Lesson 07 Demo 06

Configuring AWS Inspector for Network Reachability and Vulnerability

Objective: To demonstrate the process of configuring AWS Inspector to enhance the security and compliance of the AWS environment

Tools required: AWS Management Console

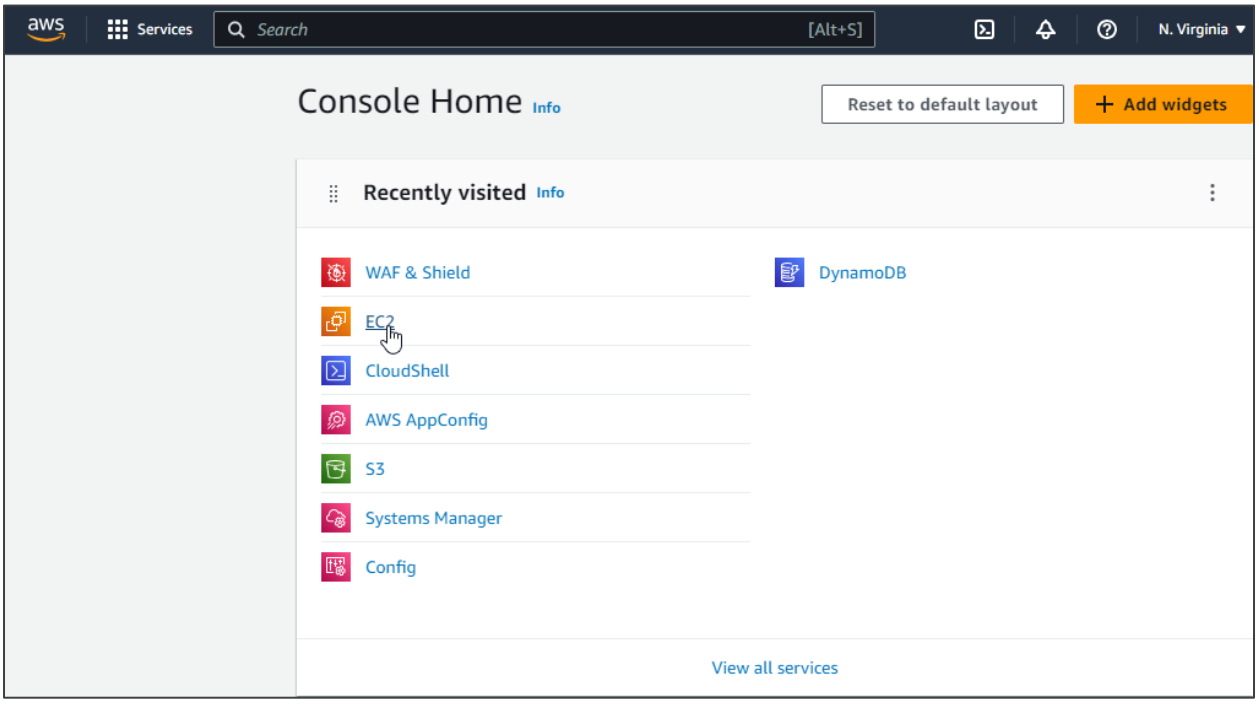
Prerequisites: AWS account

Steps to be followed:

