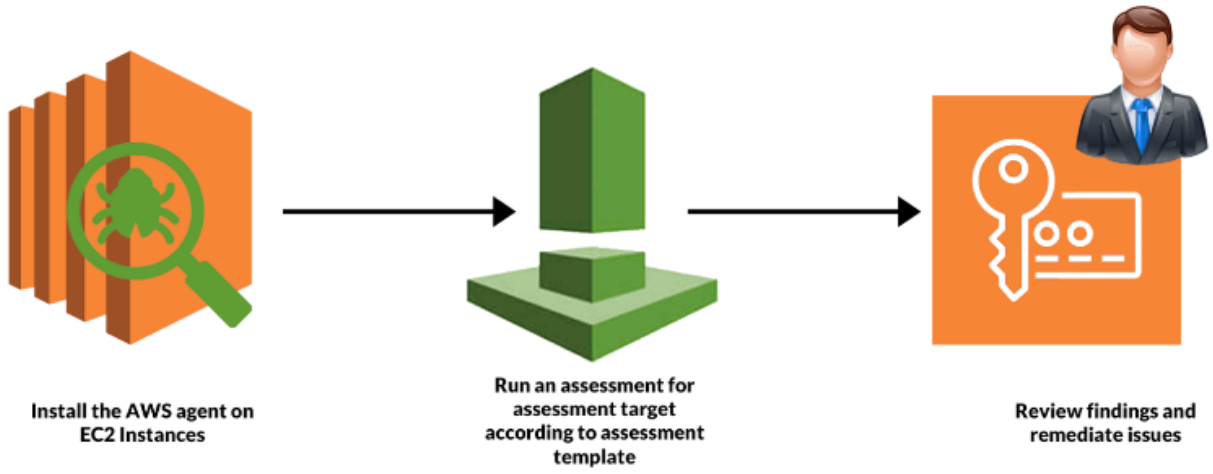
AWS INSPECTOR

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?

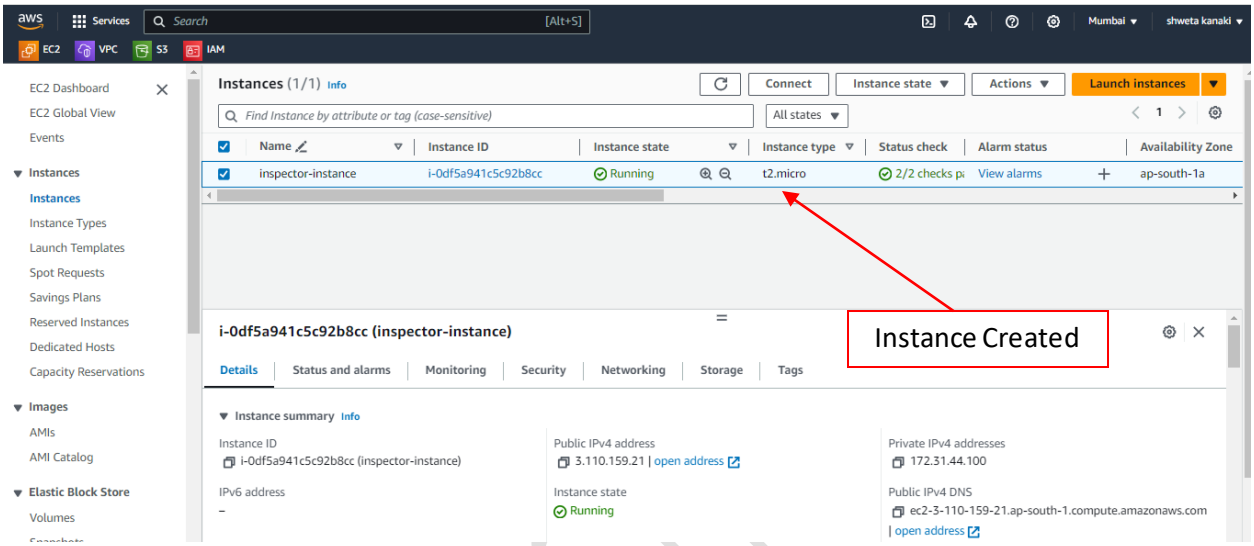


Amazon Inspector performs an automatic assessment and generates a findings report containing steps to keep the environment safe. To use this service, you need to define the collection of AWS and all the resources that complete the application to proceed and tested. It is followed by adding and performing 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.

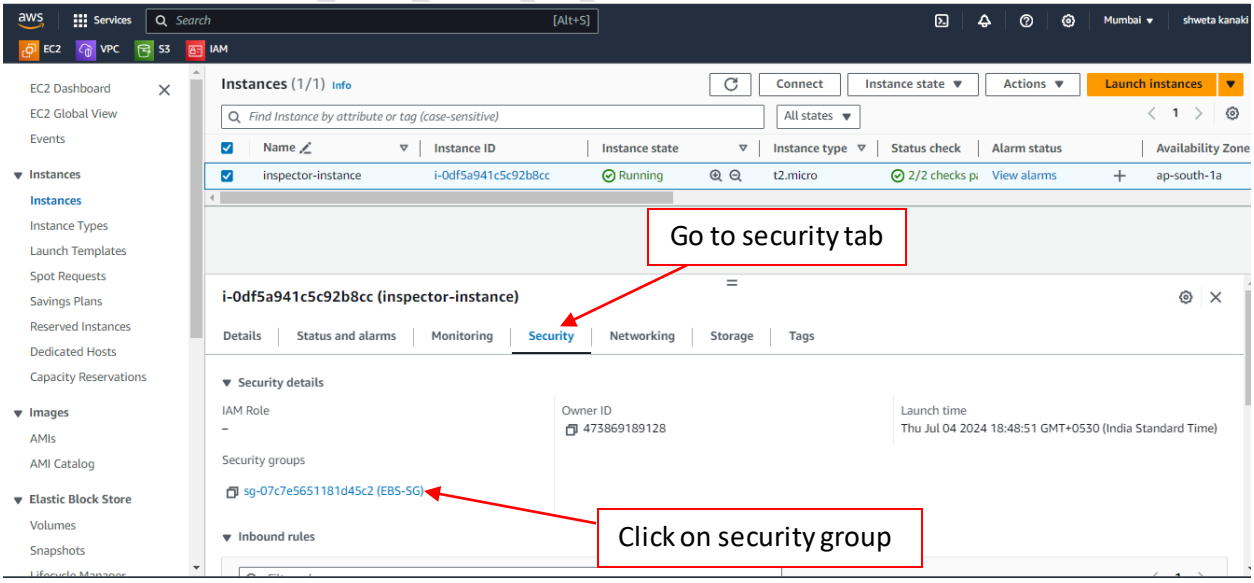
An Inspector Agent runs on the EC2 machines hosting the application that monitors the network, file system, and process activity. After collecting all the required data, it is compared with the built-in security rules to identify security or compliance issues.

