Lesson 07 Demo 06

Configuring AWS Inspector for Network Reachability and Vulnerability

Objective: To configure AWS Inspector to enhance the security and compliance of the AWS environment

Tools required: AWS Management Console

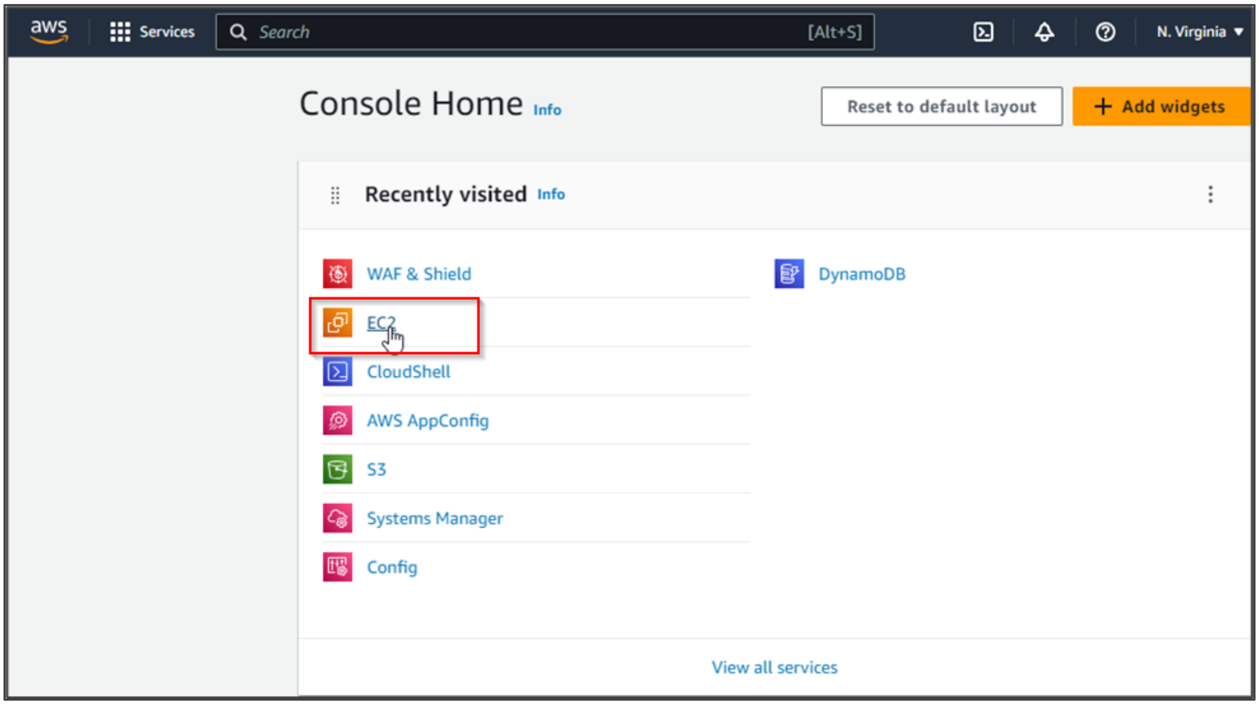
Prerequisites: AWS account

Steps to be followed:

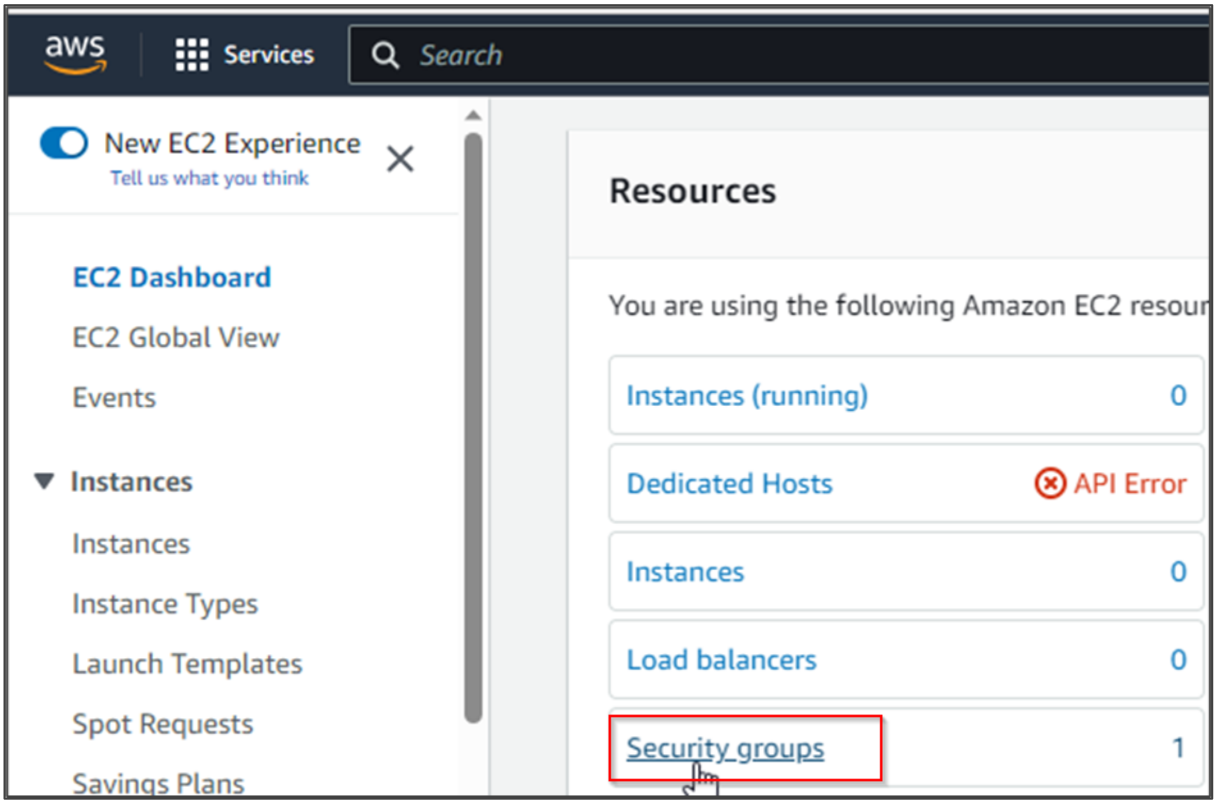
1. Create security group and launch instances
2. Configure the AWS Inspector