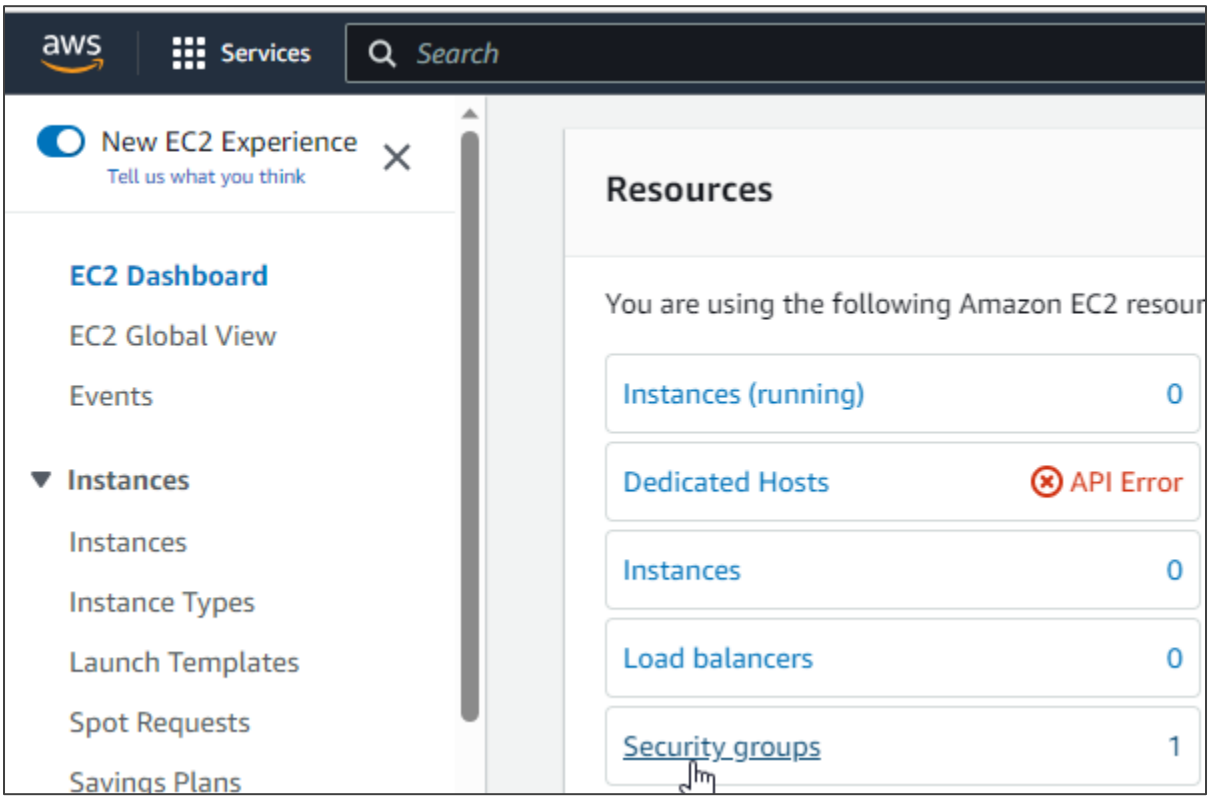
1. Create security group and launch instances
2. Configure the AWS Inspector

Step 1: Create security group and launch instances

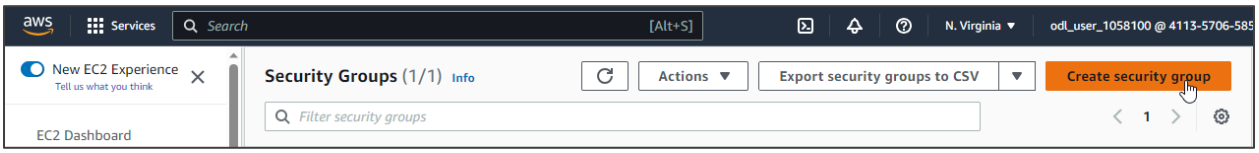
1.1 Navigate to the AWS portal, search for and select **EC2** from the services



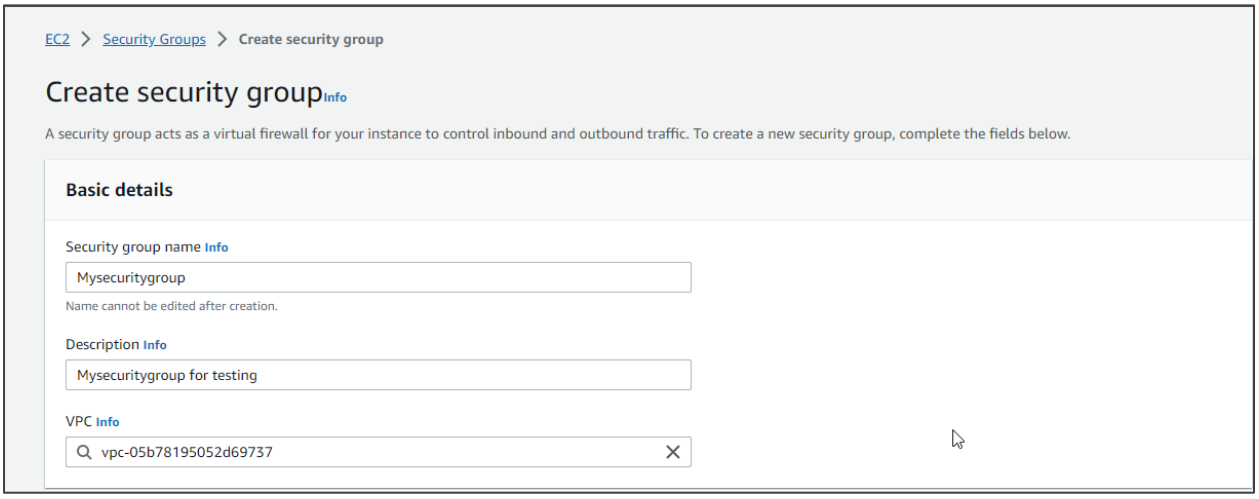
1.2 In the EC2 dashboard, click on **Security groups**