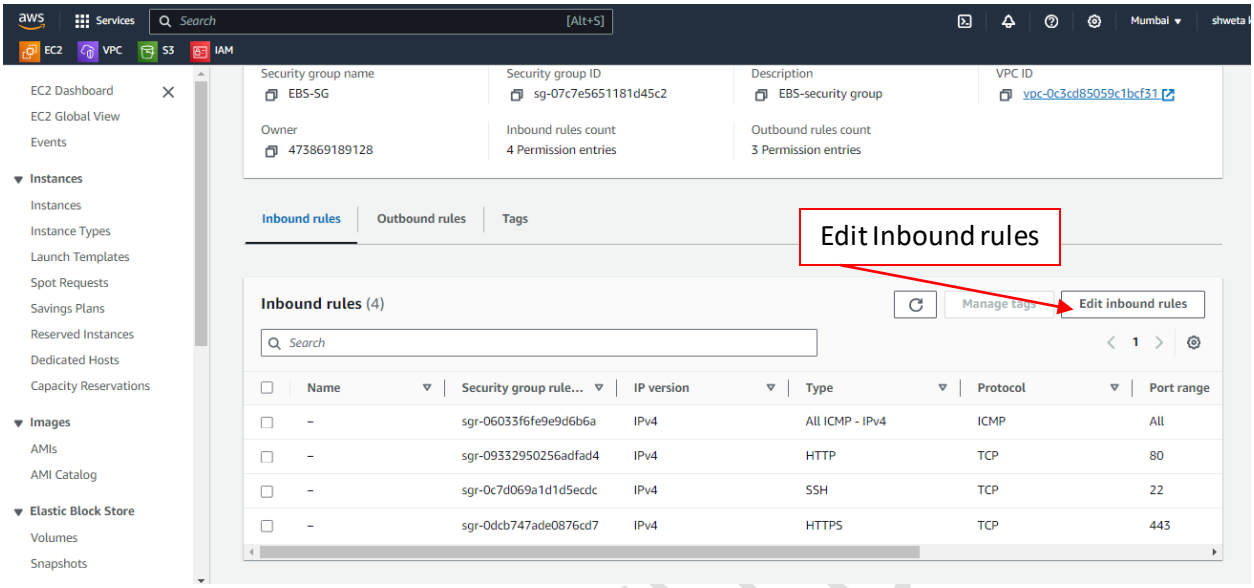
GETTING STARTED WITH AMAZON INSPECTOR

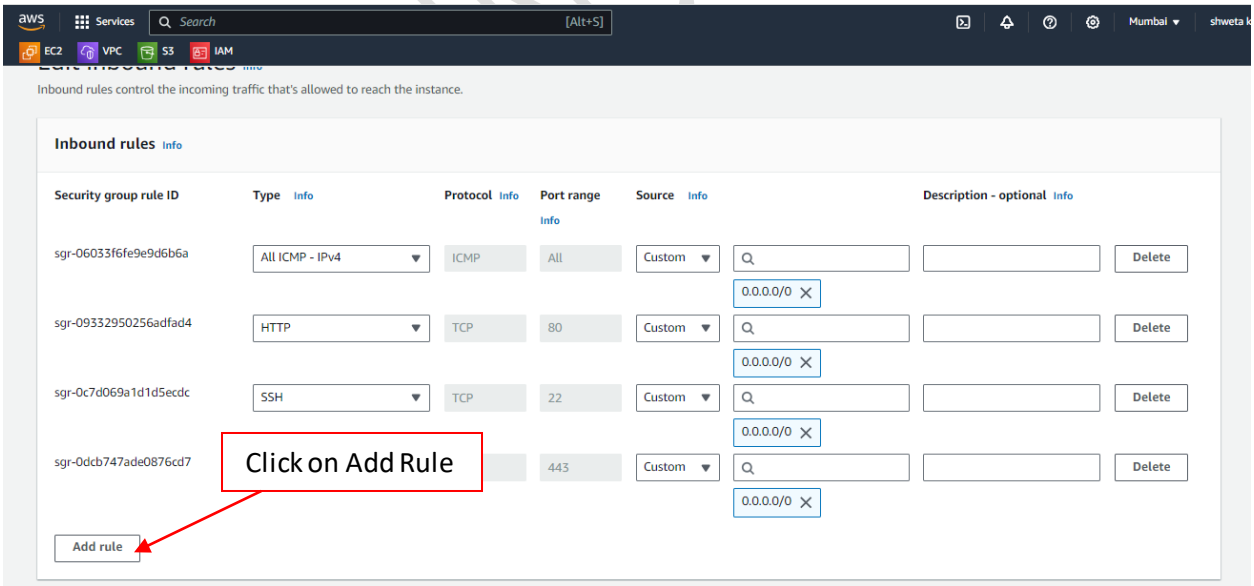
Step 1: Create a EC2 instance

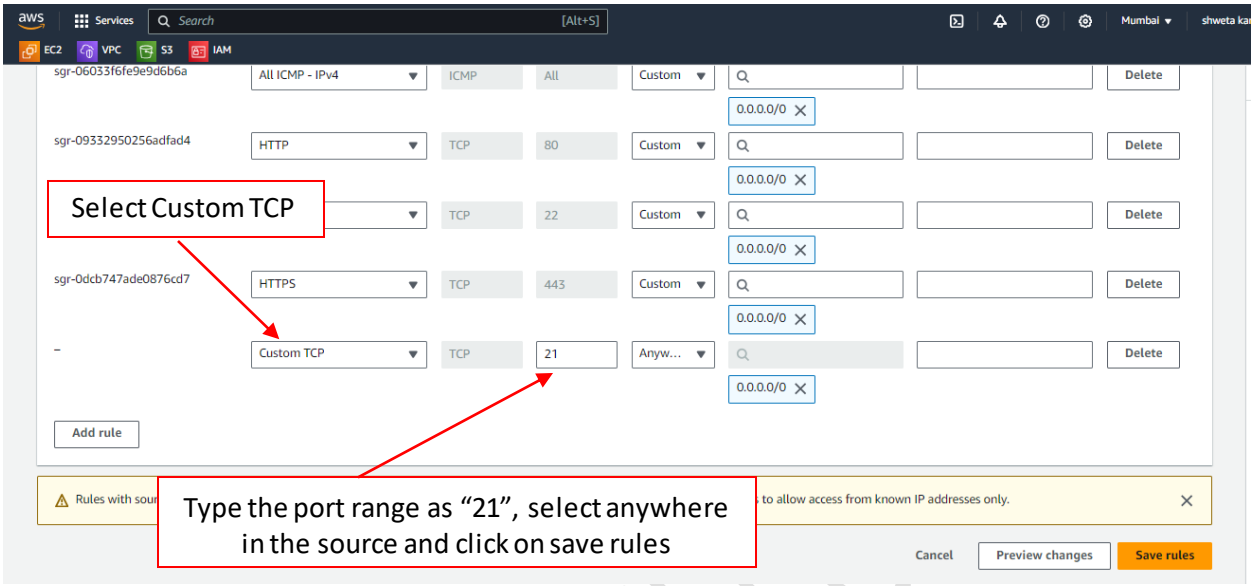


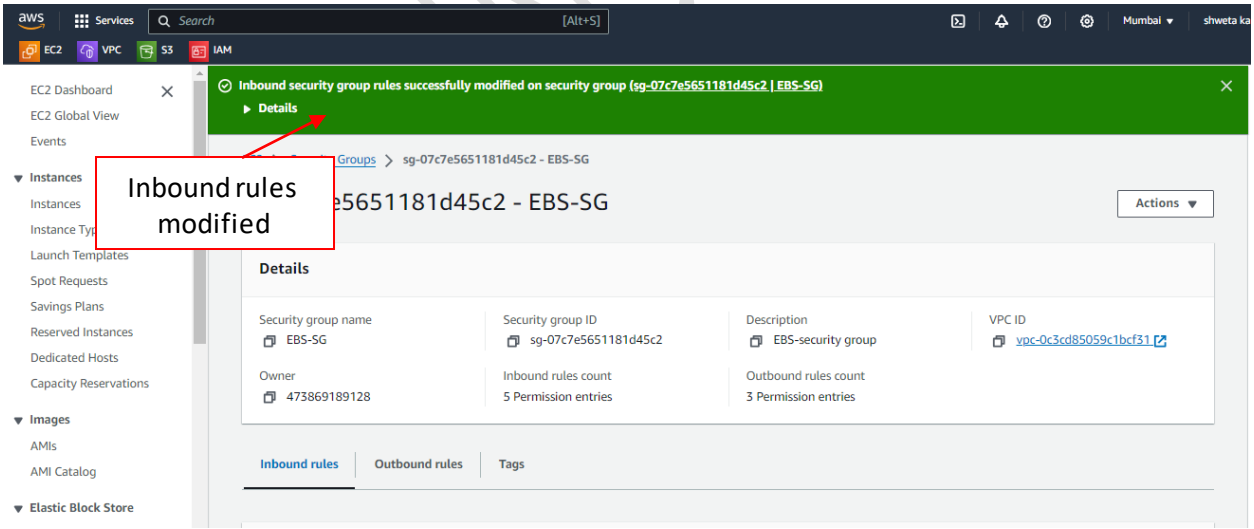
Step 2: Modify Security Group



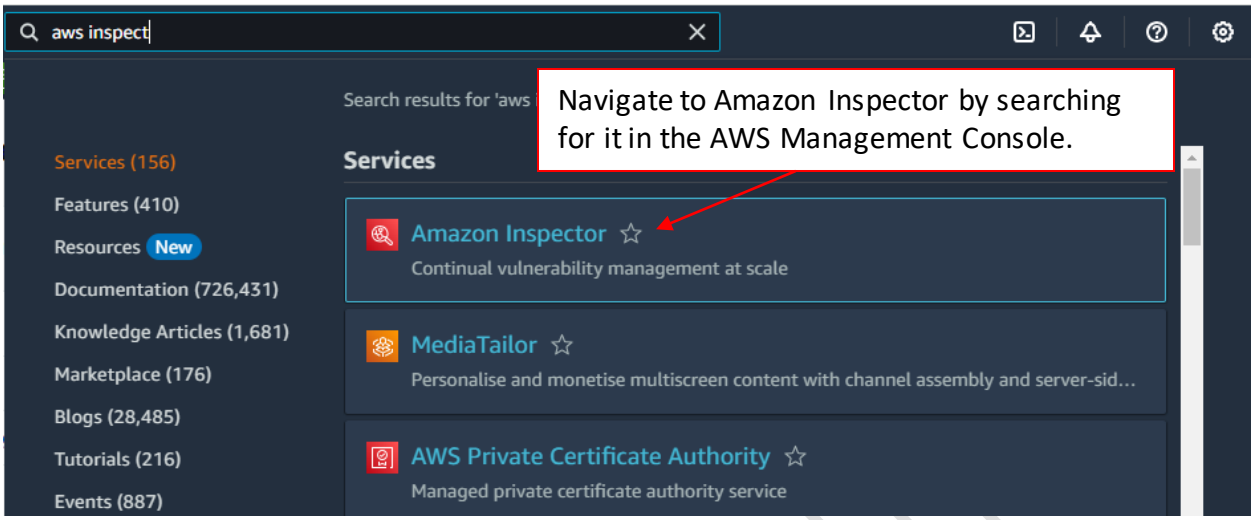

Edit Inbound rules
Edit inbound rules

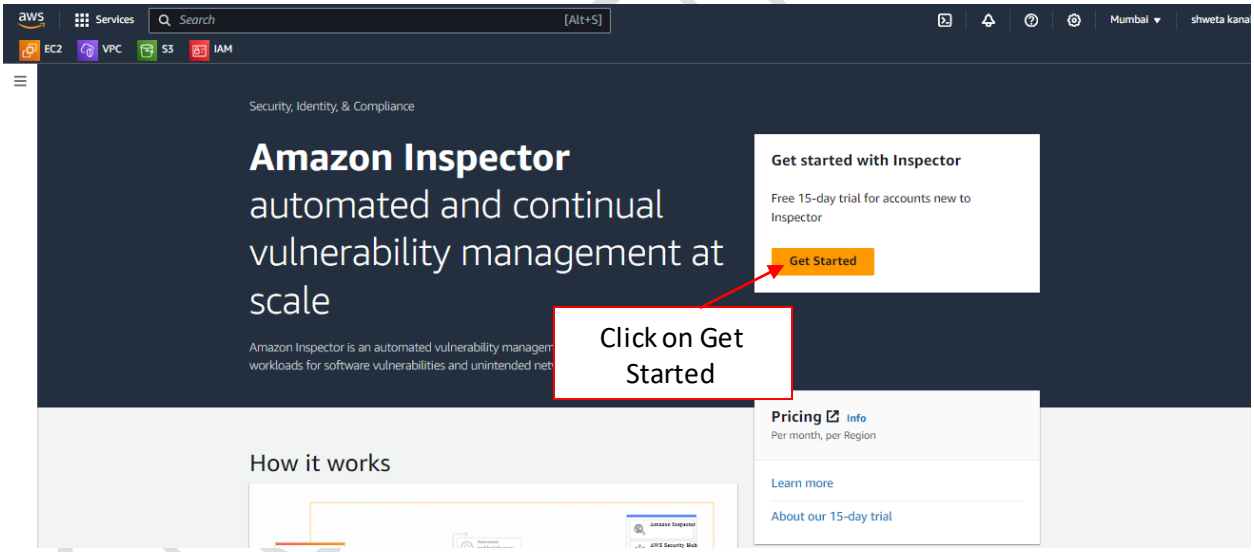

Click on Add Rule
Add rule

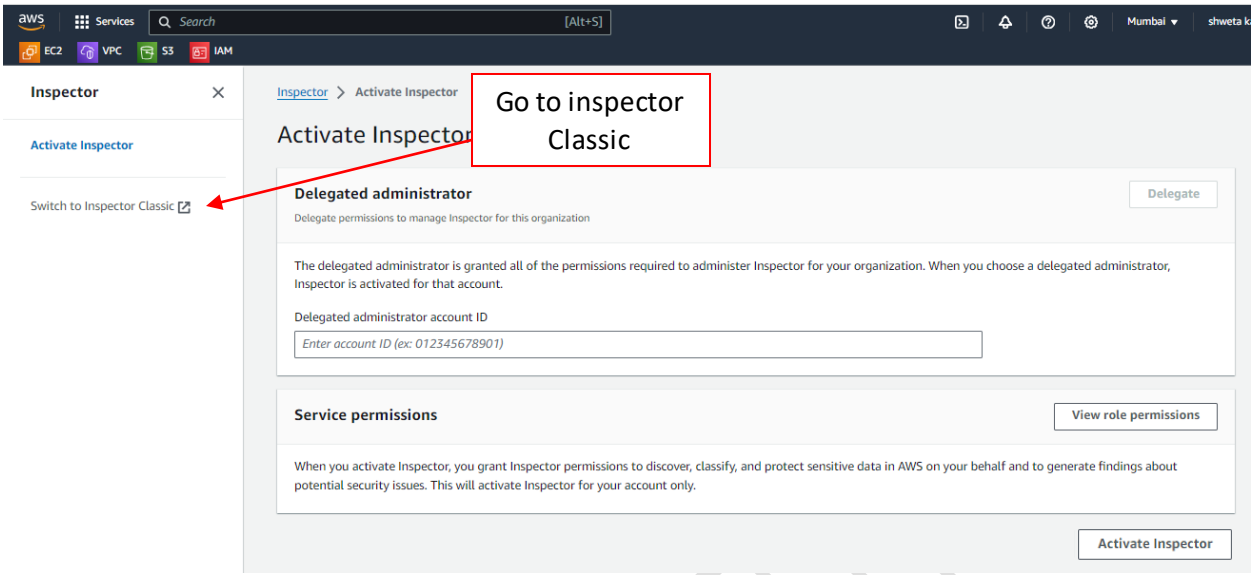

Select Custom TCP
