**Amazon Inspector: Overview, Benefits and How to Get Started?**

* [What is Amazon Inspector](https://k21academy.com/amazon-web-services/amazon-inspector/#1)
* [Benefits of AWS Inspector](https://k21academy.com/amazon-web-services/amazon-inspector/#2)
* [How Amazon Inspector Works](https://k21academy.com/amazon-web-services/amazon-inspector/#3)
* [Getting Started with Amazon Inspector](https://k21academy.com/amazon-web-services/amazon-inspector/#4)
* [Case Study](https://k21academy.com/amazon-web-services/amazon-inspector/#5)

**What is Amazon 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.

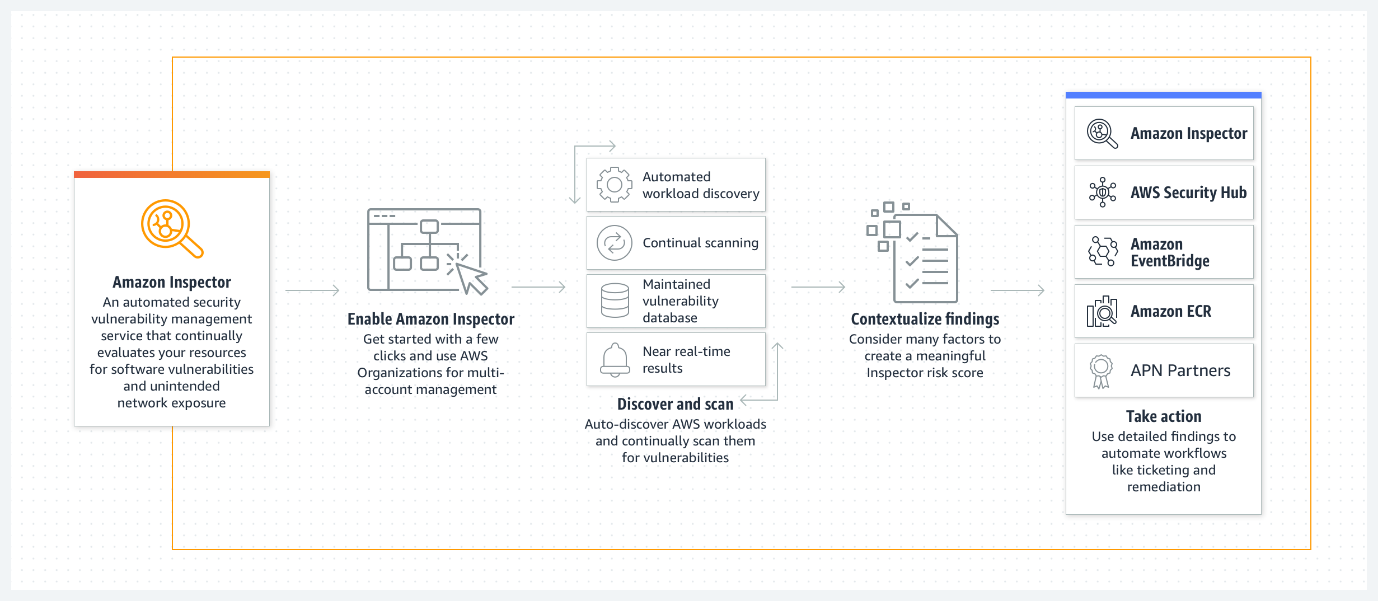
Amazon Inspector provides a clear list of security and compliance findings assigned a priority by the severity level. Moreover, these findings can be analyzed directly or as part of comprehensive assessment records available via the API or AWS Inspector console. AWS Inspector security assessments help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

**Benefits of AWS Inspector**

Amazon Inspector is a safe and reliable service we can use for security purposes in our services, deployed applications, etc. It’s an automated and managed service. Let’s see some key benefits of AWS Inspector.