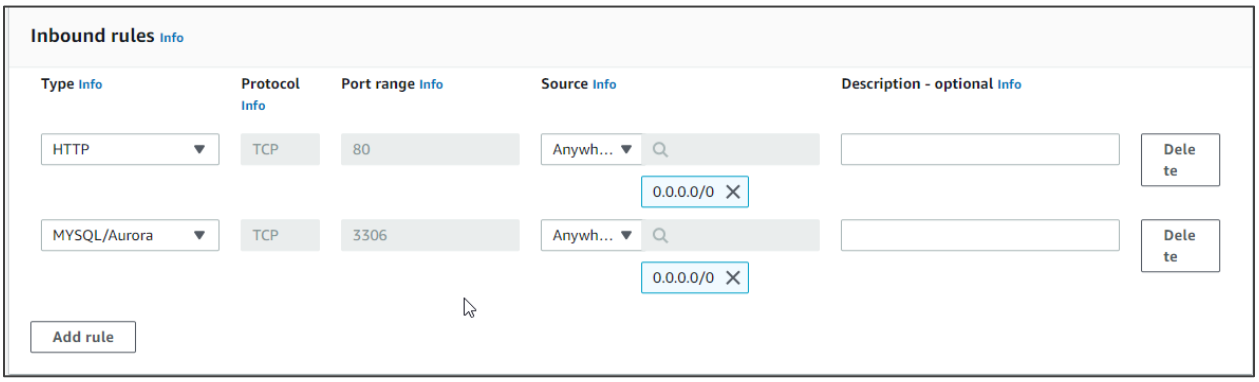
1.3 Click on **Create security group**



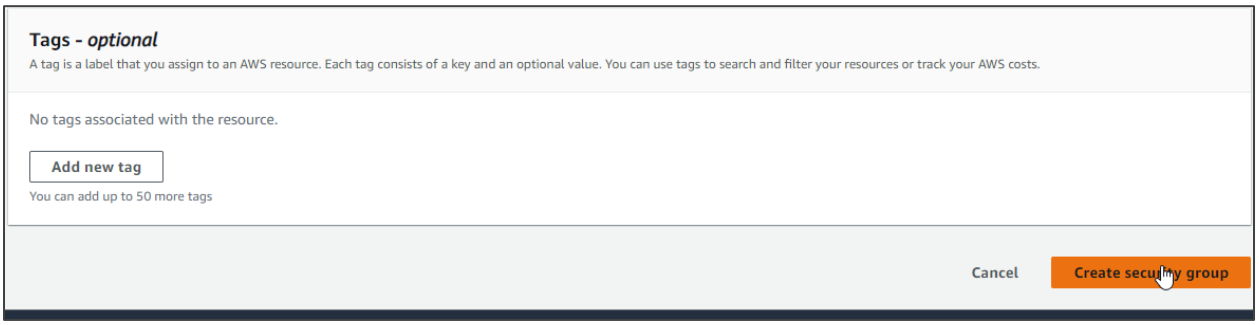
1.4 Provide the name and the description for the security group



