

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

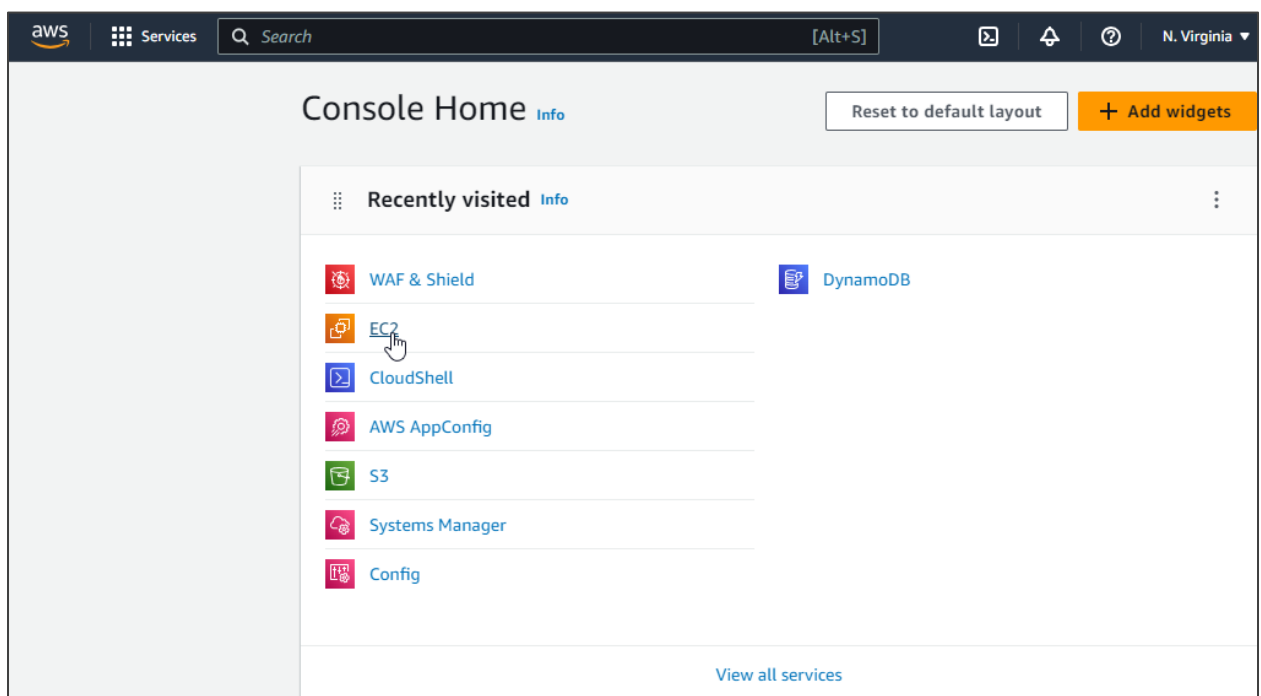
Prerequisites: AWS account

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



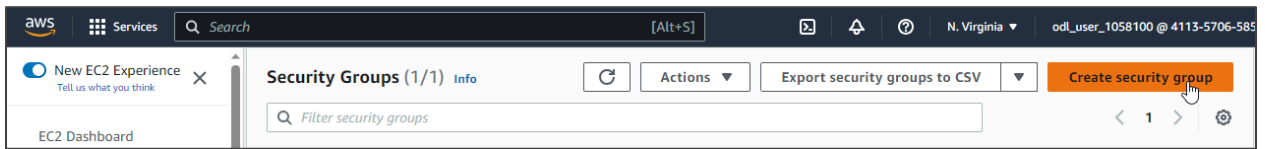
1.2 In the EC2 dashboard, click on **Security groups**

The screenshot shows the AWS Management Console interface for the EC2 dashboard. The top navigation bar includes the AWS logo, a 'Services' menu, and a search bar. The left-hand navigation pane lists various EC2-related options: 'New EC2 Experience' (with a feedback link), 'EC2 Dashboard', 'EC2 Global View', 'Events', and a collapsed 'Instances' section which contains links to 'Instances', 'Instance Types', 'Launch Templates', 'Spot Requests', and 'Savings Plans'. The main content area, titled 'Resources', displays a list of EC2 resources currently in use. A table shows the following data:

| Resource Type | Count |
|------------------------|-------------|
| Instances (running) | 0 |
| Dedicated Hosts | ⊗ API Error |
| Instances | 0 |
| Load balancers | 0 |
| <u>Security groups</u> | 1 |

A mouse cursor is pointing at the 'Security groups' link, which is underlined. The 'Dedicated Hosts' row shows an 'API Error' status.