* **Automated Service:** AWS Inspector is a beneficial service for the application’s security in the AWS cloud.  It can fix automatically without the interaction of human resources.
* **Regular Security Monitoring:**Amazon Inspector helps to find security vulnerabilities in applications, as well as departures from security best practices, both before they’ve been deployed or running in production. This improves the overall security of your AWS-hosted applications.
* **Leverage Aws Security Expertise:**AWS Inspector includes a knowledge base of the number of rules charted to common security best practices and vulnerability definitions. It uses AWS’s Security Expertise, where AWS is constantly updating the security best practices and rules, so one gets the best of both worlds.
* **Integrate Security Into DevOps:** AWS Inspector is an API-bound service that analyzes network configurations in your AWS account. Moreover, it uses an optional agent for visibility into EC2 instances. The agent makes it easy to build Inspector assessments right into your existing DevOps process and empowers both development and operations teams to make security assessments an essential part of the deployment process.
* **Network reachability price package regulations**: Assessments performed by Amazon Inspector Classic that include network reachability rules are priced per instance per assessment (instance assessment) per month. One instance assessment is one that you perform against one instance. Ten instance assessments will result from doing one assessment against ten instances. With bulk reductions, pricing can be lowered to $0.04 per instance assessment per month from the starting price of $0.15 per instance assessment per month.
* **Package prices for host assessment rules:** The host assessment rules packages for Amazon Inspector Classic employ an agent that is deployed on the Amazon EC2 Instances running the apps you want to evaluate. Each month, host rules assessments (sometimes known as “agent assessments”) are charged per agent. A single-agent assessment is one that is performed against a single agent. Ten agent assessments will result from running one assessment against ten agents. With volume reductions, pricing can be lowered to as little as $0.05 per agent assessment per month from the starting price of $0.30 per agent assessment per month.

**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.

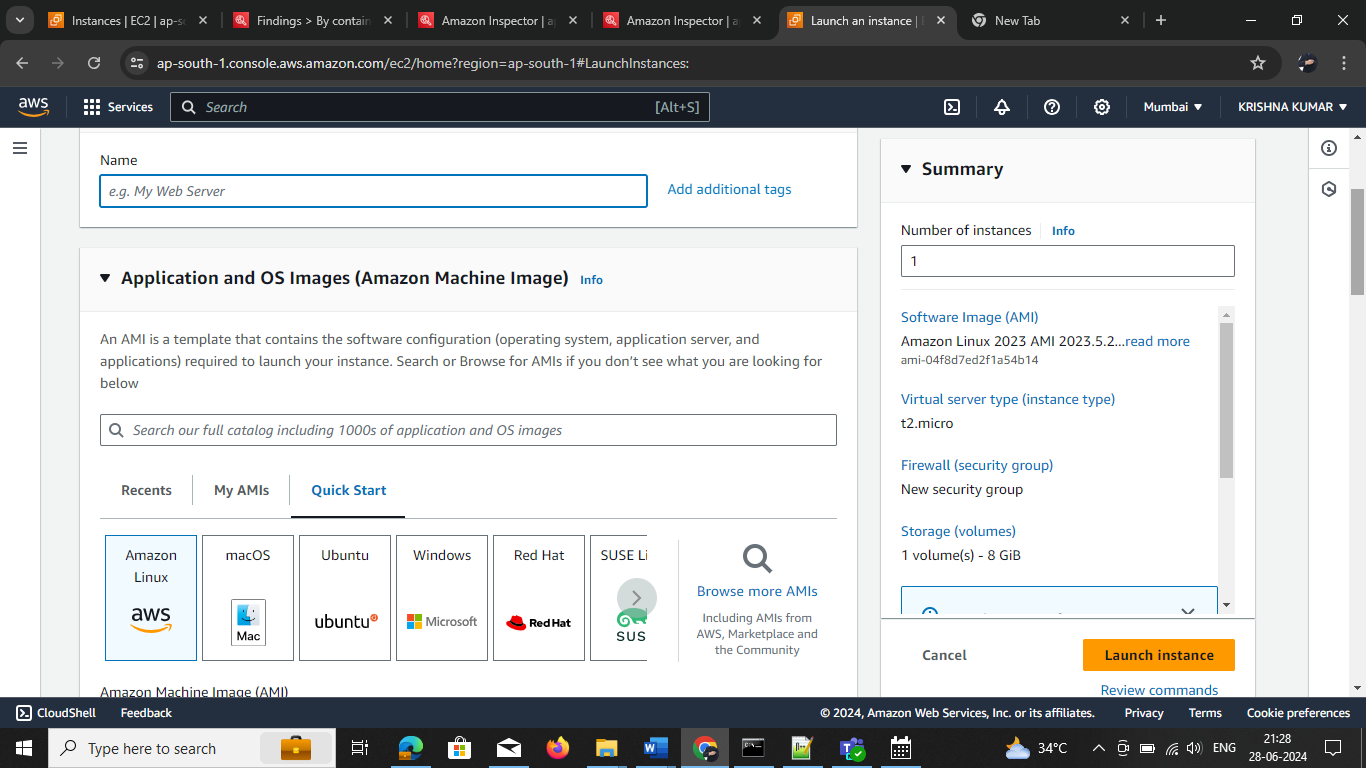
An Inspector Agent runs on the EC2 machines hosting the application that monitors the network, file system, and process activity. After collecting all the required data, it is compared with the built-in security rules to identify security or compliance issues.