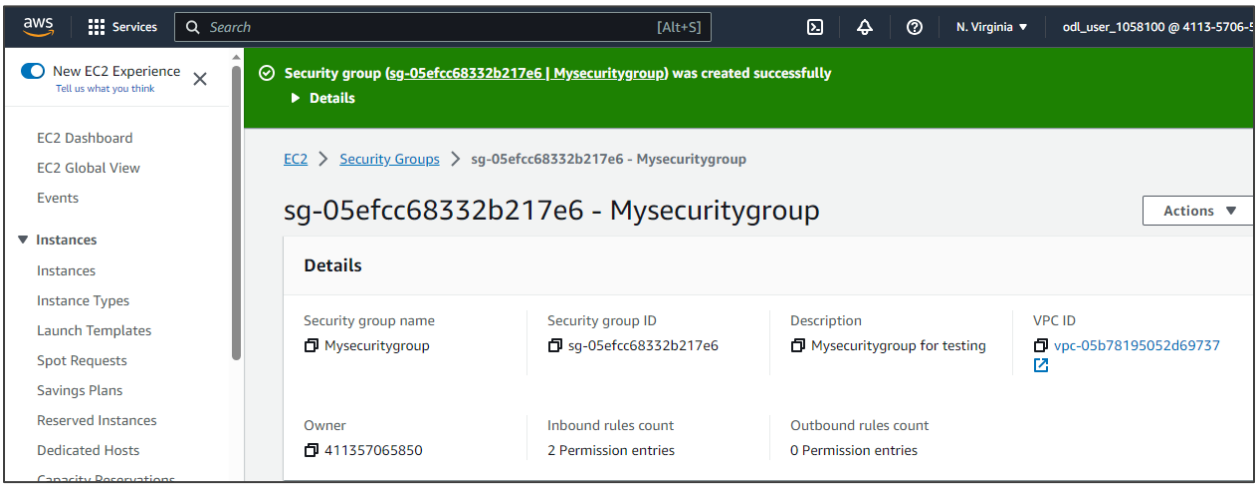
1.5 Add the Inbound rules



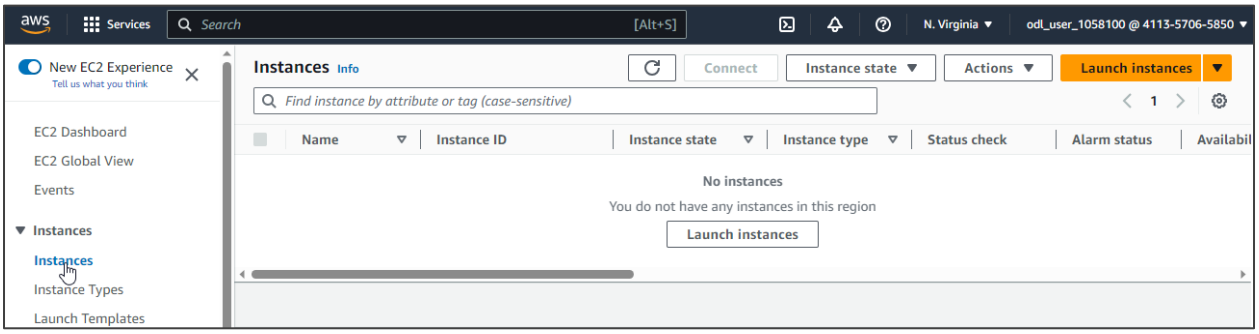
1.6 Now, click on **Create security group**



The security group is created successfully.