1.3 Click on **Create security group**



1.4 Provide the name and the description for the security group

[EC2](#) > [Security Groups](#) > Create security group

Create security group Info

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

Security group name Info

Name cannot be edited after creation.

Description Info

VPC Info

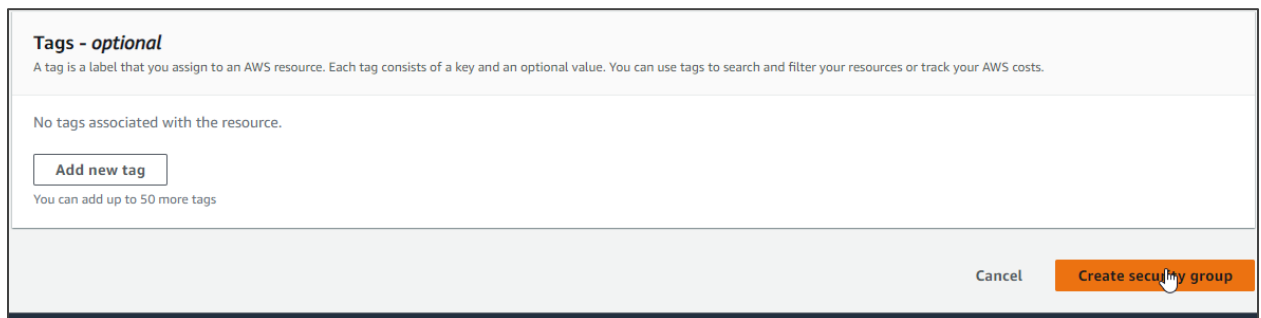
1.5 Add the Inbound rules

Inbound rules Info

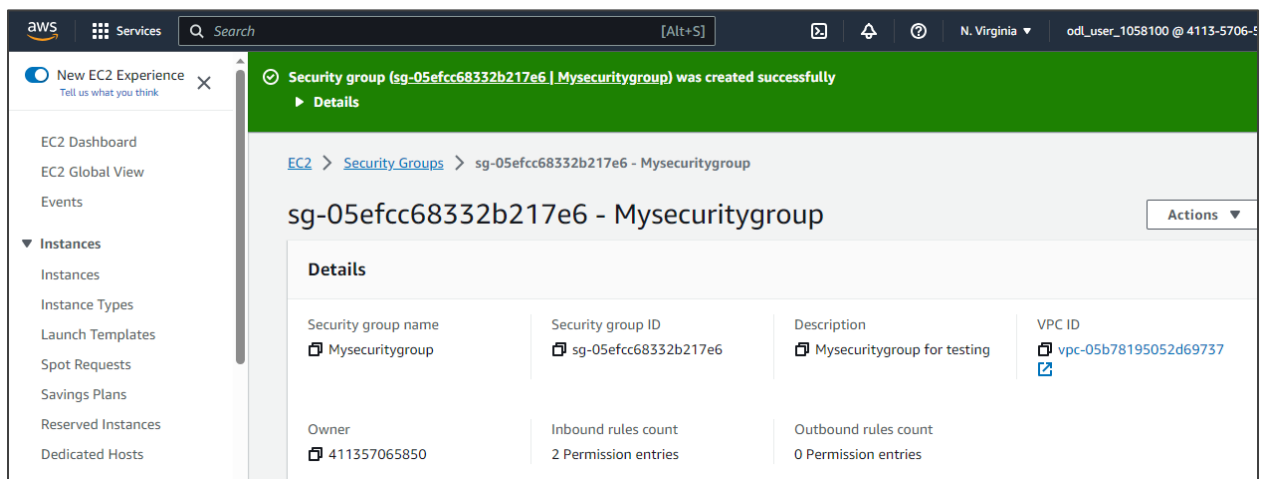
| Type <small>Info</small> | Protocol <small>Info</small> | Port range <small>Info</small> | Source <small>Info</small> | Description - optional <small>Info</small> | |
|--------------------------|------------------------------|--------------------------------|---|--|--------|
| HTTP | TCP | 80 | Anywh... <input type="text" value="0.0.0.0/0"/> | | Delete |
| MYSQL/Aurora | TCP | 3306 | Anywh... <input type="text" value="0.0.0.0/0"/> | | Delete |