Step 1: Create security group and launch instances

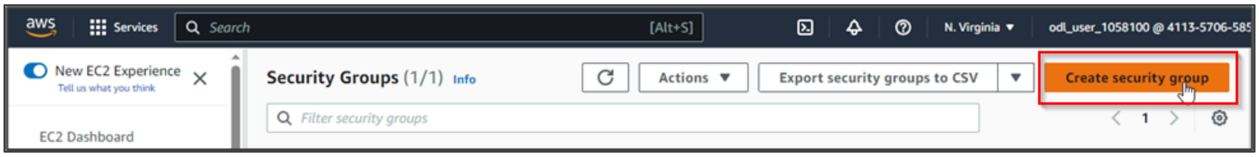
1.1 Navigate to the AWS Management Console, select **EC2** from the recently visited services



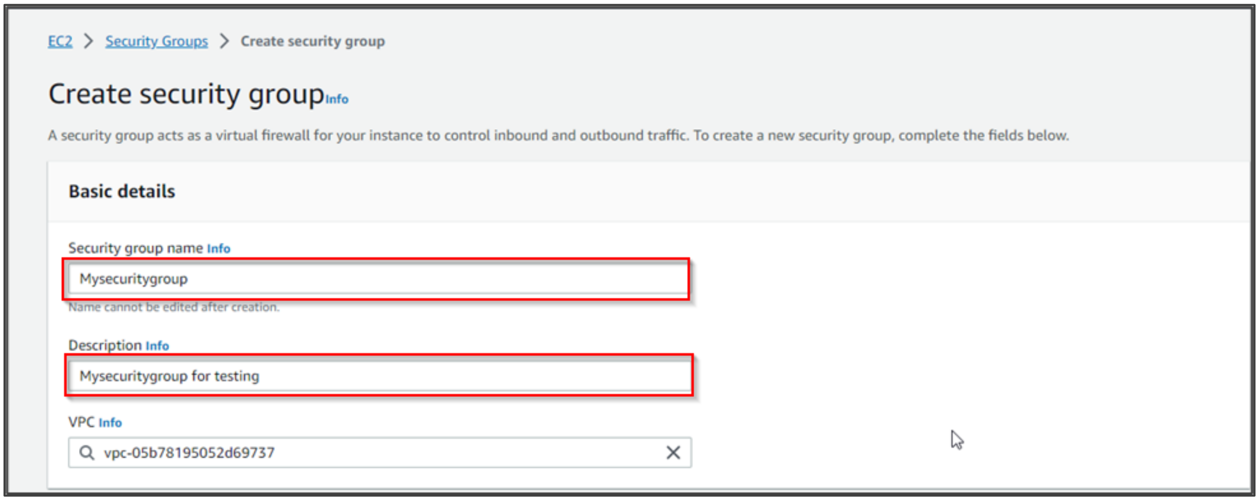
1.2 In the EC2 dashboard, click on **Security groups**



1.3 Click on **Create security group**



1.4 Provide the name and the description for the security group



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

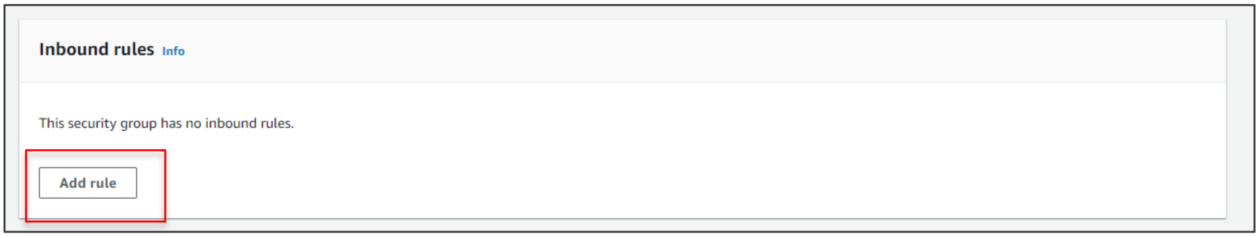
Security group name Info: Mysecuritygroup

Name cannot be edited after creation.

Description Info: Mysecuritygroup for testing

VPC Info: vpc-05b78195052d69737

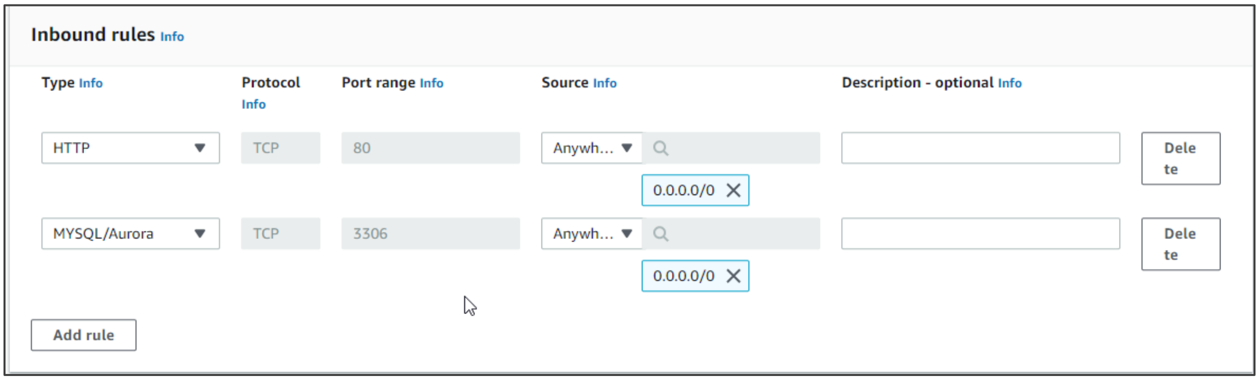
1.5 Scroll down to Inbound rules and click on **Add rule**