**Getting Started With Amazon Inspector**

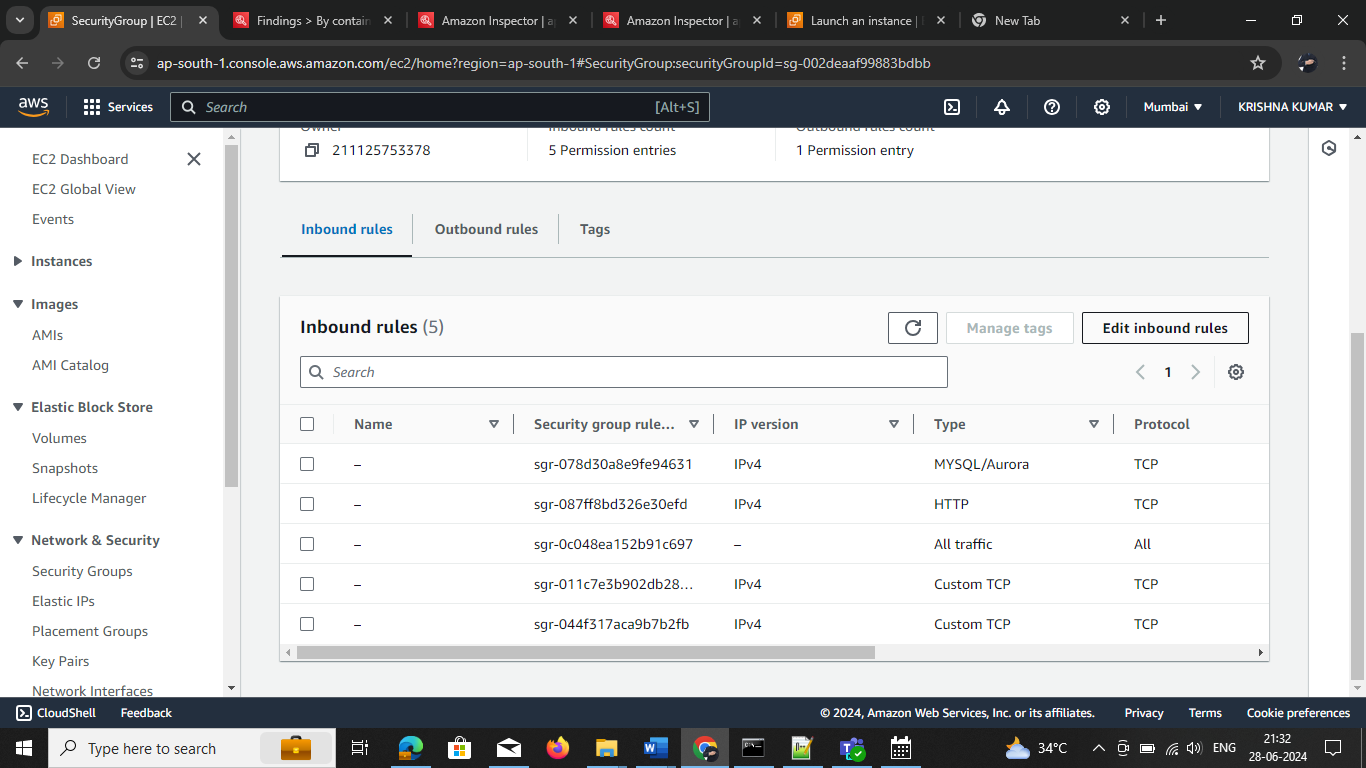
AWS Inspector is a security service that helps to monitor and improve the security and compliance of web applications running inside AWS. So in this guide, we have a production EC2 instance for which we need to perform a network accessibility check.