Add rule

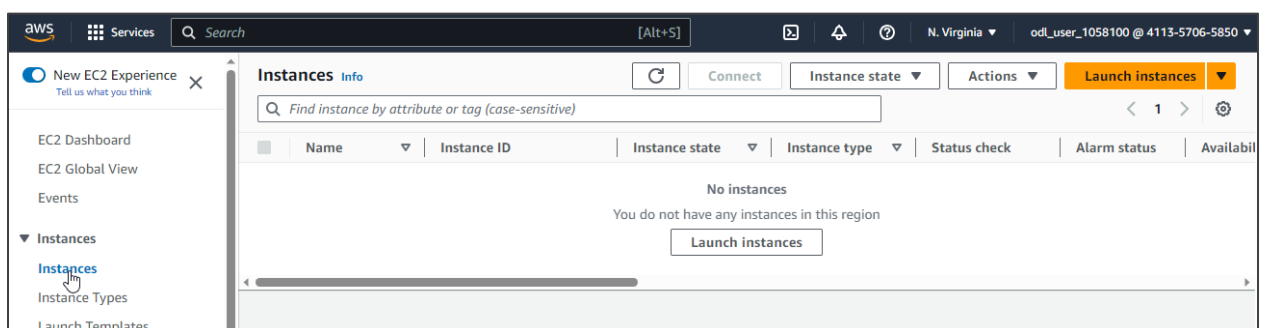
1.6 Now, click on **Create security group**



The security group is created successfully.