Inbound rules Info

This security group has no inbound rules.

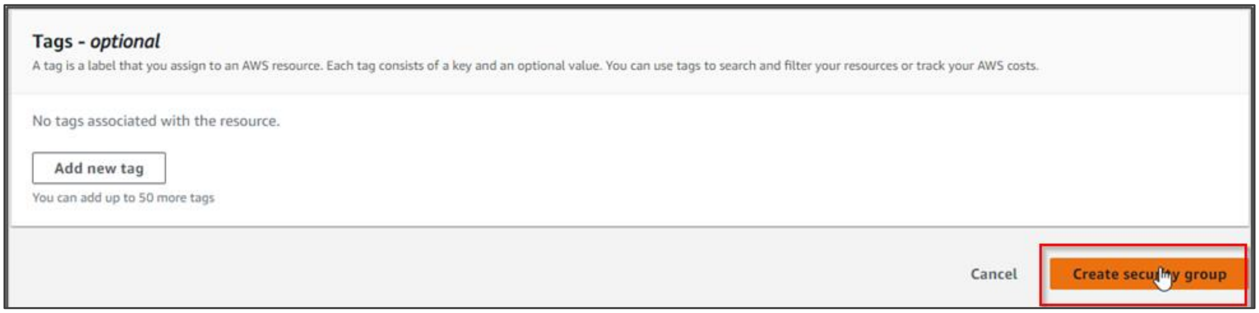
1.6 Add the Inbound rules as shown below



Inbound rules Info

Type Info	Protocol Info	Port range Info	Source Info	Description - optional Info	
HTTP	TCP	80	Anywh... 0.0.0.0/0		Delete
MYSQL/Aurora	TCP	3306	Anywh... 0.0.0.0/0		Delete

1.7 Click on **Create security group**



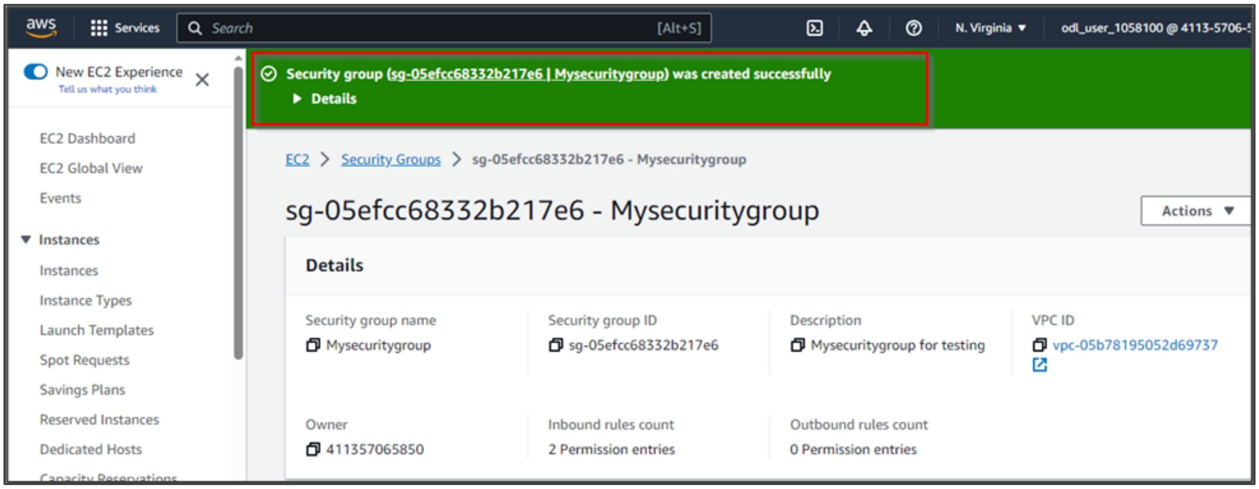
Tags - *optional*

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

No tags associated with the resource.

You can add up to 50 more tags

The security group is created successfully.