We will set up an EC2 instance to use with Amazon Inspector and induce a security thread, and we will open port 21 on EC2. Port 21 is generally not recommended to keep open on your instances. Follow the steps mentioned below.

**Step 1. Launch An EC2 Instance:** Firstly, if you don’t have an AWS account, [Register for AWS Free Tier Account](https://k21academy.com/amazon-web-services/aws-solutions-architect/create-aws-free-tier-account/). Secondly, we will launch a [Linux EC2 instance](https://docs.aws.amazon.com/quickstarts/latest/vmlaunch/step-1-launch-instance.html).

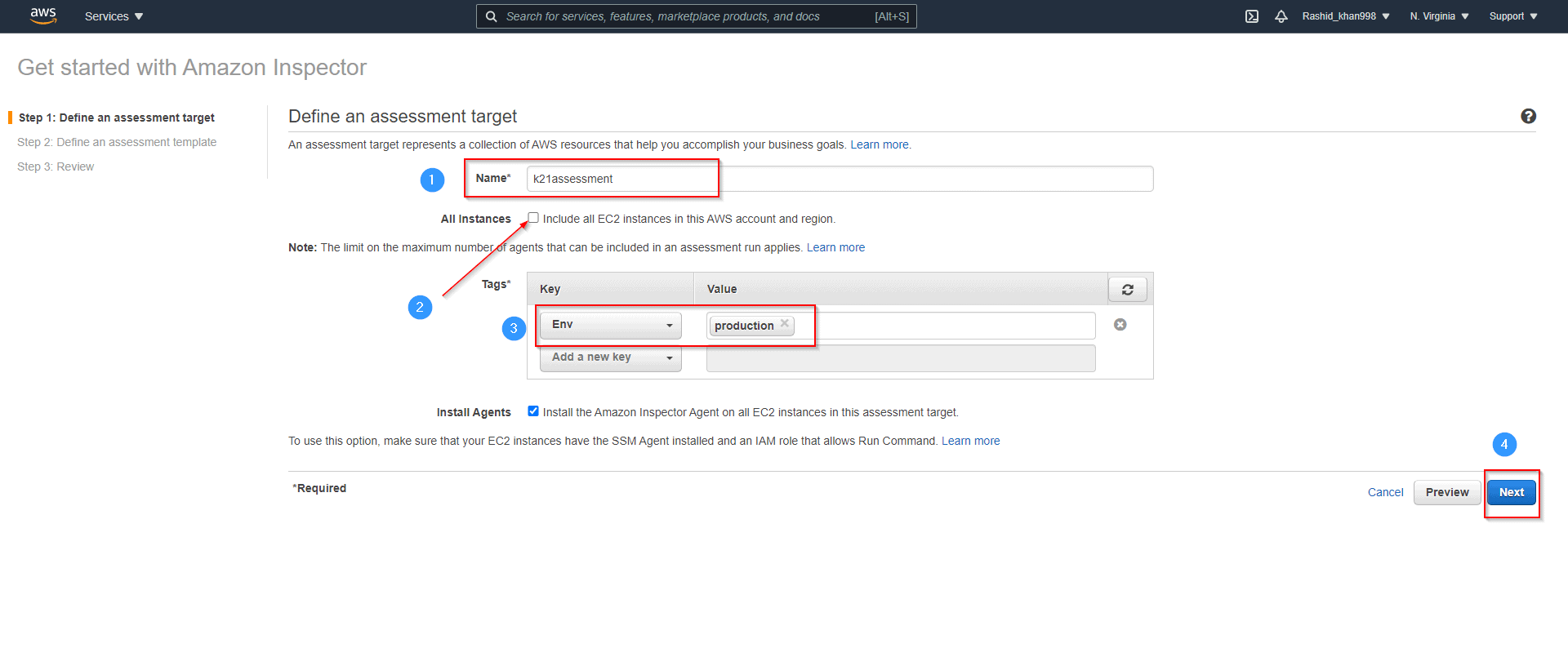
1. Click on **Launch Instance.**
2. Select Amazon Linux AMI(HVM), SSD Volume Type.
3. **Select** Subnet and **Enable** Auto-assign public IP
4. Add a **Tag** to your EC2 instance.
5. Configure Security Group and Select **EC2-SG**(existing security group)

**Step 2. Modify Security Group & Open Port 21:**After launching the EC2 instance, we have to modify the security group**inbound port 21 open**.



