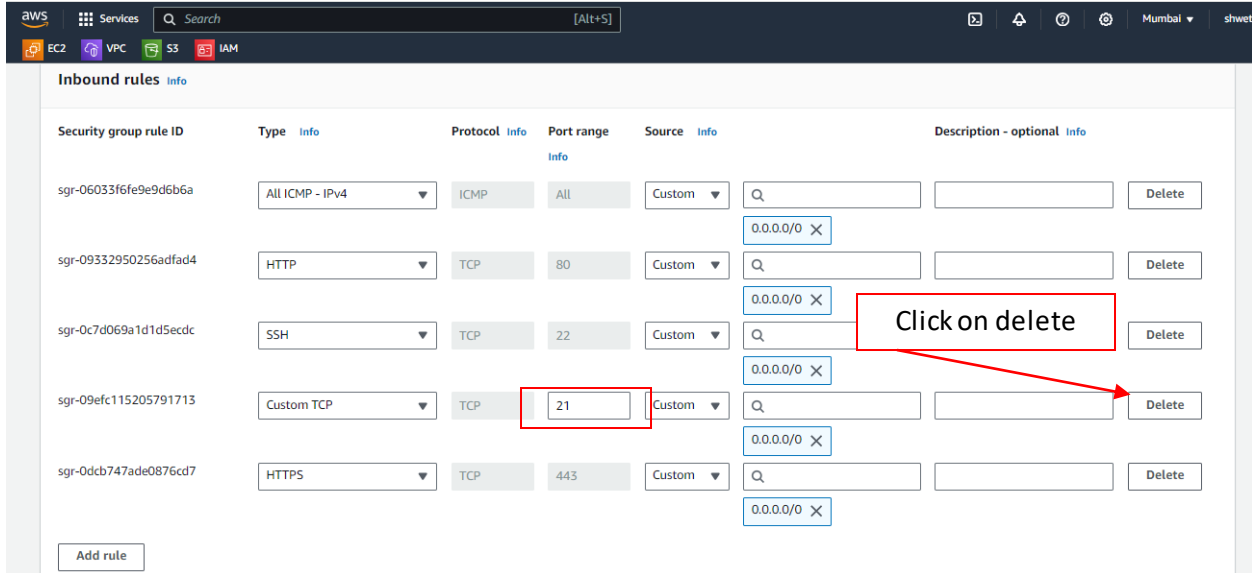
Outbound rules count: 3 Permission entries

Edit inbound rules

Inbound rules (5)

[Manage tags](#) [Edit inbound rules](#)

Name	Security group rule...	IP version	Type	Protocol	Port range
-	sgr-06033f6fe9e9d6b6a	IPv4	All ICMP - IPv4	ICMP	All
-	sgr-09332950256adfad4	IPv4	HTTP	TCP	80
-	sgr-0c7d069a1d1d5ecdc	IPv4	SSH	TCP	22
-	sgr-09efc115205791713	IPv4	Custom TCP	TCP	21
-	sgr-0dc747ade0876cd7	IPv4	HTTPS	TCP	443