Security group (sg-05efcc68332b217e6 | Mysecuritygroup) was created successfully

EC2 > Security Groups > sg-05efcc68332b217e6 - Mysecuritygroup

sg-05efcc68332b217e6 - Mysecuritygroup

Details

Security group name: Mysecuritygroup

Security group ID: sg-05efcc68332b217e6

Description: Mysecuritygroup for testing

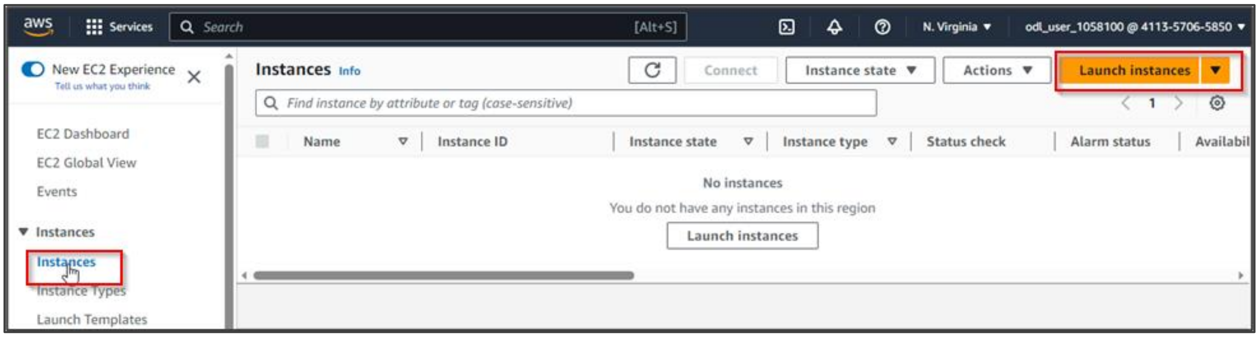
VPC ID: vpc-05b78195052d69737

Owner: 411357065850

Inbound rules count: 2 Permission entries

Outbound rules count: 0 Permission entries

1.8 Navigate to the EC2 dashboard, select **Instances**, and then click on **Launch instances**



Instances Info

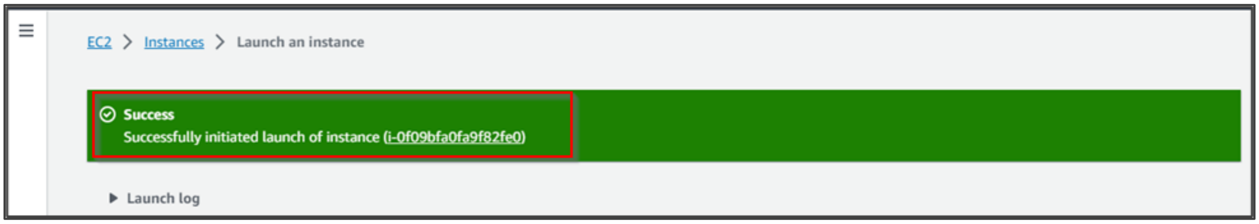
Find instance by attribute or tag (case-sensitive)

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availabil

No instances

You do not have any instances in this region

Note: Please refer to **Lesson 07 Demo 03_Creating_and_Changing_AWS_Security_Groups** to launch an EC2 instance.



EC2 > Instances > Launch an instance

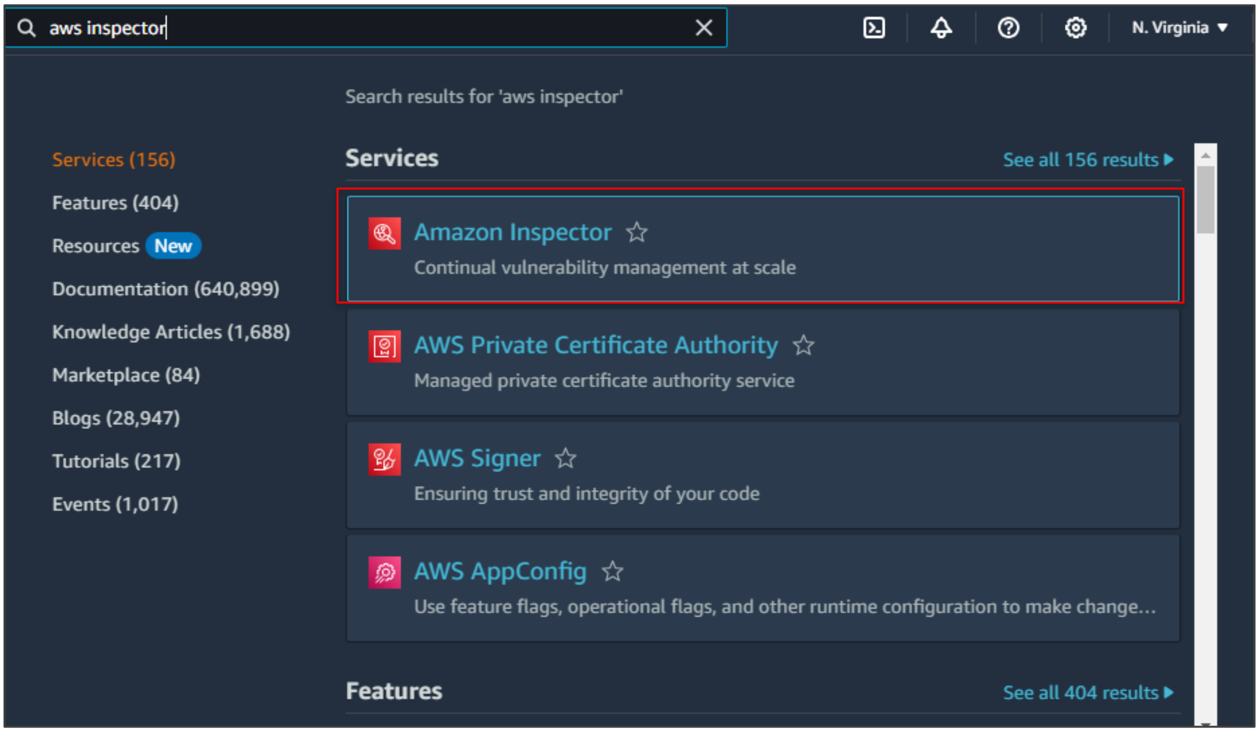
Success
Successfully initiated launch of instance (i-0f09bfa0fa9f82fe0)

Launch log

The instance is created successfully.