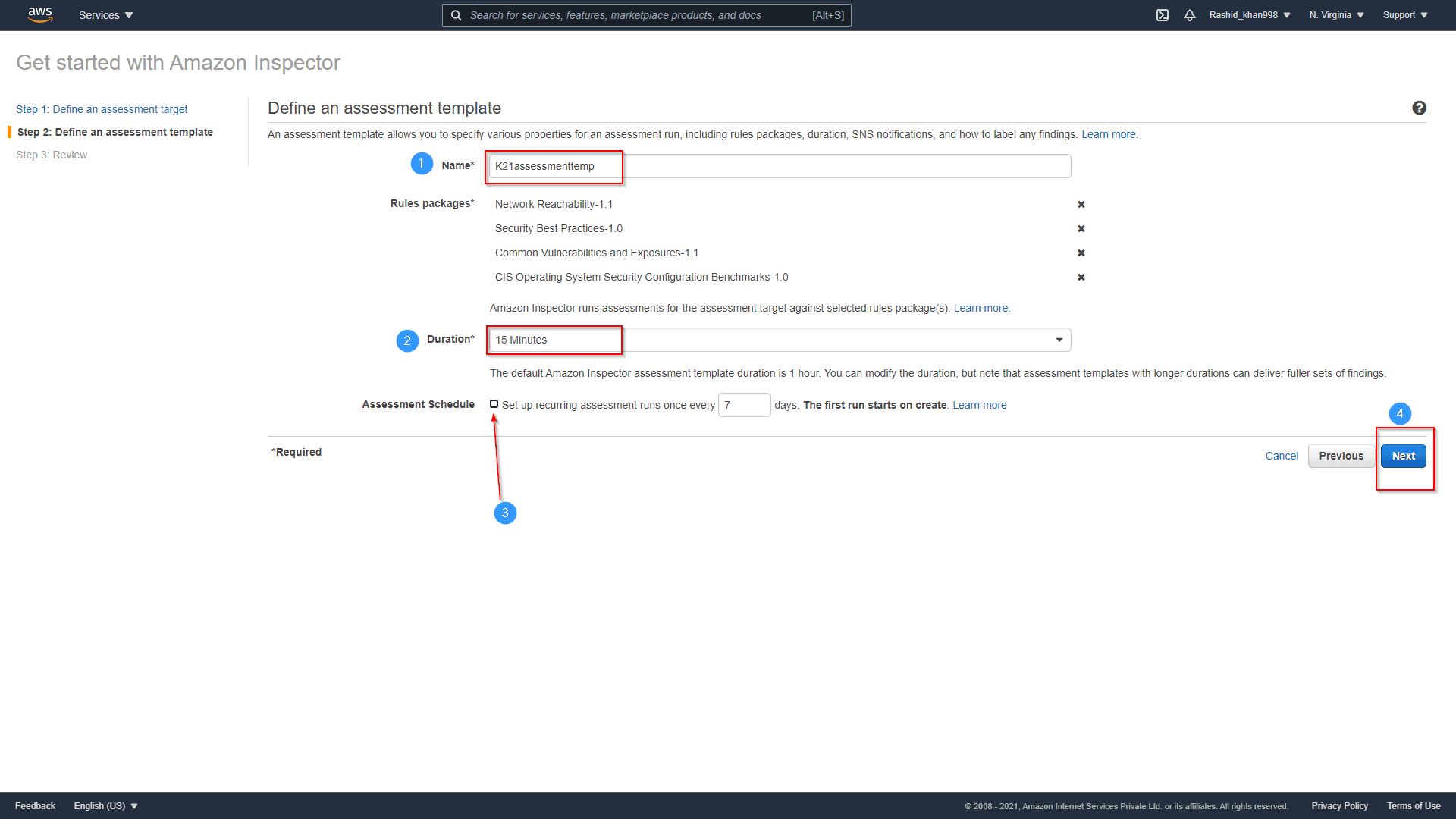
**Step 3. Define An Assessment target:**Now, select the EC2 instance as the assessment target