Type the port range as “21”, select anywhere in the source and click on save rules
Add rule
Cancel
Preview changes
Save rules

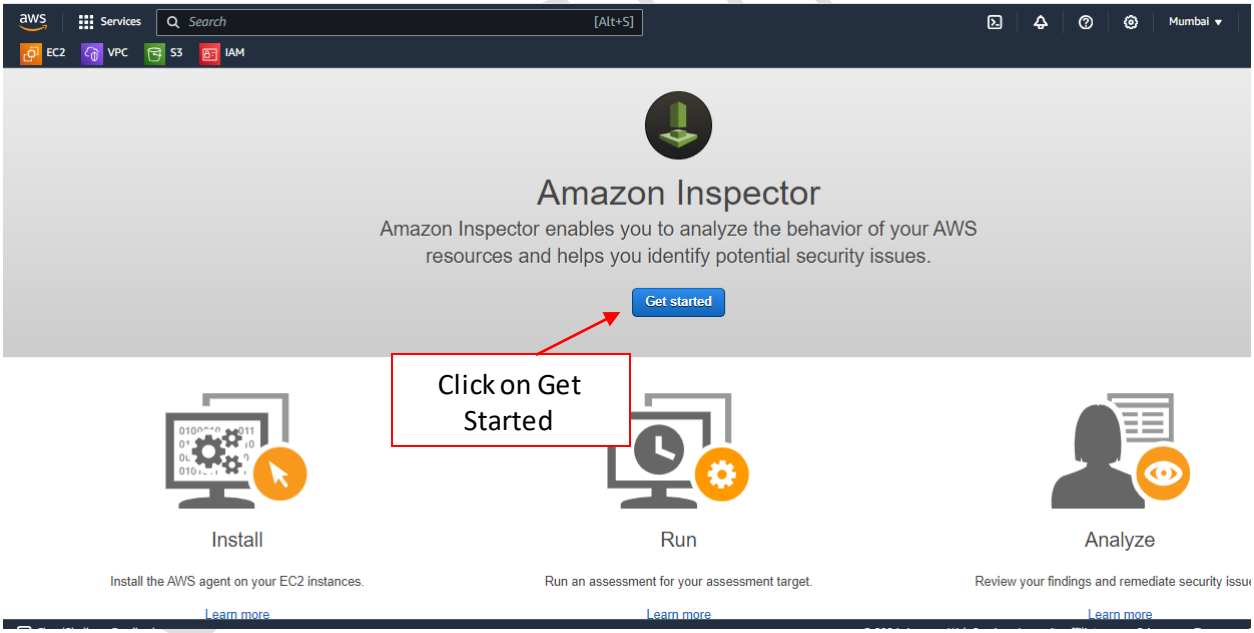

Inbound security group rules successfully modified on security group (sg-07c7e5651181d45c2 | EBS-SG)
Details
Inbound rules modified
Actions
Details
Security group name
EBS-SG
Security group ID
sg-07c7e5651181d45c2
Description
EBS-security group
VPC ID
Owner
473869189128
Inbound rules count
5 Permission entries
Outbound rules count
3 Permission entries
Inbound rules
Outbound rules
Tags