Step 2: Configure the AWS Inspector

2.1 Search for and select **Amazon Inspector** from the Services and click on **Get Started**



aws inspector

N. Virginia

Search results for 'aws inspector'

Services (156)
Features (404)
Resources New
Documentation (640,899)
Knowledge Articles (1,688)
Marketplace (84)
Blogs (28,947)
Tutorials (217)
Events (1,017)

Services — See all 156 results

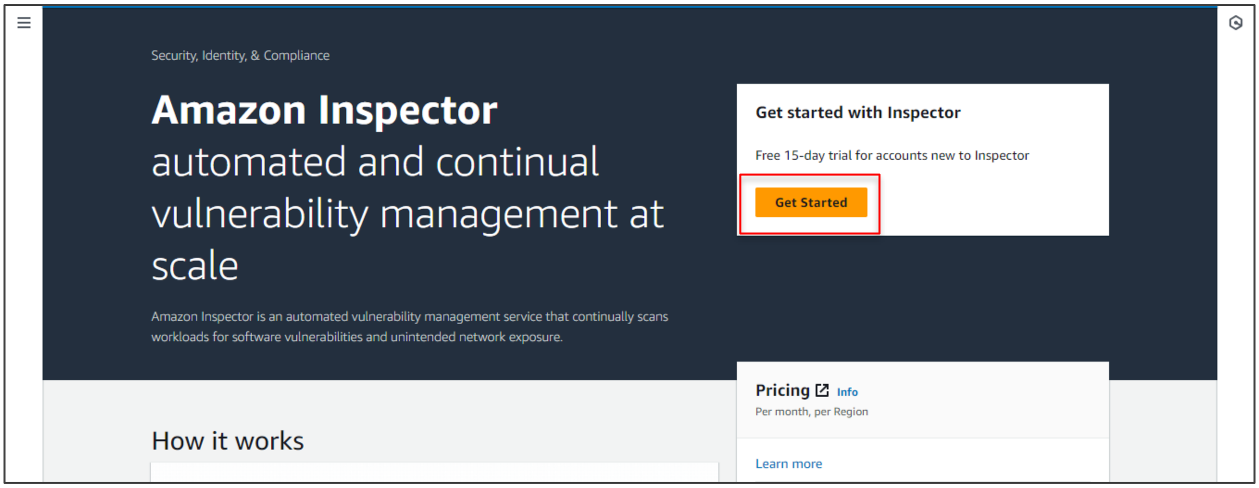
Amazon Inspector
Continual vulnerability management at scale

AWS Private Certificate Authority
Managed private certificate authority service

AWS Signer
Ensuring trust and integrity of your code

AWS AppConfig
Use feature flags, operational flags, and other runtime configuration to make change...

Features — See all 404 results



Security, Identity, & Compliance

Amazon Inspector
automated and continual vulnerability management at scale

Amazon Inspector is an automated vulnerability management service that continually scans workloads for software vulnerabilities and unintended network exposure.

Get started with Inspector

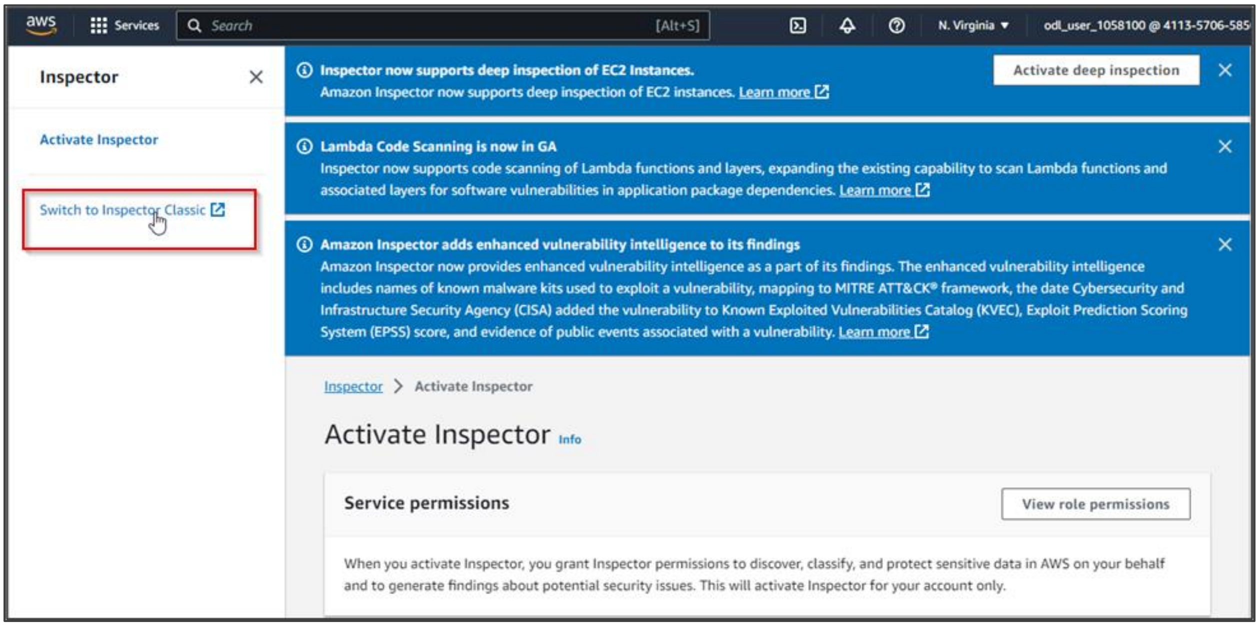
Free 15-day trial for accounts new to Inspector

Pricing Info

Per month, per Region

How it works

2.2 In the Inspector dashboard, select **Switch to Inspector Classic** from the left pane, and then click on **Help me create an Assessment**



Inspector now supports deep inspection of EC2 Instances.
Amazon Inspector now supports deep inspection of EC2 instances. Learn more