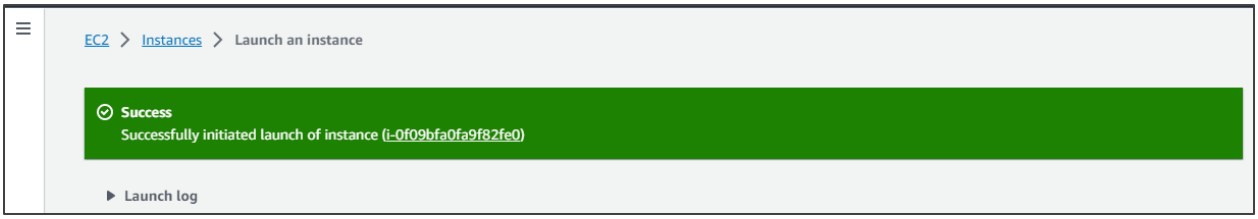


1.7 Now, navigate to the EC2 dashboard, select **Instances**, and then click on **Launch instances**



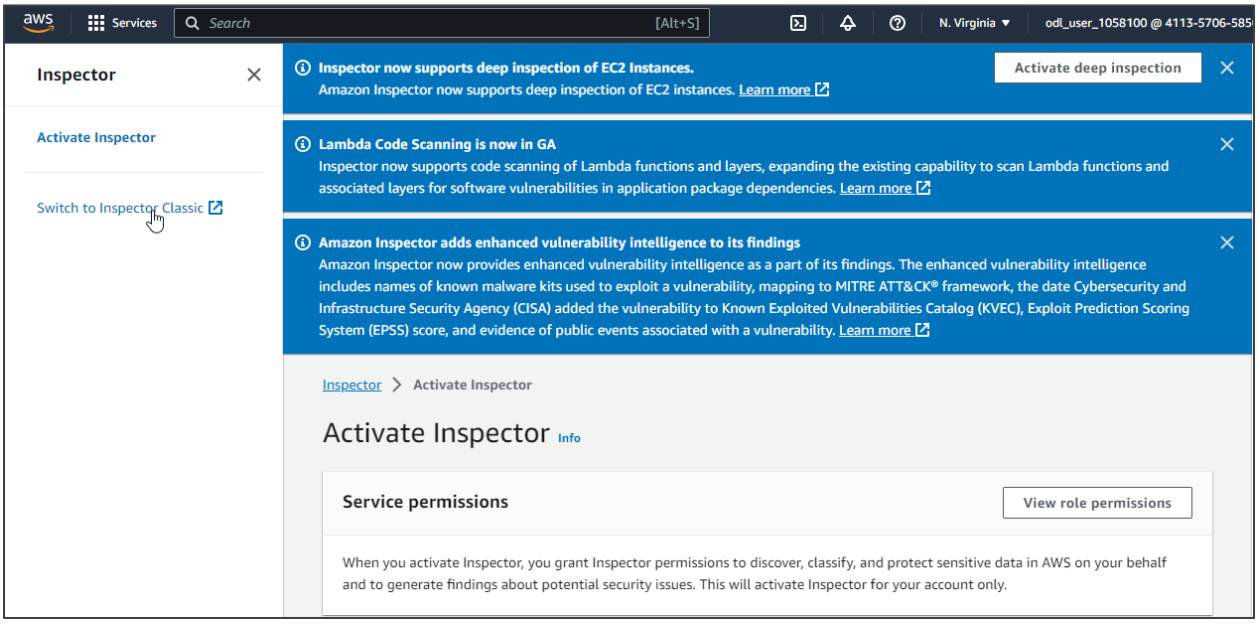
Note: Please refer to previous lesson demos on how to launch an EC2 instance.

The instance is created successfully.