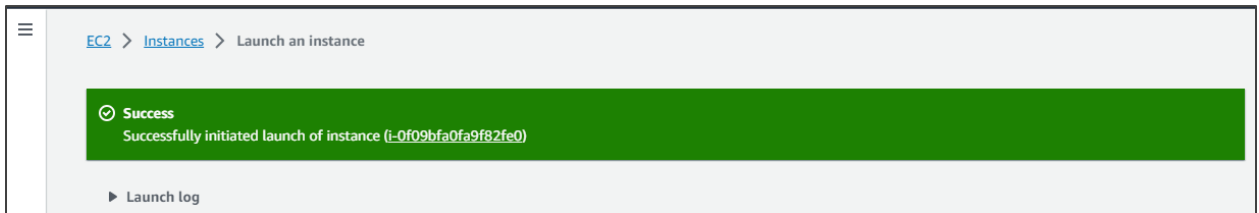


1.7 Now, navigate to the EC2 dashboard, select **Instances**, and then click on **Launch instances**



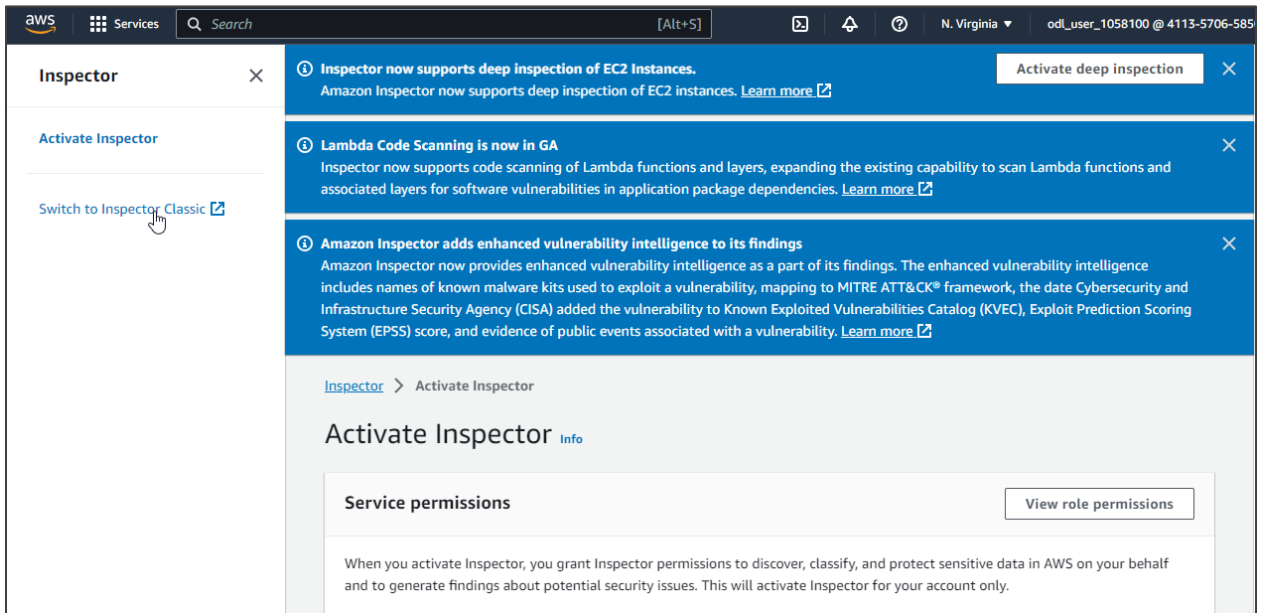
Note: Please refer to previous lesson demos on how to launch an EC2 instance.

The instance is created successfully.