Lambda Code Scanning is now in GA
Inspector now supports code scanning of Lambda functions and layers, expanding the existing capability to scan Lambda functions and associated layers for software vulnerabilities in application package dependencies. Learn more

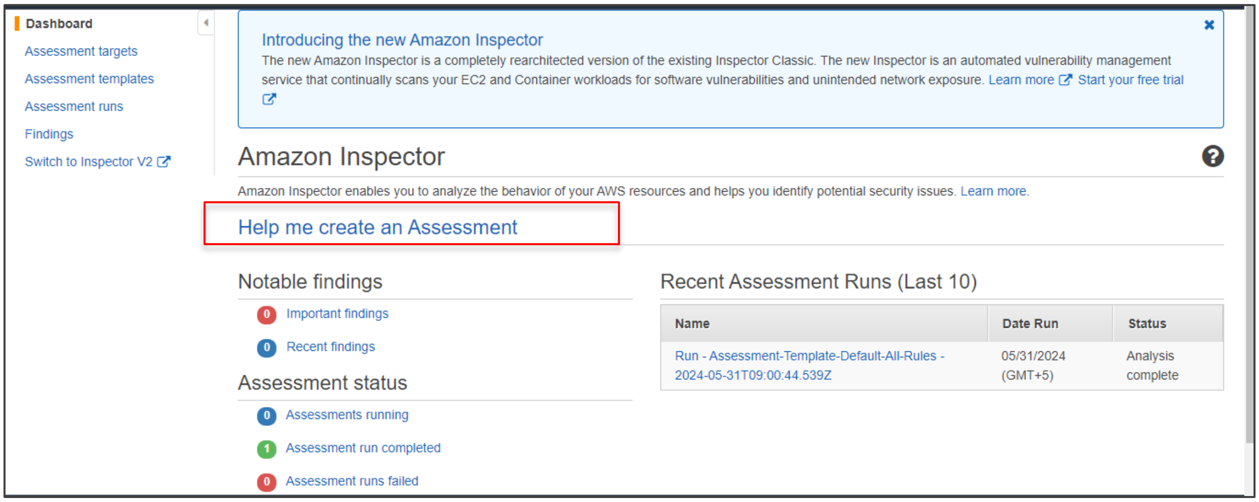
Amazon Inspector adds enhanced vulnerability intelligence to its findings
Amazon Inspector now provides enhanced vulnerability intelligence as a part of its findings. The enhanced vulnerability intelligence includes names of known malware kits used to exploit a vulnerability, mapping to MITRE ATT&CK® framework, the date Cybersecurity and Infrastructure Security Agency (CISA) added the vulnerability to Known Exploited Vulnerabilities Catalog (KVEC), Exploit Prediction Scoring System (EPSS) score, and evidence of public events associated with a vulnerability. Learn more

Inspector > Activate Inspector

Activate Inspector Info

Service 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.



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

Amazon Inspector enables you to analyze the behavior of your AWS resources and helps you identify potential security issues. Learn more.

Help me create an Assessment

Notable findings

- 0 Important findings
- 0 Recent findings

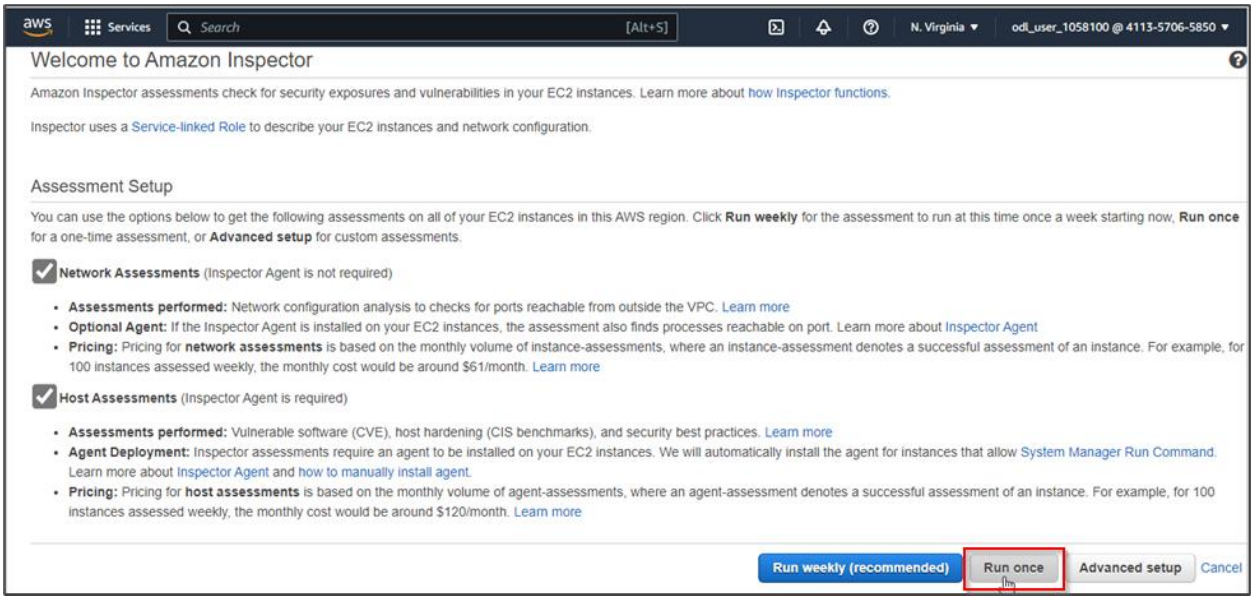
Assessment status

- 0 Assessments running
- 1 Assessment run completed
- 0 Assessment runs failed

Recent Assessment Runs (Last 10)

Name	Date Run	Status
Run - Assessment-Template-Default-All-Rules - 2024-05-31T09:00:44.539Z	05/31/2024 (GMT+5)	Analysis complete

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



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.