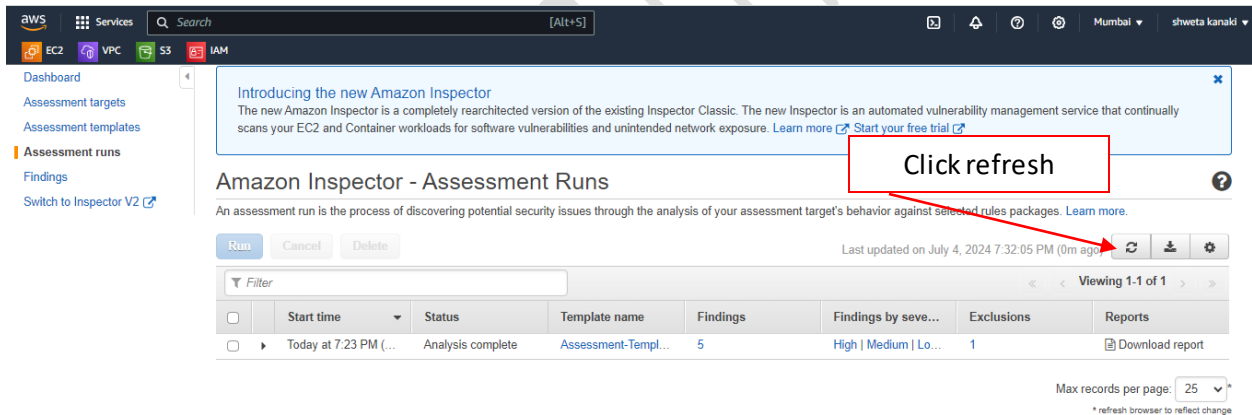


Inbound rules Info

Security group rule ID	Type Info	Protocol Info	Port range Info	Source Info	Description - optional Info	
sgr-06033f6fe9e9d6b6a	All ICMP - IPv4	ICMP	All	Custom	Q 0.0.0.0/0 X	Delete
sgr-09332950256adf4d4	HTTP	TCP	80	Custom	Q 0.0.0.0/0 X	Delete
sgr-0c7d069a1d1d5ecd	SSH	TCP	22	Custom	Q 0.0.0.0/0 X	Delete
sgr-09efc115205791713	Custom TCP	TCP	21	Custom	Q 0.0.0.0/0 X	Delete
sgr-0dc747ade0876cd7	HTTPS	TCP	443	Custom	Q 0.0.0.0/0 X	Delete

Add rule

Now go back to assessment runs



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](#).

Run Cancel Delete

Last updated on July 4, 2024 7:32:05 PM (0m ago)

Filter

	Start time	Status	Template name	Findings	Findings by severity	Exclusions	Reports
<input type="checkbox"/>	Today at 7:23 PM (...)	Analysis complete	Assessment-Templ...	5	High Medium Lo...	1	Download report

Max records per page: 25

* refresh browser to reflect change

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](#).

Run Cancel Delete

updated on July 4, 2024 7:34:25 PM (0m ago)

Filter

	Start time	Status	Template name	Findings	Findings by severity	Exclusions	Reports
<input type="checkbox"/>	Today at 7:32 PM (...)	Analysis complete	Assessment-Templ...	4	High Medium Lo...	1	Download report
<input type="checkbox"/>	Today at 7:23 PM (...)	Analysis complete	Assessment-Templ...	5	High Medium Lo...	1	Download report

Max records per page: 25

* refresh browser to reflect change

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](#).

Run Cancel Delete

Last updated on July 4, 2024 7:34:25 PM (0m ago)

Filter

	Start time	Status	Template name	Findings	Findings by severity	Exclusions	Reports
<input type="checkbox"/>	Today at 7:32 PM (...)	Analysis complete	Assessment-Templ...	4	High Medium Lo...	1	Download report
<input type="checkbox"/>	Today at 7:23 PM (...)	Analysis complete	Assessment-Templ...	5	High Medium Lo...	1	Download report

Max records per page: 25

* refresh browser to reflect change

Assessment - Run - Assessment-Template-Default - 2024-07-04T14:02:51.996Z

ARN [arn:aws:inspector:ap-south-1:473869189128:target/0-RIMDS27w/template/0-vfQhwh/run/0-So2HGjDG](#)

Start Today at 7:32 PM (GMT+5) (2 minutes ago)

End Today at 7:33 PM (GMT+5) (2 minutes ago)

Target name [Assessment-Target-ec2-prod](#)

Template name [Assessment-Template-Default](#)

Rules packages [Network Reachability-1.1](#)