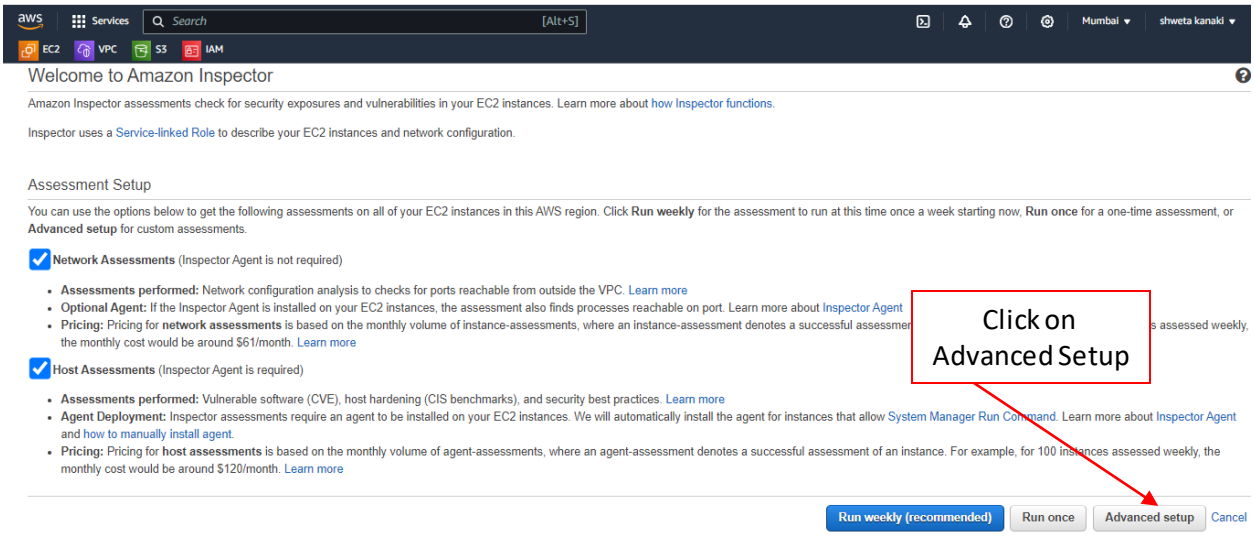
Step 3: Setting up AWS Inspector

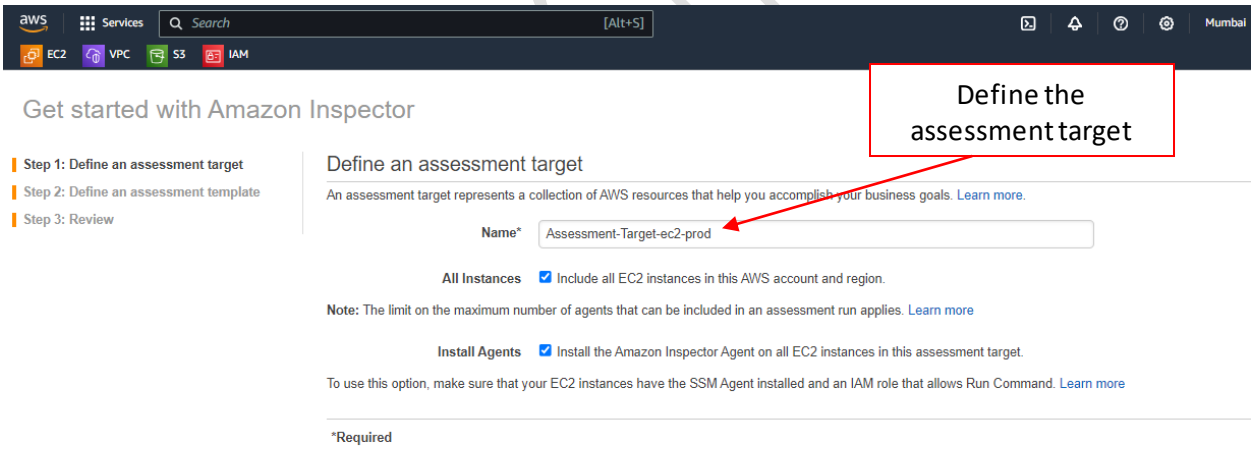


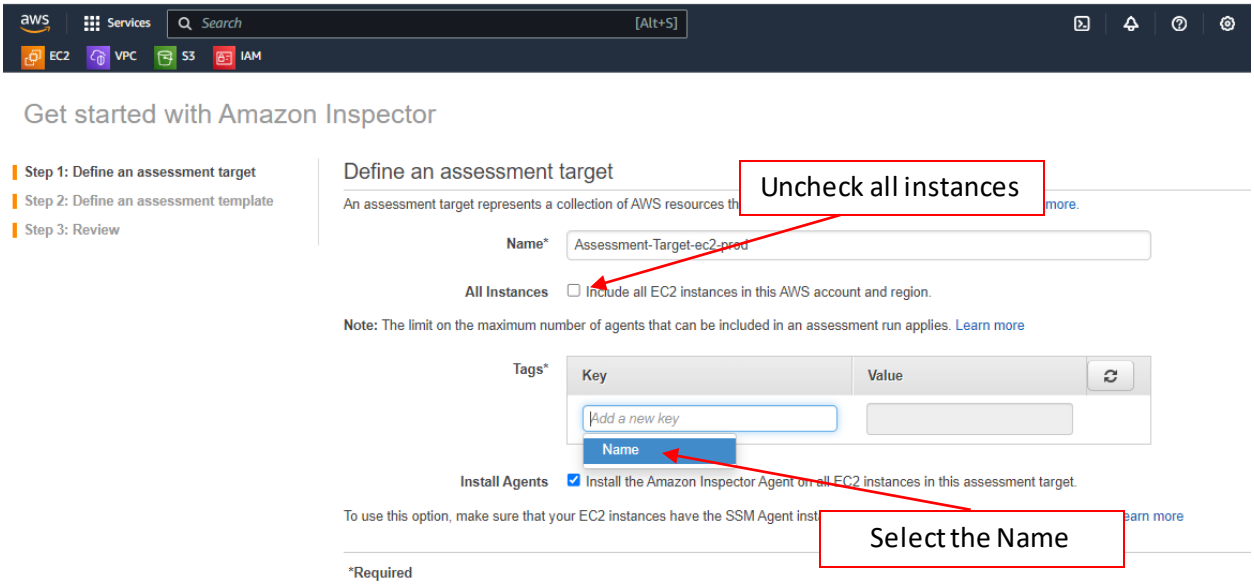


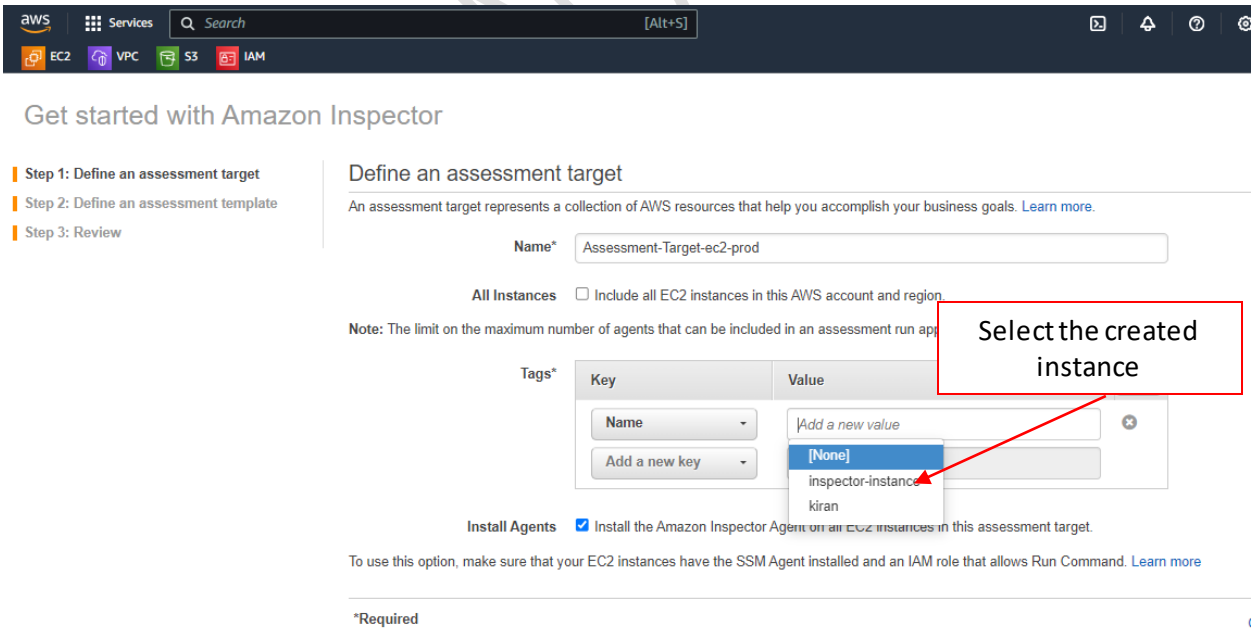

Inspector
Activate Inspector
Switch to Inspector Classic
Inspector > Activate Inspector
Activate Inspector
Go to inspector Classic
Delegated administrator
Delegate permissions to manage Inspector for this organization
Delegate
The delegated administrator is granted all of the permissions required to administer Inspector for your organization. When you choose a delegated administrator, Inspector is activated for that account.
Delegated administrator account ID
Enter account ID (ex: 012345678901)
Service permissions
View role permissions
When you activate Inspector, you grant Inspector permissions to discover, classify, and protect sensitive data in AWS on your behalf and to generate findings about potential security issues. This will activate Inspector for your account only.
Activate Inspector