* Go to Services and choose **Amazon Inspector**, click on **Get Started.**
* **Define** an Assessment target and **check** Install Agent on EC2

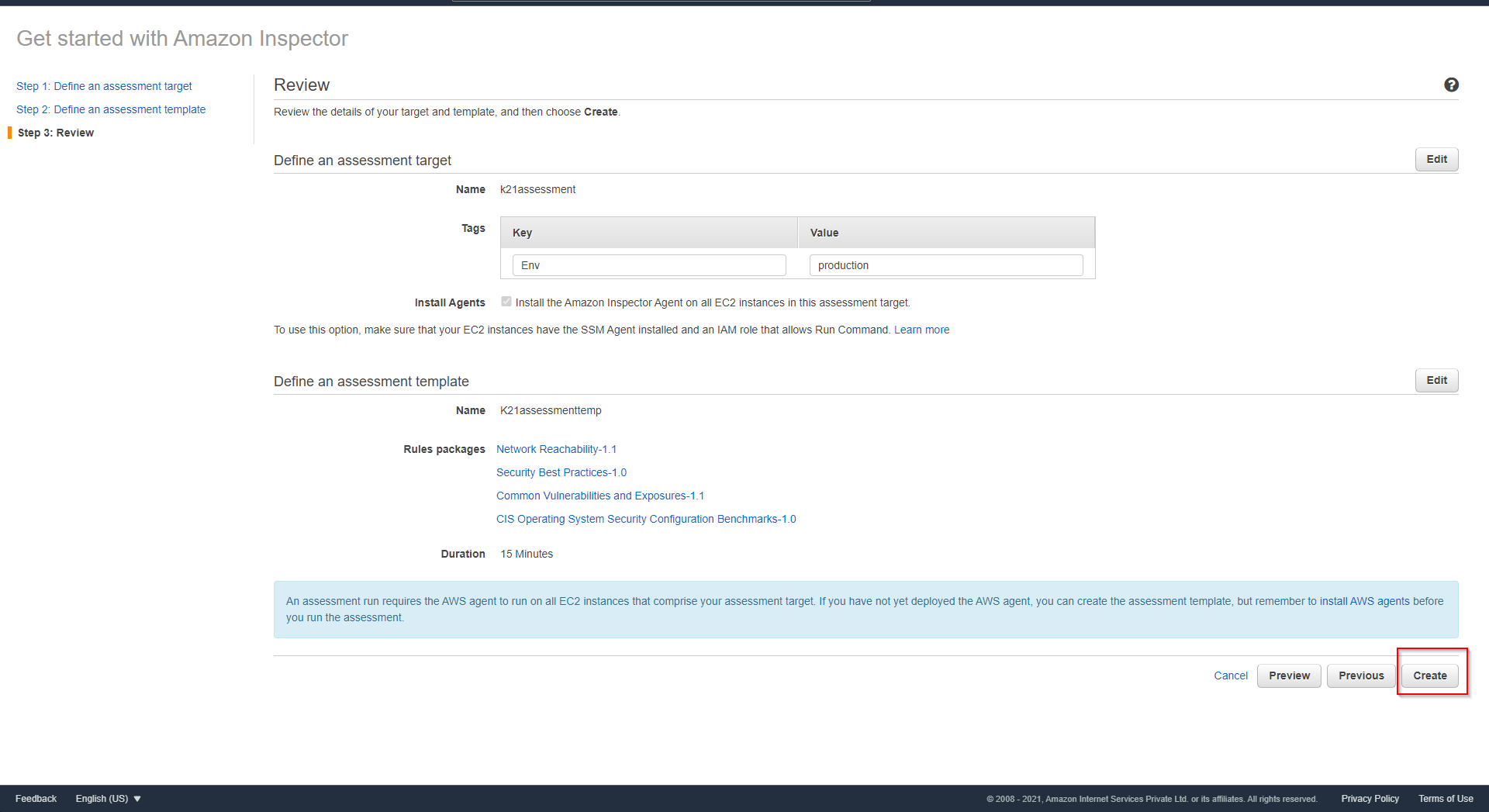


**Step 3. Define An Assessment Template:**After the