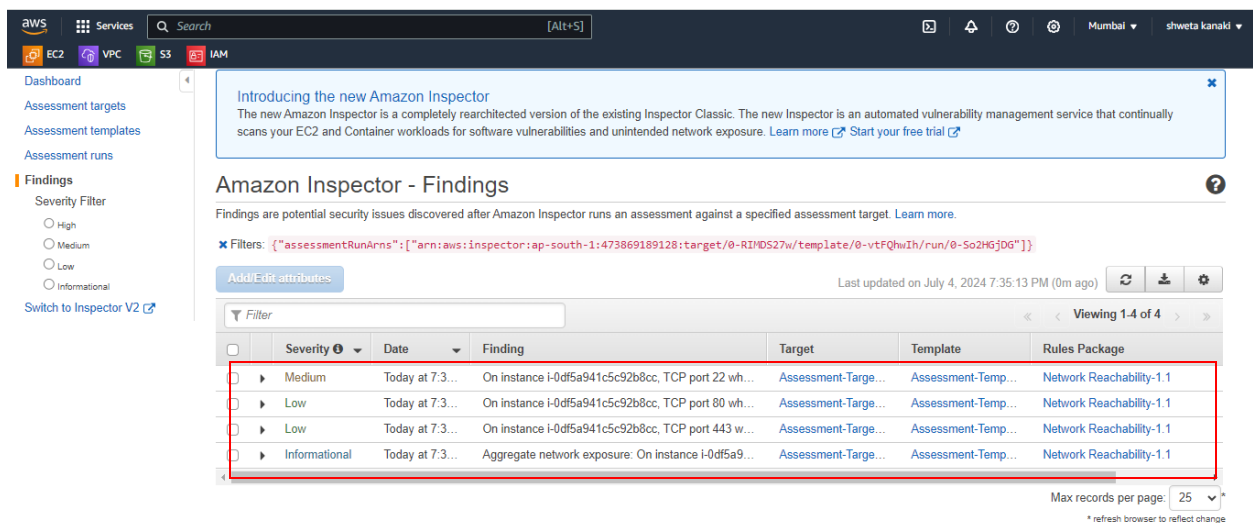
Duration 15 Minutes

Status Analysis complete

Findings 4

[Show AWS agents](#) [Show status](#)

High risk has been eliminated

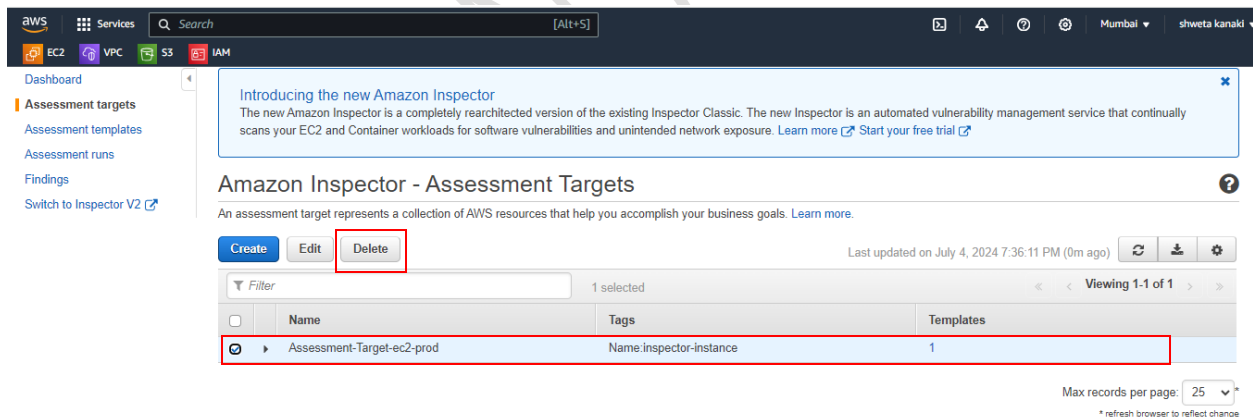


The screenshot shows the Amazon Inspector console. The left sidebar has a 'Findings' section with a 'Severity Filter' showing 'High', 'Medium', 'Low', and 'Informational' options. The main content area is titled 'Amazon Inspector - Findings'. It displays a table of findings with columns: Severity, Date, Finding, Target, Template, and Rules Package. The table shows four findings, all with a severity of 'Low' or 'Medium'. The 'Findings' table is highlighted with a red border. The 'Findings' table has the following data:

Severity	Date	Finding	Target	Template	Rules Package
Medium	Today at 7:3...	On instance i-0df5a941c5c92b8cc, TCP port 22 wh...	Assessment-Targe...	Assessment-Temp...	Network Reachability-1.1
Low	Today at 7:3...	On instance i-0df5a941c5c92b8cc, TCP port 80 wh...	Assessment-Targe...	Assessment-Temp...	Network Reachability-1.1
Low	Today at 7:3...	On instance i-0df5a941c5c92b8cc, TCP port 443 w...	Assessment-Targe...	Assessment-Temp...	Network Reachability-1.1
Informational	Today at 7:3...	Aggregate network exposure: On instance i-0df5a9...	Assessment-Targe...	Assessment-Temp...	Network Reachability-1.1

Step 5: Delete assessment targets after practicing.

Go to assessment targets, select the assessment and click delete



The screenshot shows the Amazon Inspector console. The left sidebar has an 'Assessment targets' section. The main content area is titled 'Amazon Inspector - Assessment Targets'. It displays a table of assessment targets with columns: Name, Tags, and Templates. The table shows one assessment target, 'Assessment-Target-ec2-prod'. The 'Delete' button is highlighted with a red border. The 'Assessment Targets' table has the following data:

Name	Tags	Templates
Assessment-Target-ec2-prod	Name:inspector-instance	1