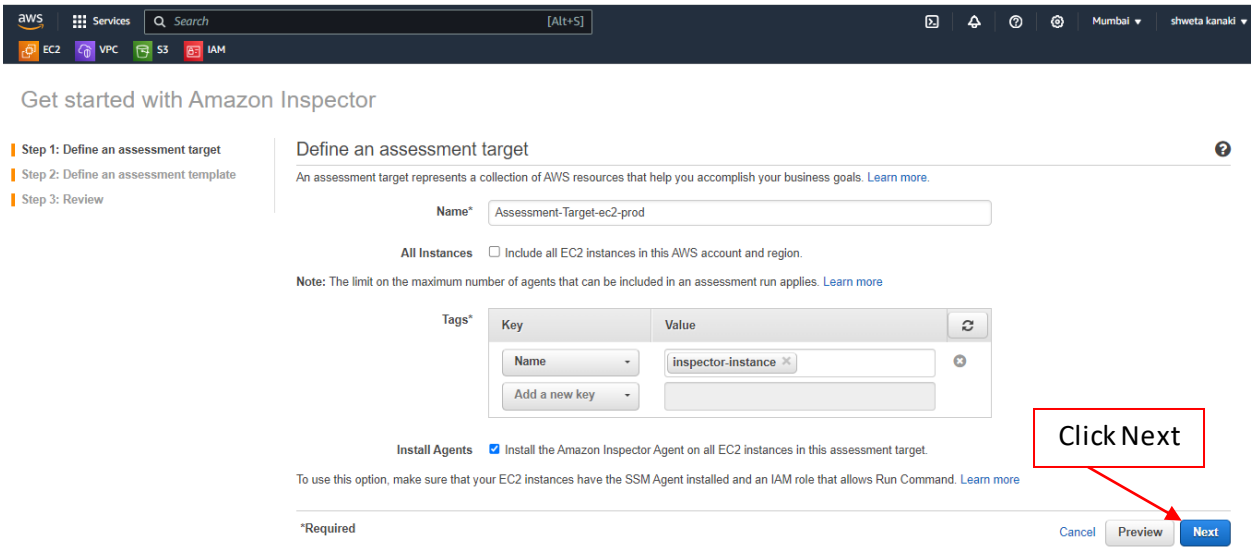

Amazon Inspector
Amazon Inspector enables you to analyze the behavior of your AWS resources and helps you identify potential security issues.
Get started
Click on Get Started
Install
Install the AWS agent on your EC2 instances.
Learn more
Run
Run an assessment for your assessment target.
Learn more
Analyze
Learn more

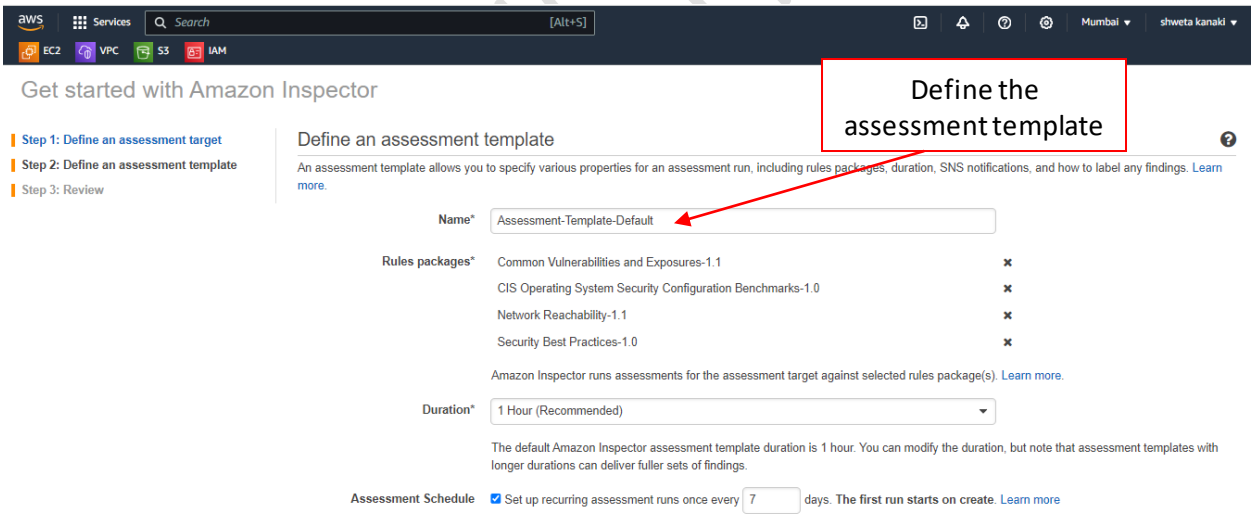

Welcome to Amazon Inspector
Amazon Inspector assessments check for security exposures and vulnerabilities in your EC2 instances. Learn more about how Inspector functions.
Inspector uses a Service-linked Role to describe your EC2 instances and network configuration.
Assessment Setup
You can use the options 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 assessmer
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
Click on Advanced Setup
Run weekly (recommended)
Run once
Advanced setup
Cancel

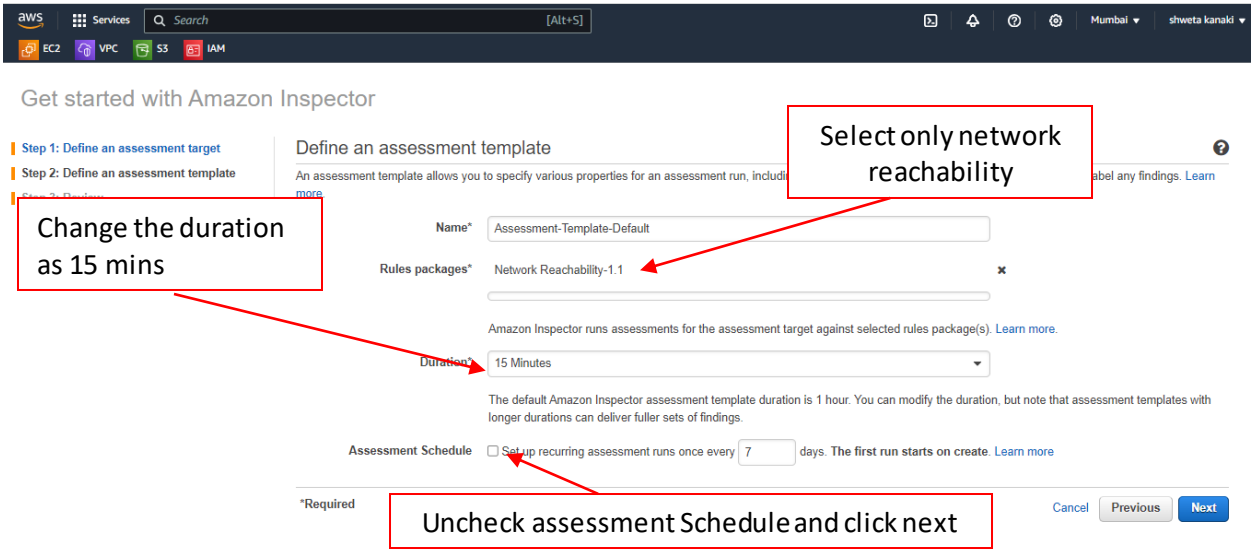

Get started with Amazon Inspector
Define the assessment target
Step 1: Define an assessment target
Step 2: Define an assessment template
Step 3: Review
Define an assessment target
An assessment target represents a collection of AWS resources that help you accomplish your business goals. Learn more.
Name*
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
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