assessment target, now define the assessment template.

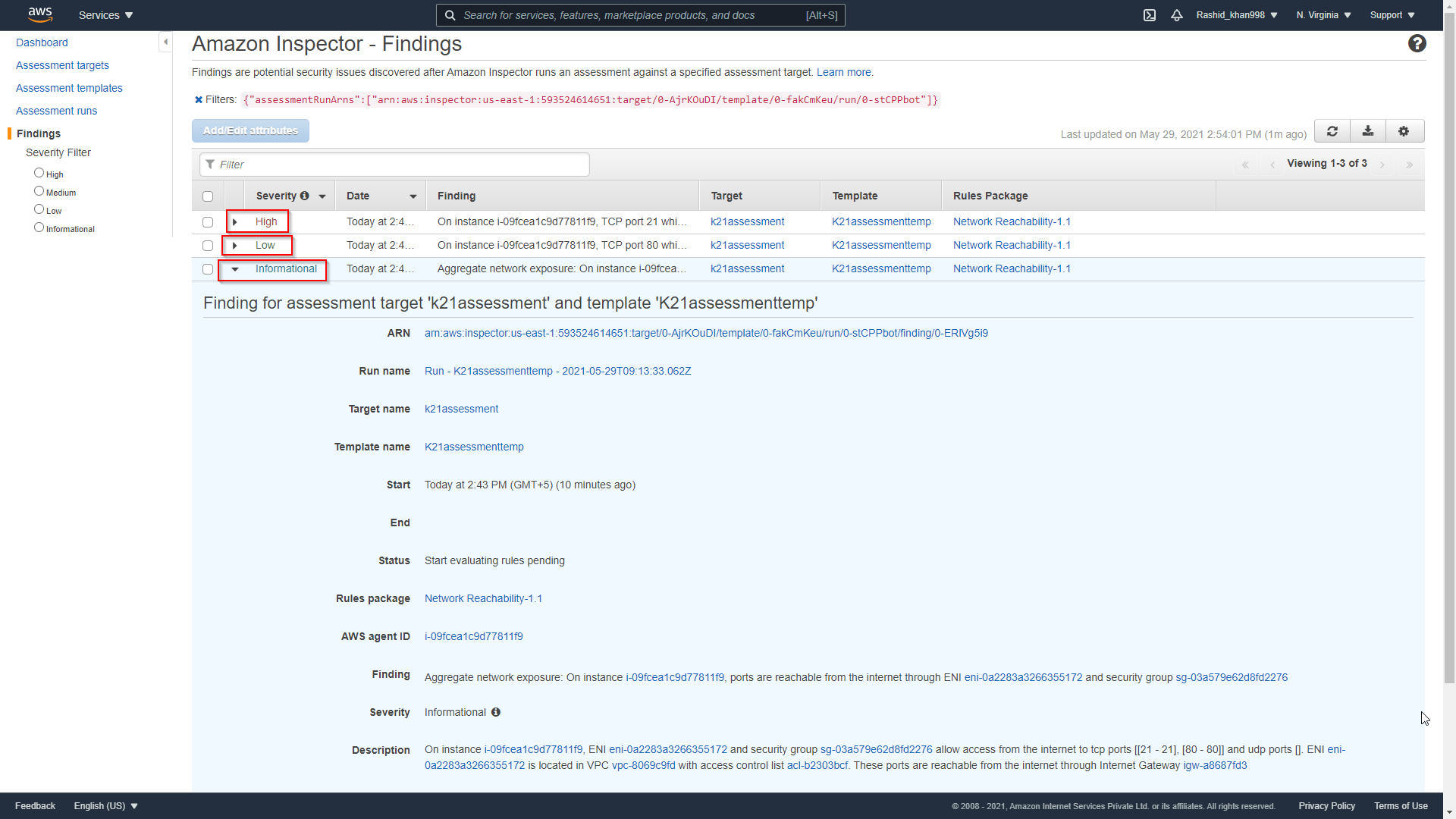
1. Please give it a name: K21assessmenttemp
2. Set Duration to **15 Min** ( as its demo)
3. **Uncheck** Assessment Schedule and hit **Next**