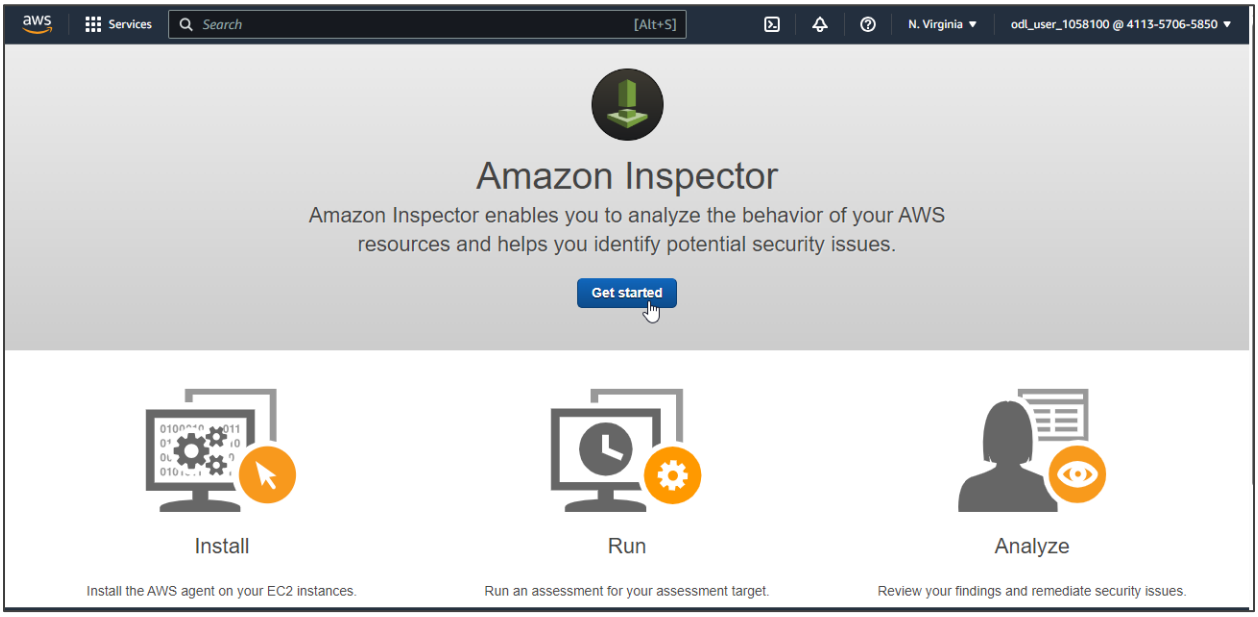


Step 2: Configure the AWS Inspector

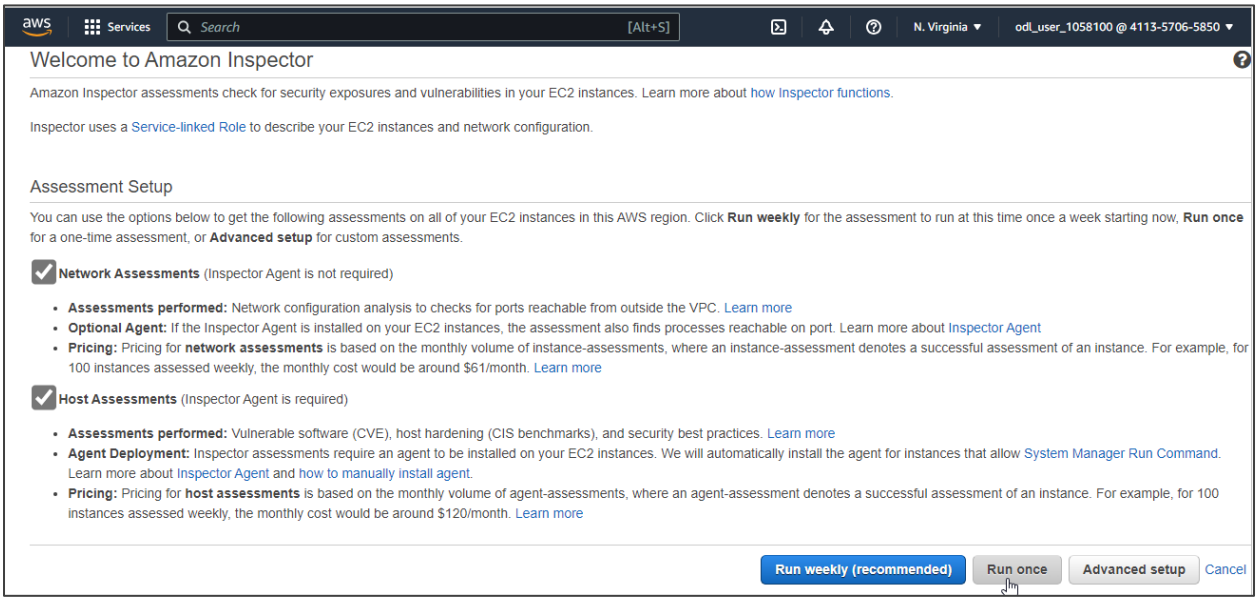
2.1 Now, search for and select **Amazon Inspector** from the Services