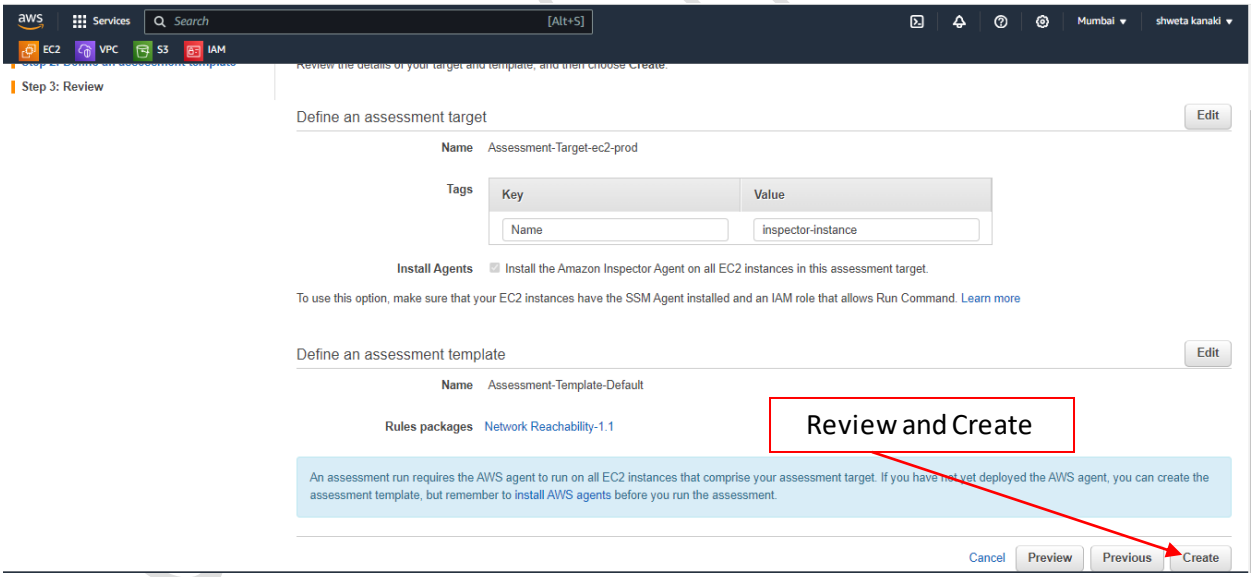

Get started with Amazon Inspector
Step 1: Define an assessment target
Step 2: Define an assessment template
Step 3: Review
Define an assessment target
Uncheck all instances
Name*
Assessment-Target-ec2-prod
All Instances
Include all EC2 instances in this AWS account and region.
Note: The limit on the 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.
Select the Name
*Required


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.
Select the created instance
Tags*
Key
Value
Name
Add a new value
Add a new key
[None]
inspector-instance
kiran
Install Agents
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


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
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
Cancel
Preview
Next
Click Next

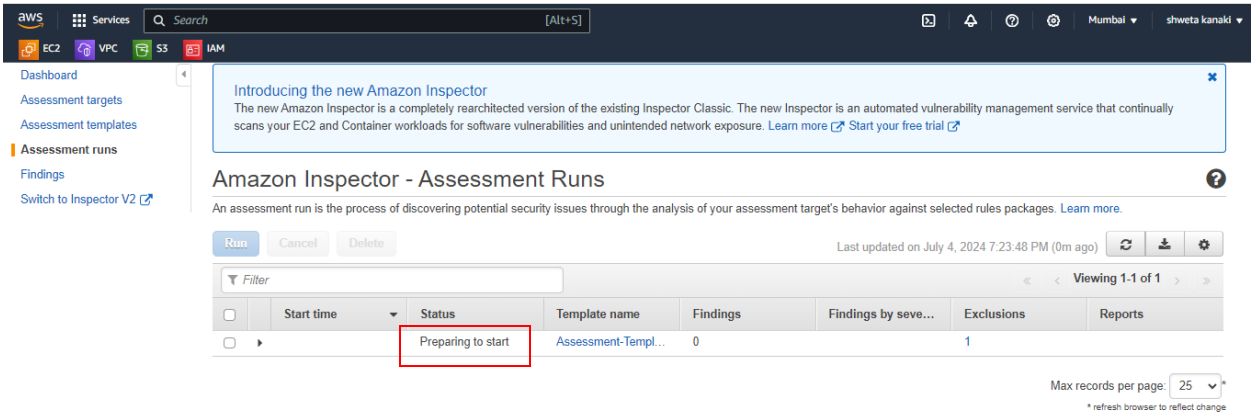

Get started with Amazon Inspector
Step 1: Define an assessment target
Step 2: Define an assessment template
Step 3: Review
Define the assessment template
Define an assessment template
An assessment template allows you to specify various properties for an assessment run, including rules packages, duration, SNS notifications, and how to label any findings. Learn more.
Name*
Assessment-Template-Default
Rules packages*
Common Vulnerabilities and Exposures-1.1
CIS Operating System Security Configuration Benchmarks-1.0
Network Reachability-1.1
Security Best Practices-1.0
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



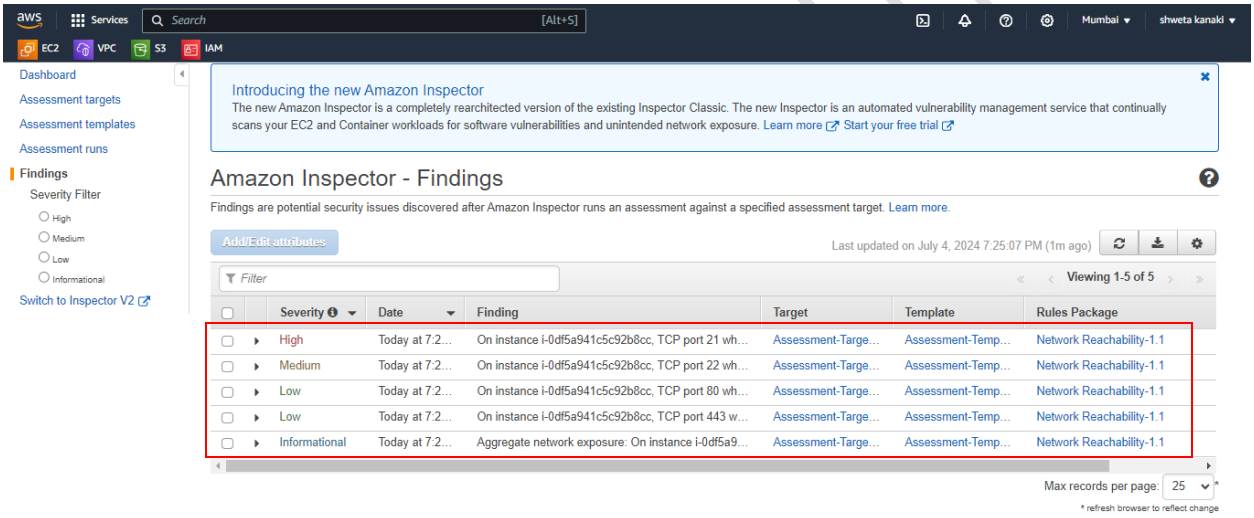


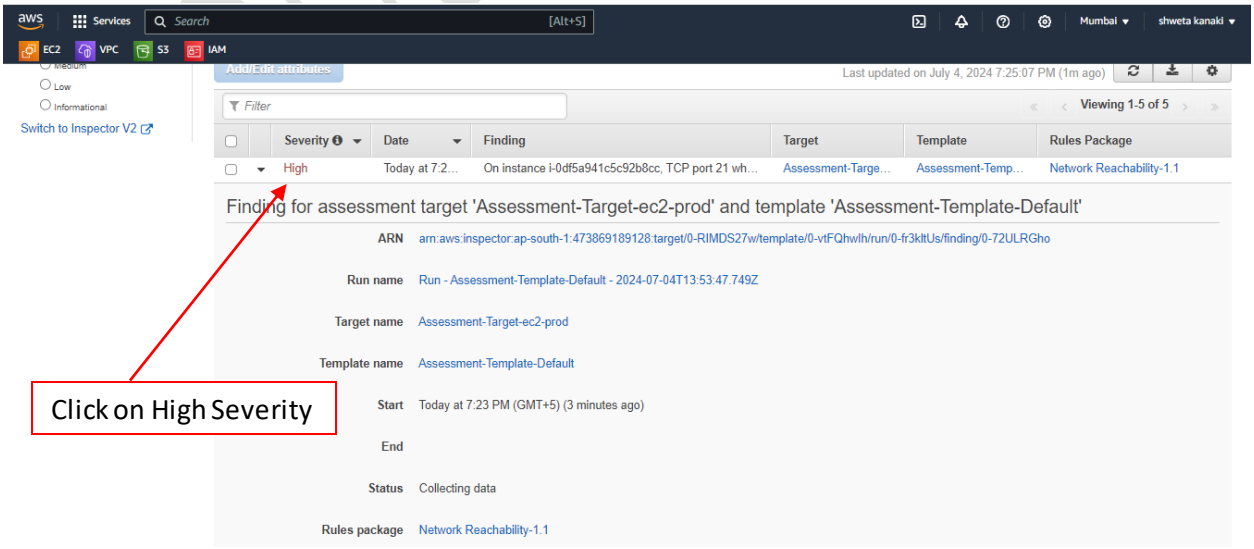
Assessment Run will start automatically.