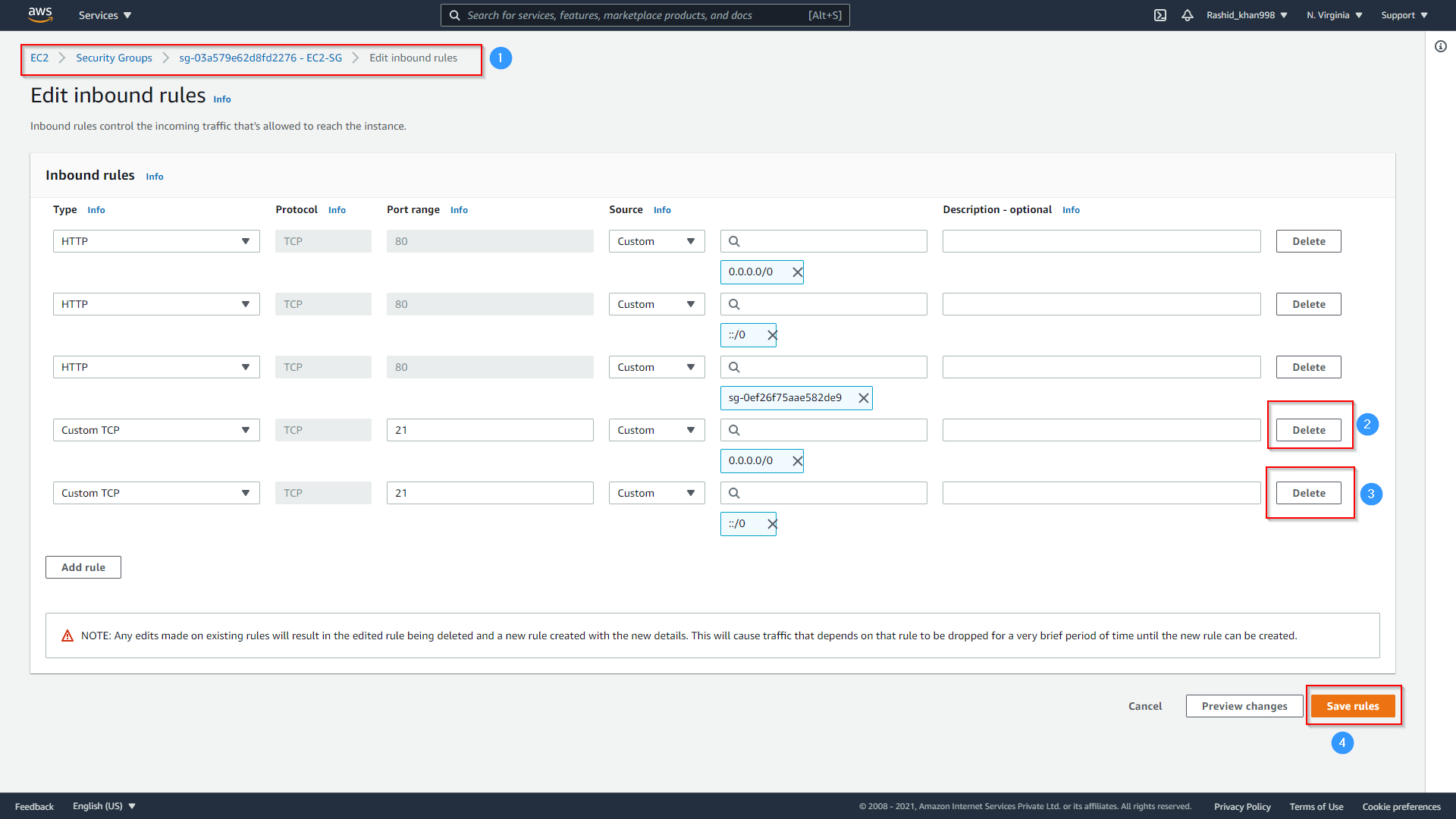
Now Review and click on Create



**Step 4. Findings:** Assessment Run will start automatically. Now, go to the findings and Review the risk.



**Step 5. Remove Open Port:**Go back to EC2 and **Delete open ports**.



**Step 6. Again Review Findings:**After successfully deleting open ports, we will run the Assessment and review Finding; this time, there is no High-risk showing.