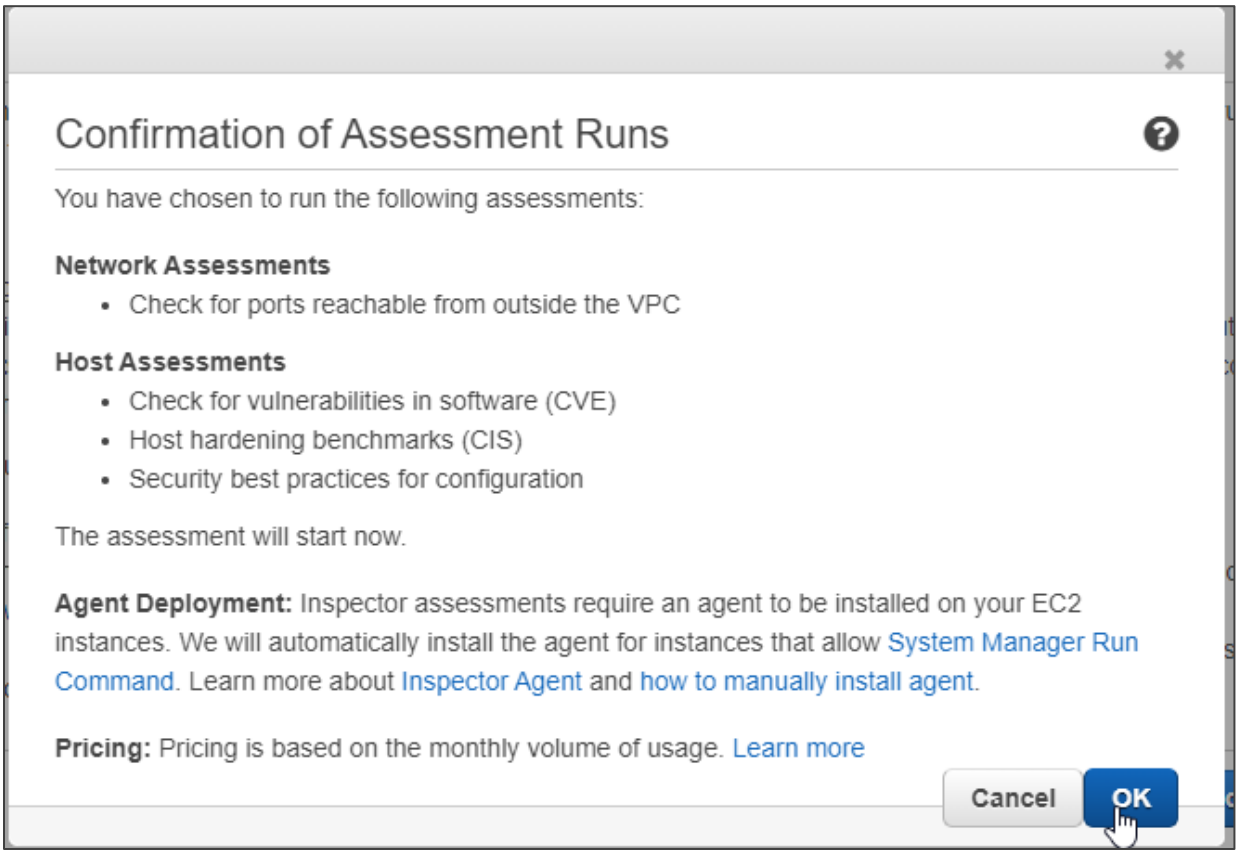
2.2 In the Inspector dashboard, select **Switch to Inspector Classic** from the left pane, and then click on **Get started**



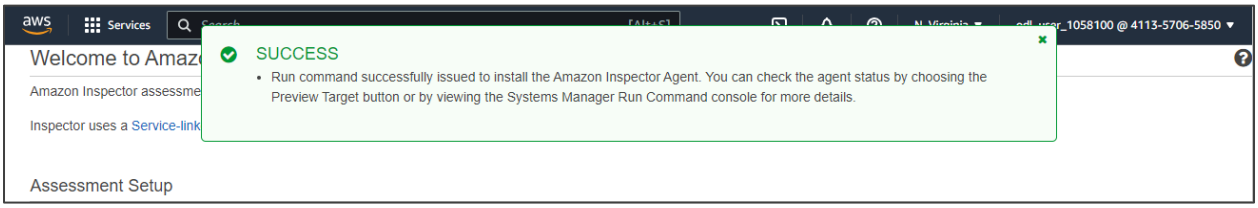
2.3 In the **Welcome to Amazon Inspector page**, select **Run once**