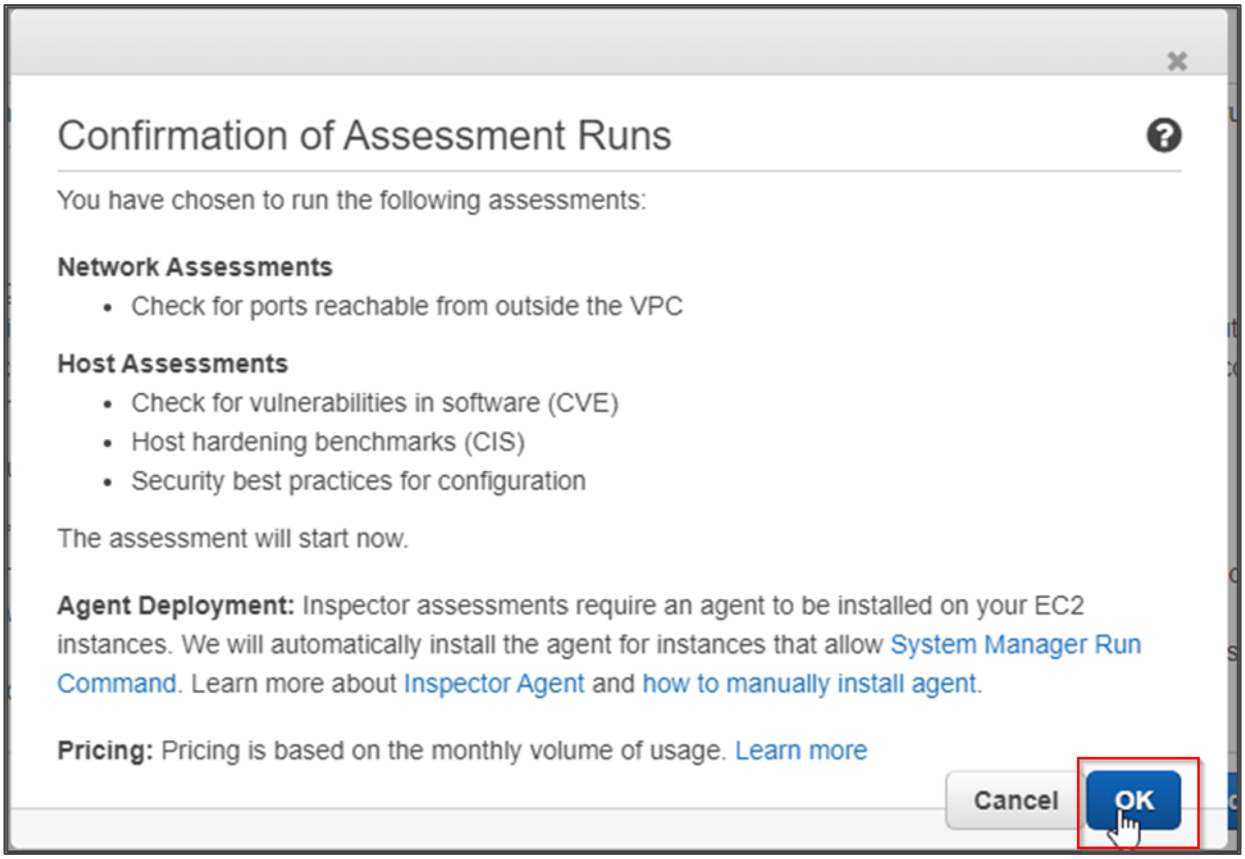
☑ **Network Assessments** (Inspector Agent is not required)

- **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 of an instance. 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

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



Confirmation of Assessment Runs

You have chosen to run the following assessments:

Network Assessments

- Check for ports reachable from outside the VPC

Host Assessments

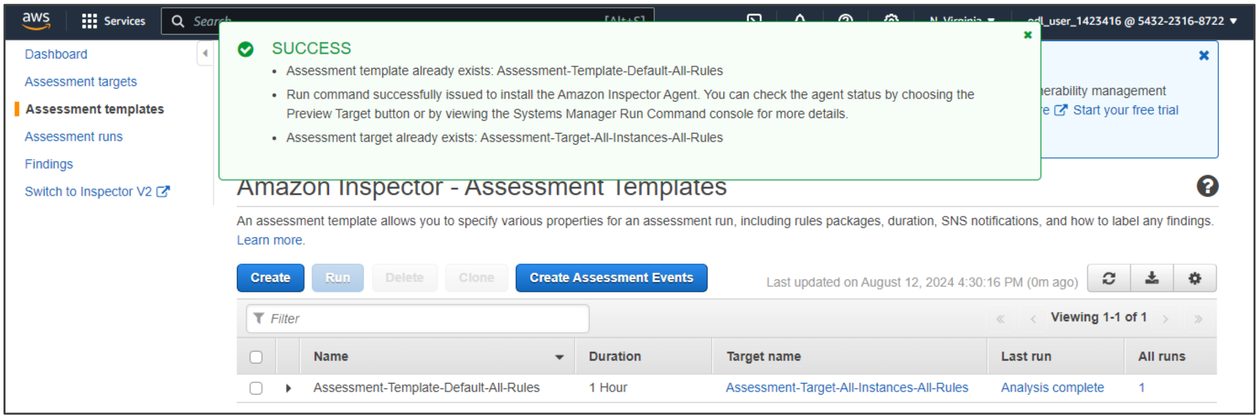
- Check for vulnerabilities in software (CVE)
- Host hardening benchmarks (CIS)
- Security best practices for configuration

The assessment will start now.