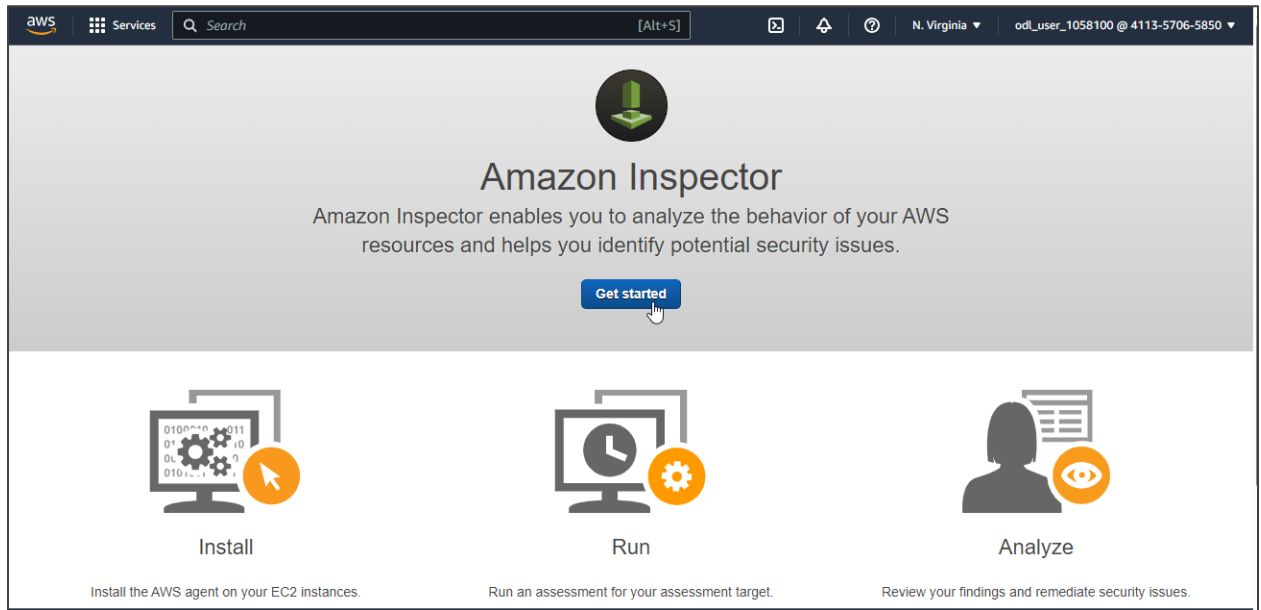


Step 2: Configure the AWS Inspector

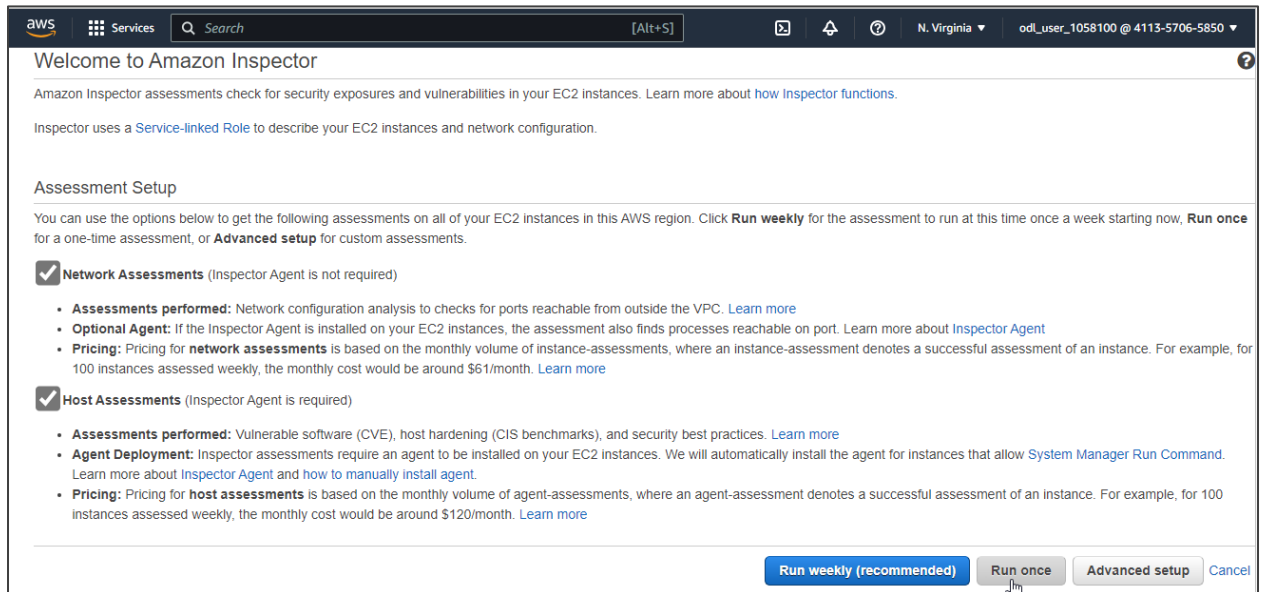
2.1 Now, search for and select **Amazon Inspector** from the Services