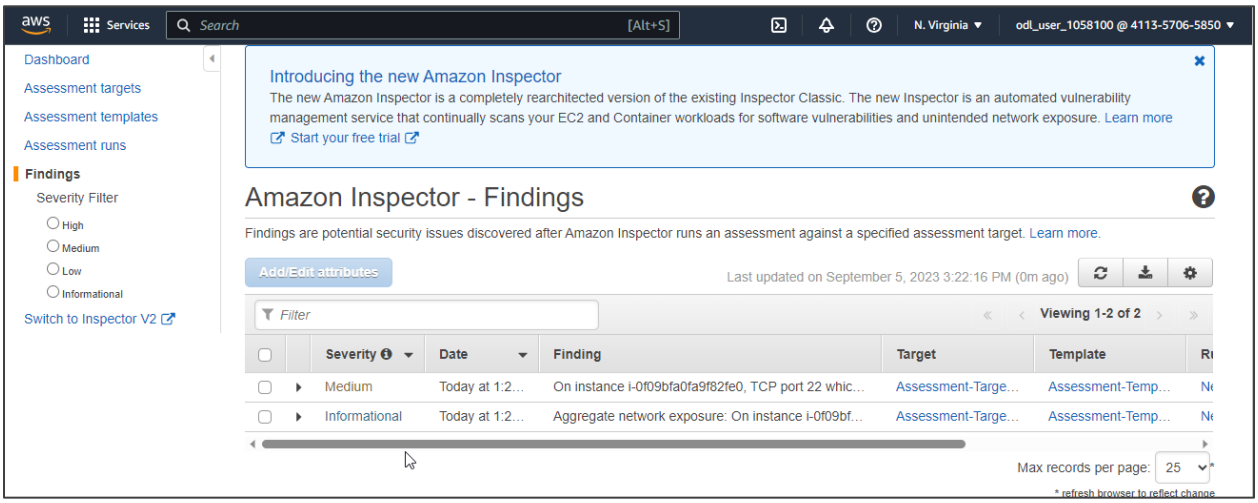
2.4 Select **OK** from the pop-up window



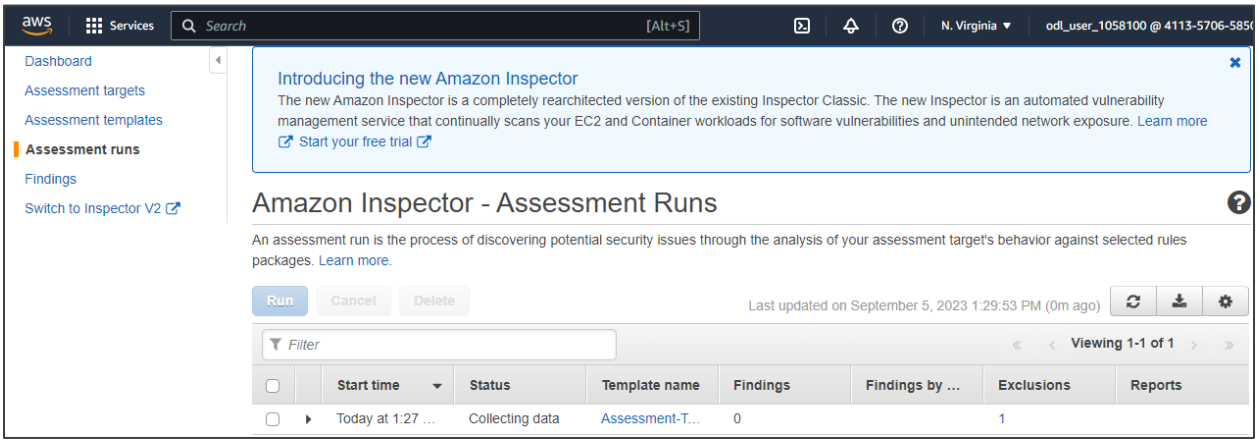
The set up for Amazon Inspector is completed.



2.5 Now, select **Findings** from the left navigation pane in the Inspector dashboard to view the severity in the Inspector



2.6 Now, select **Assessment runs** from the left navigation pane to view the template name and its status



By following these steps, you have successfully demonstrated the process of creating the security groups, launching the instances, and configuring the AWS Inspector.