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 is based on the monthly volume of usage. Learn more

The setup for Amazon Inspector is completed.



SUCCESS

- Assessment template already exists: Assessment-Template-Default-All-Rules
- Run command successfully issued to install the Amazon Inspector Agent. You can check the agent status by choosing the Preview Target button or by viewing the Systems Manager Run Command console for more details.
- Assessment target already exists: Assessment-Target-All-Instances-All-Rules

Amazon Inspector - Assessment Templates

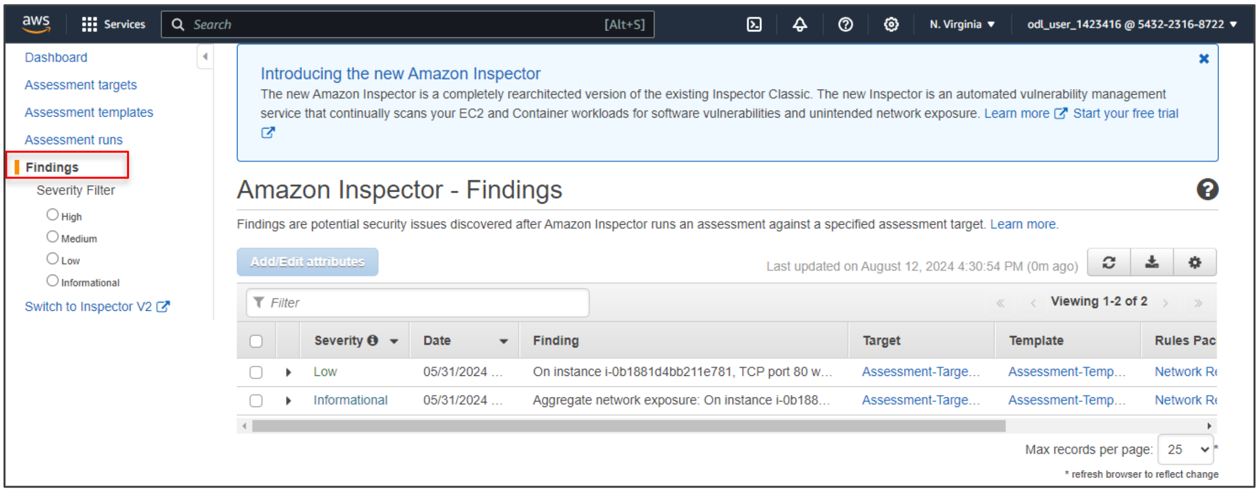
An assessment template allows you to specify various properties for an assessment run, including rules packages, duration, SNS notifications, and how to label any findings. Learn more.

Last updated on August 12, 2024 4:30:16 PM (0m ago)

Viewing 1-1 of 1

□		Name	Duration	Target name	Last run	All runs
□	▸	Assessment-Template-Default-All-Rules	1 Hour	Assessment-Target-All-Instances-All-Rules	Analysis complete	1

2.5 Select **Findings** from the left navigation pane in the Inspector dashboard to view the severity in the Inspector



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.

Last updated on August 12, 2024 4:30:54 PM (0m ago)

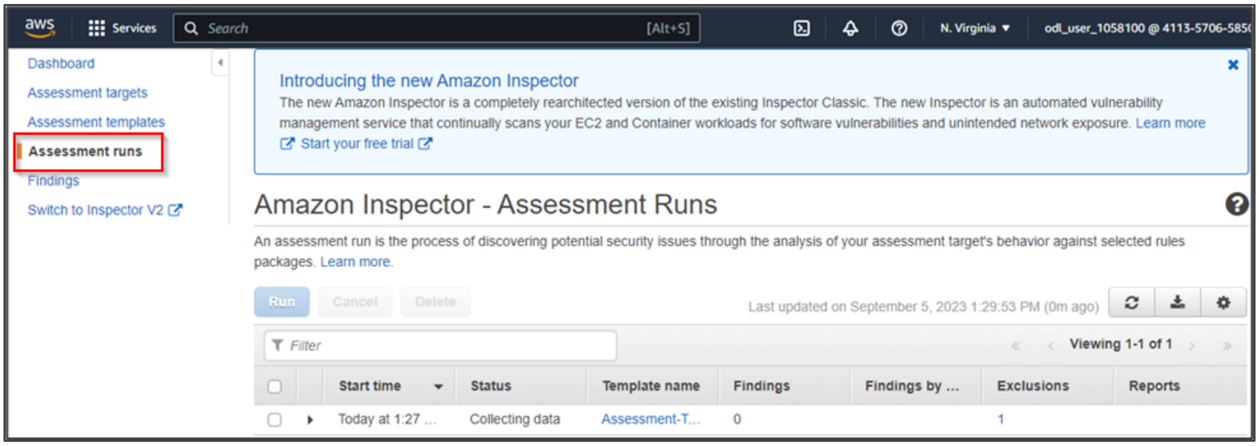
Viewing 1-2 of 2

	Severity	Date	Finding	Target	Template	Rules Pac
□	Low	05/31/2024 ...	On instance i-0b1881d4bb211e781, TCP port 80 w...	Assessment-Targe...	Assessment-Temp...	Network Ru
□	Informational	05/31/2024 ...	Aggregate network exposure: On instance i-0b188...	Assessment-Targe...	Assessment-Temp...	Network Ru

Max records per page: 25 *

* refresh browser to reflect change

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



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.

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

Viewing 1-1 of 1

	Start time	Status	Template name	Findings	Findings by ...	Exclusions	Reports
□	Today at 1:27 ...	Collecting data	Assessment-T...	0		1	

By following these steps, you have successfully configured AWS Inspector to enhance the security and compliance of the AWS environment.