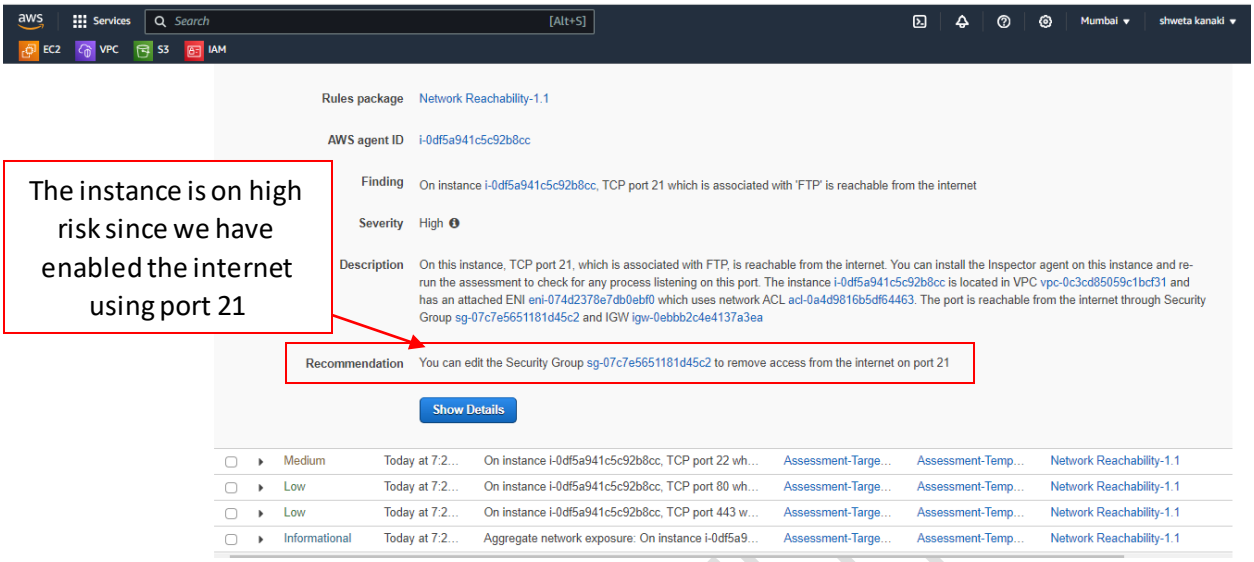
Step 4:Findings



Now go to the findings and check for the risk.

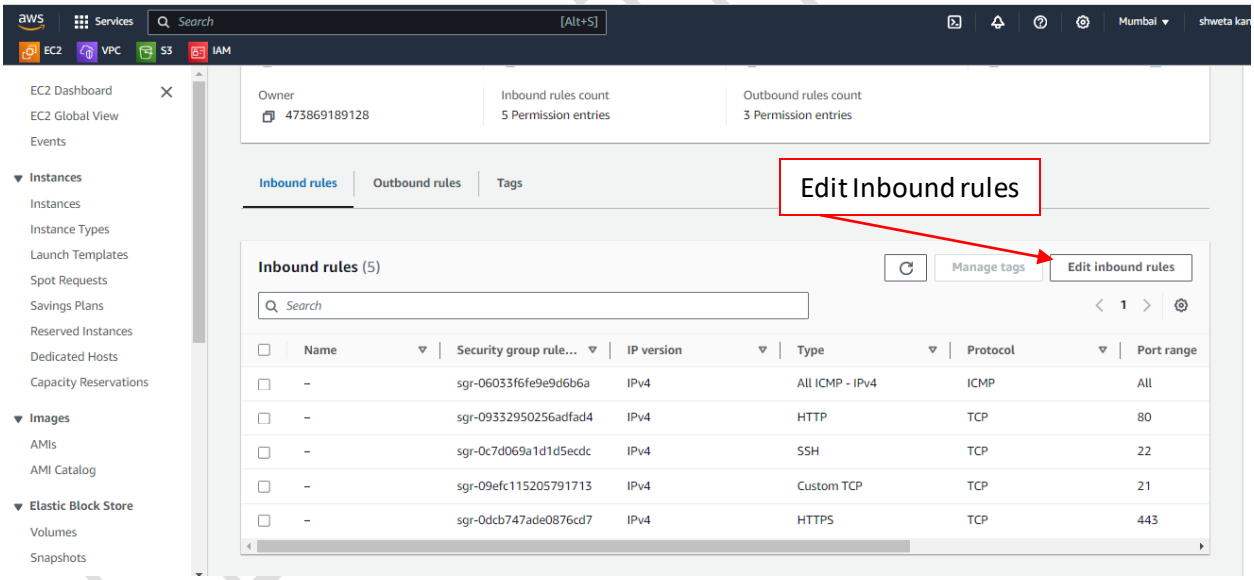


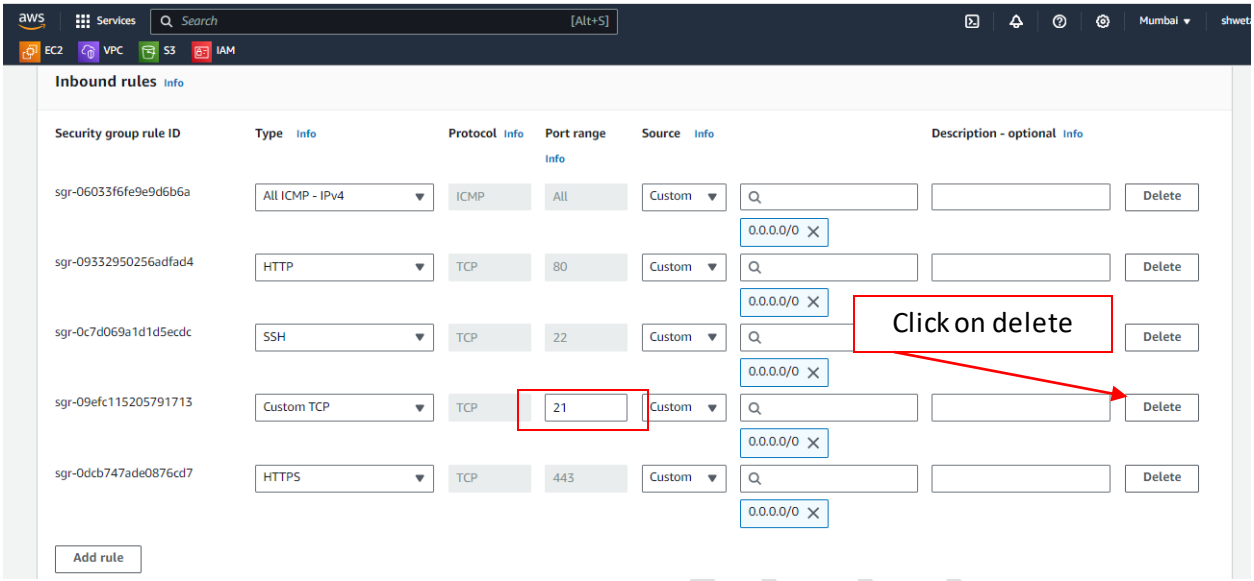




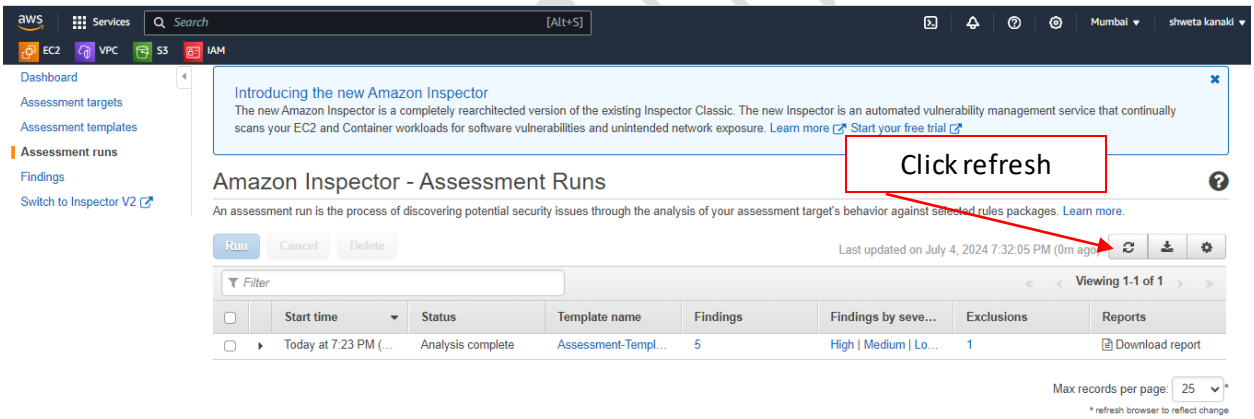
The instance is on high risk since we have enabled the internet using port 21