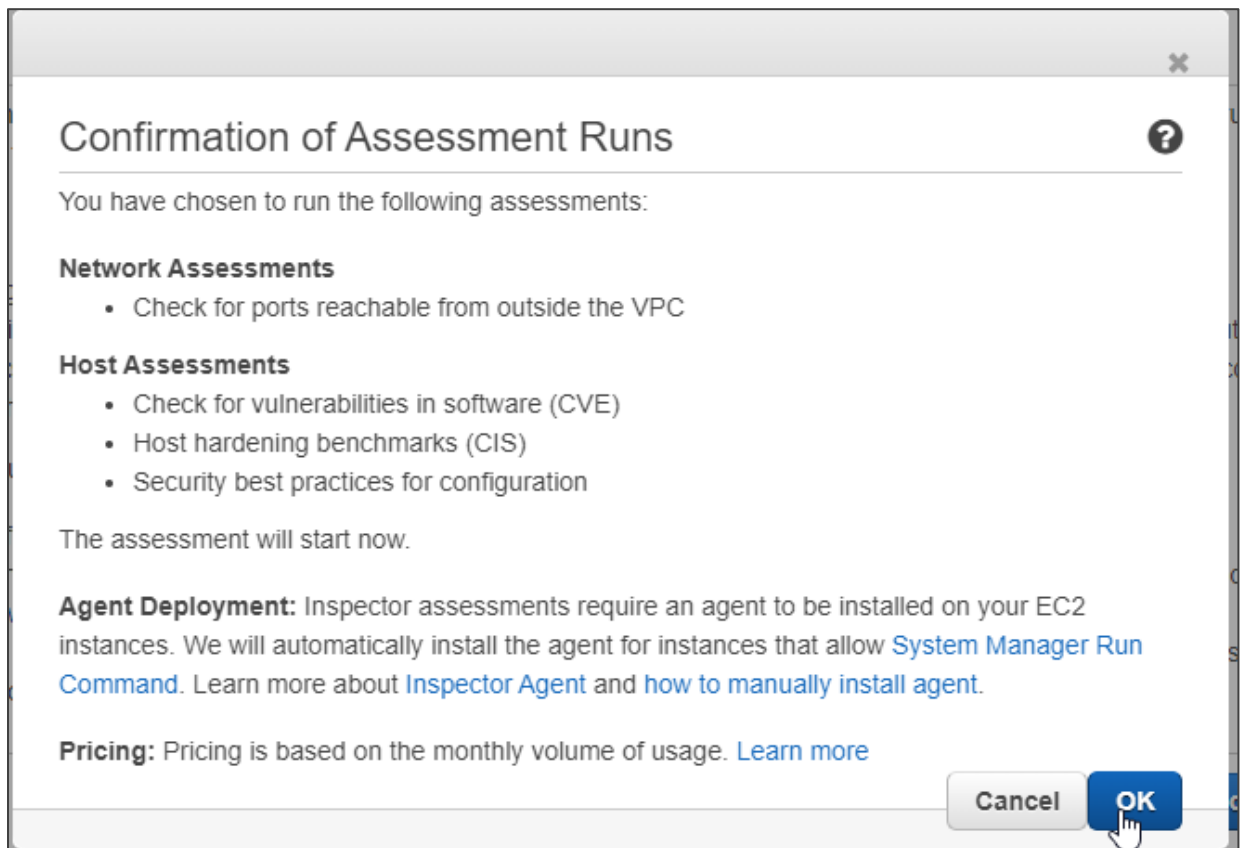
2.2 In the Inspector dashboard, select **Switch to Inspector Classic** from the left pane, and then click on **Get started**



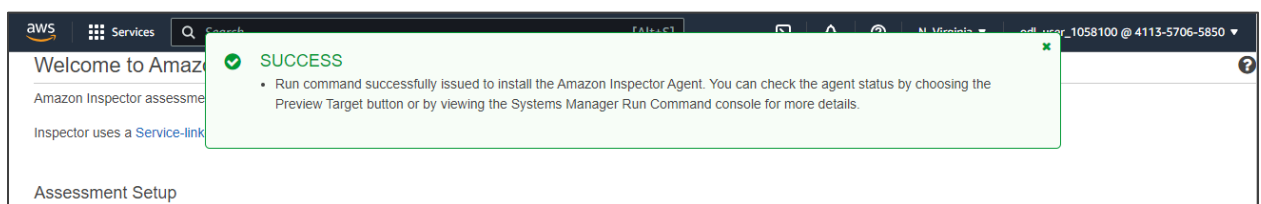
2.3 In the **Welcome to Amazon Inspector** page, select **Run once**



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

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 September 5, 2023 3:22:16 PM (0m ago)

Filter

| | Severity | Date | Finding | Target | Template | Relevance |
|--------------------------|---------------|-----------------|--|---------------------|--------------------|-----------|
| <input type="checkbox"/> | Medium | Today at 1:2... | On instance i-0f09bfa0fa9f82fe0, TCP port 22 whic... | Assessment-Targe... | Assessment-Temp... | N |
| <input type="checkbox"/> | Informational | Today at 1:2... | Aggregate network exposure: On instance i-0f09bf... | Assessment-Targe... | Assessment-Temp... | N |

Max records per page: 25 * refresh browser to reflect change

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

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 September 5, 2023 1:29:53 PM (0m ago)

Filter

| | Start time | Status | Template name | Findings | Findings by ... | Exclusions | Reports |
|--------------------------|-------------------|-----------------|-----------------|----------|-----------------|------------|---------|
| <input type="checkbox"/> | Today at 1:27 ... | Collecting data | Assessment-T... | 0 | | 1 | |

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