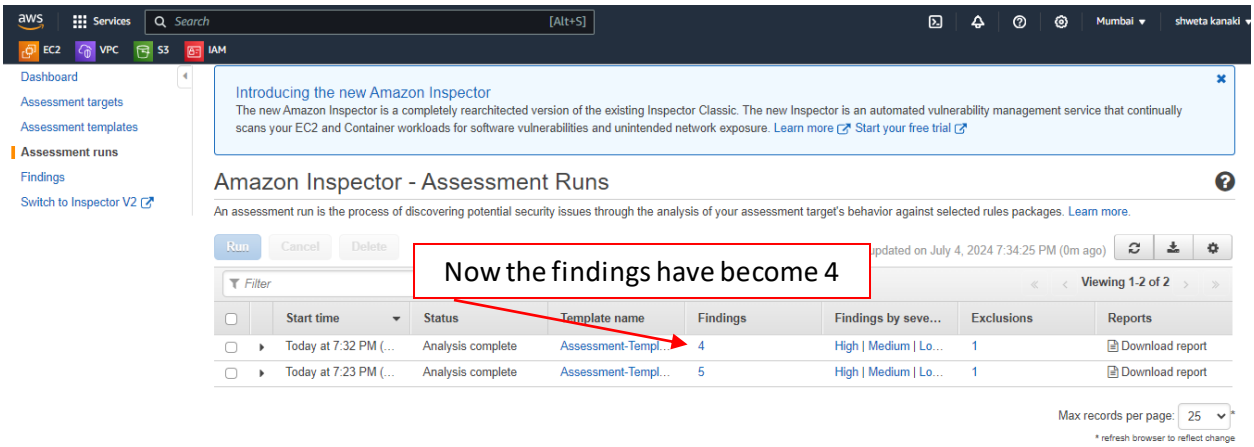
To eliminate the risk go to instance's security group and remove the port 21.

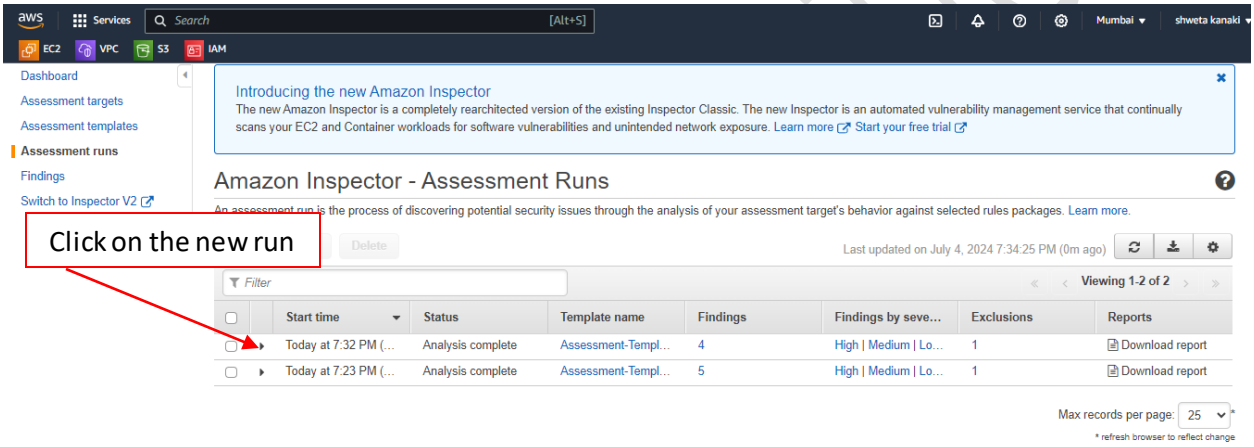


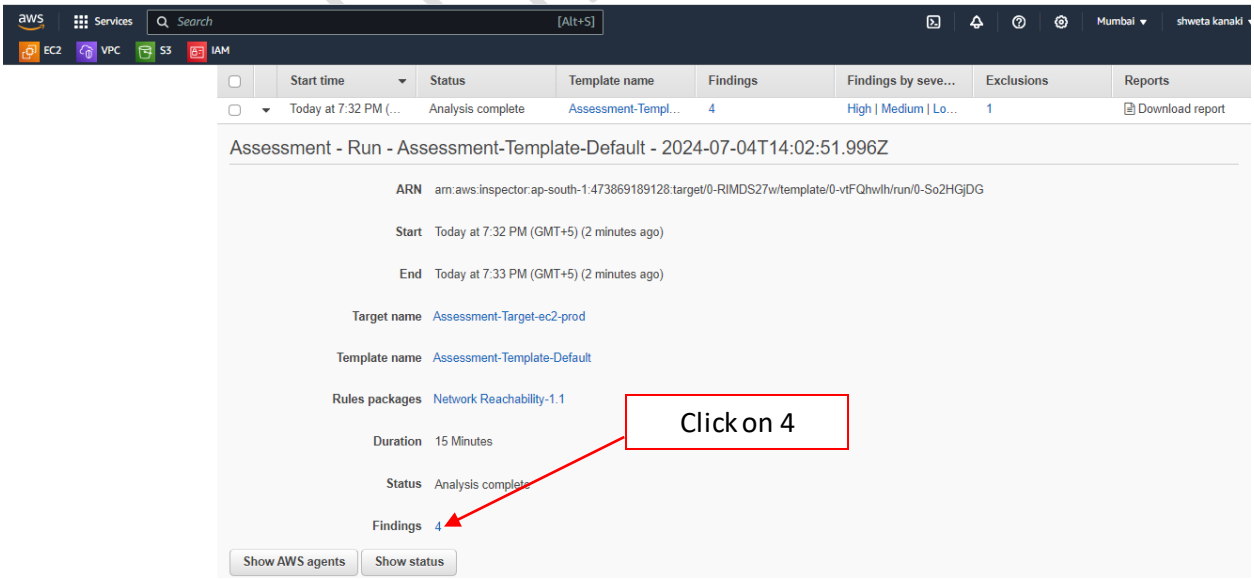


Now go back to assessment runs

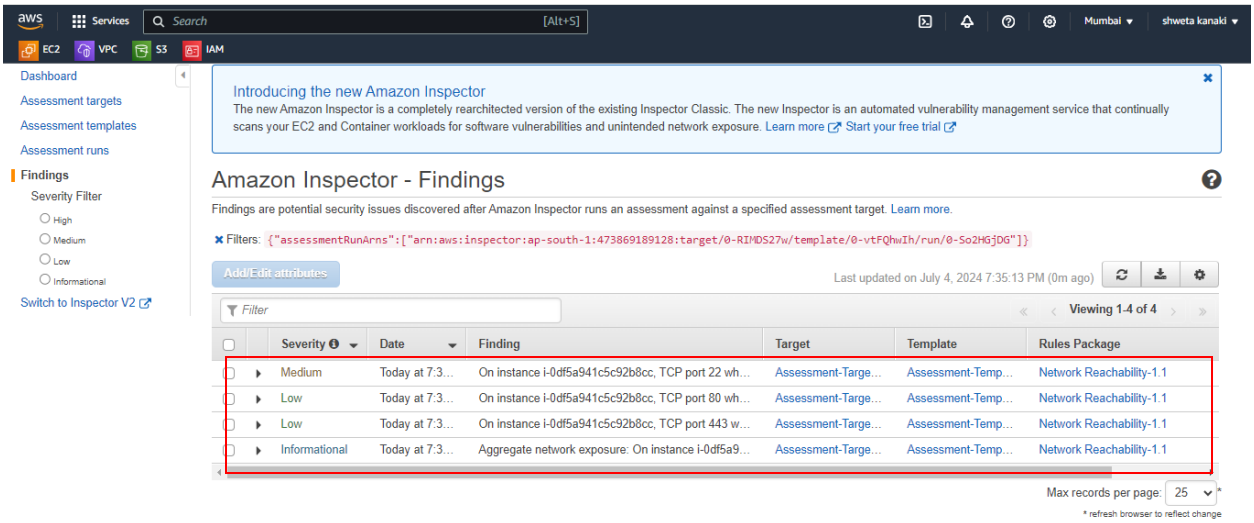



Introducing the new Amazon Inspector
Amazon Inspector - Assessment Runs
Now the findings have become 4


Introducing the new Amazon Inspector
Amazon Inspector - Assessment Runs
Click on the new run


Assessment - Run - Assessment-Template-Default - 2024-07-04T14:02:51.996Z
Click on 4

High risk has been eliminated



Step 5: Delete assessment targets after practicing.

Go to assessment targets, select the assessment and click delete