

## AWS INSPECTOR

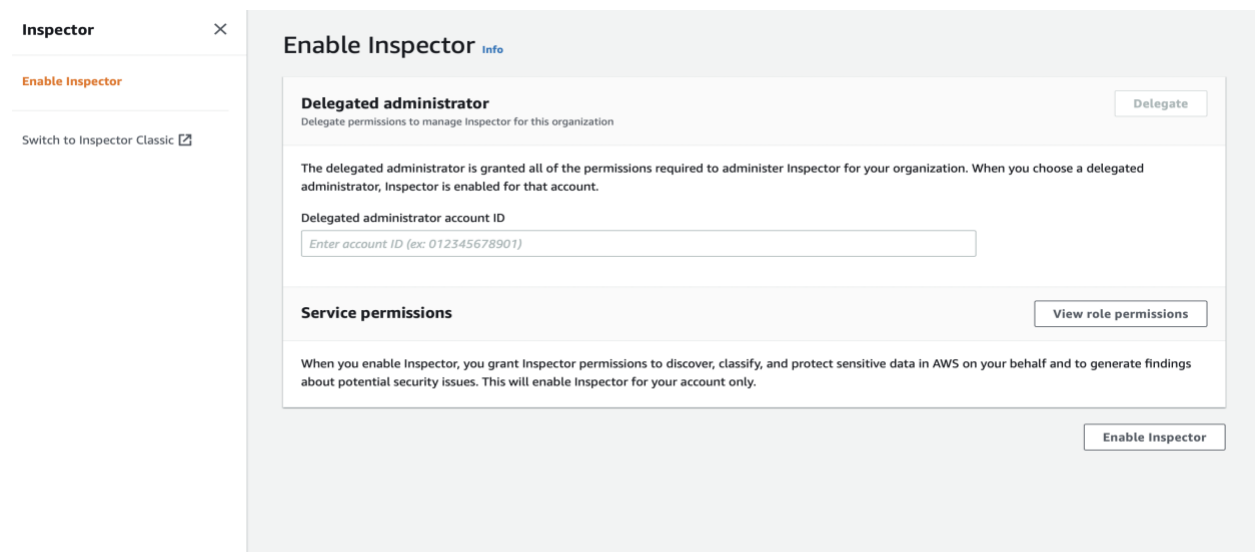
Amazon Inspector is an **automated security assessment service that helps improve the security and compliance of applications deployed on AWS**. Amazon Inspector automatically assesses applications for exposure, vulnerabilities, and deviations from best practices.

Amazon Inspector Classic tests the network accessibility of your Amazon EC2 instances and the security state of your applications that run on those instances. Amazon Inspector Classic assesses applications for exposure, vulnerabilities, and deviations from best practices. After performing an assessment, Amazon Inspector Classic produces a detailed list of security findings that is organized by level of severity.

It will create based on region, so we need have an EC2 instance i.e here I am taking in Virginia. Once EC2 instance created in the region.

Now Inspector has 2 options:

- 1) Enable through account ID (IAM user), it will take care of everything automatically just need to enable whatever it comes under that account it will monitor. If you want the check the rule View role Permission.



The screenshot shows the AWS IAM console interface for enabling Amazon Inspector. On the left, a sidebar contains the 'Inspector' header, a close button, and two links: 'Enable Inspector' (highlighted in orange) and 'Switch to Inspector Classic' (with an external link icon). The main content area is titled 'Enable Inspector' with an 'Info' link. It features three sections: 1) 'Delegated administrator' with a 'Delegate' button and explanatory text about permissions; 2) 'Delegated administrator account ID' with a text input field containing the placeholder 'Enter account ID (ex: 012345678901)'; 3) 'Service permissions' with a 'View role permissions' button and explanatory text about the permissions granted. At the bottom right, there is an 'Enable Inspector' button.

- 2) **Inspector classic** where we need to provide rules and template and there is check mark to all the Ec2 instances in region and to install Amazon Inspector Agent on all EC2 options.

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-All-Instances

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

Cancel

Next

Get started with Amazon Inspector

- Step 1: Define an assessment target
- Step 2: Define an assessment template
- Step 3: Review

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\*

Network Reachability-1.1

Security Best Practices-1.0

Common Vulnerabilities and Exposures-1.1

CIS Operating System Security Configuration Benchmarks-1.0

×

×

×

×

Amazon Inspector runs assessments for the assessment target against selected rules package(s). [Learn more.](#)

Duration\*

15 Minutes

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](#)

\*Required

Cancel

Previous

Next

- Dashboard
- Assessment targets
- Assessment templates
- Assessment runs
- Findings

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.](#)

Create

Run

Delete

Clone

Create Assessment Events

Last updated on December 29, 2021 12:58:53 PM (0m ago)

↺

↻

⬇

⚙

Filter

Viewing 1-1 of 1

<input type="checkbox"/>	Name	Duration	Target name	Last run	All runs
<input type="checkbox"/>	▶ Assessment-Template-Default	15 Minutes	Assessment-Target-All-Instances	Collecting data	1

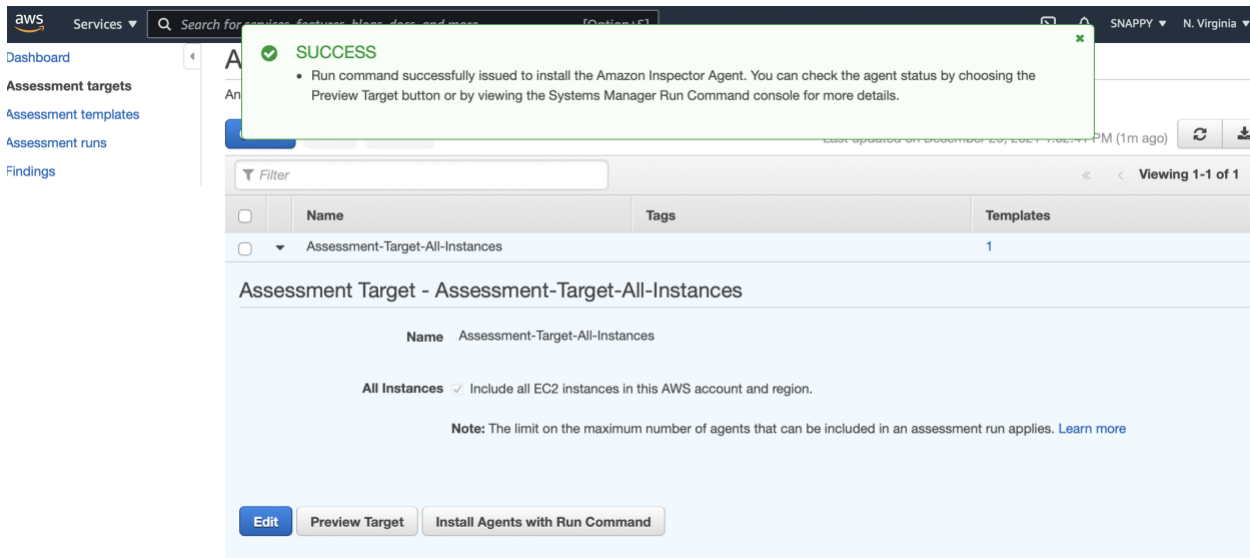
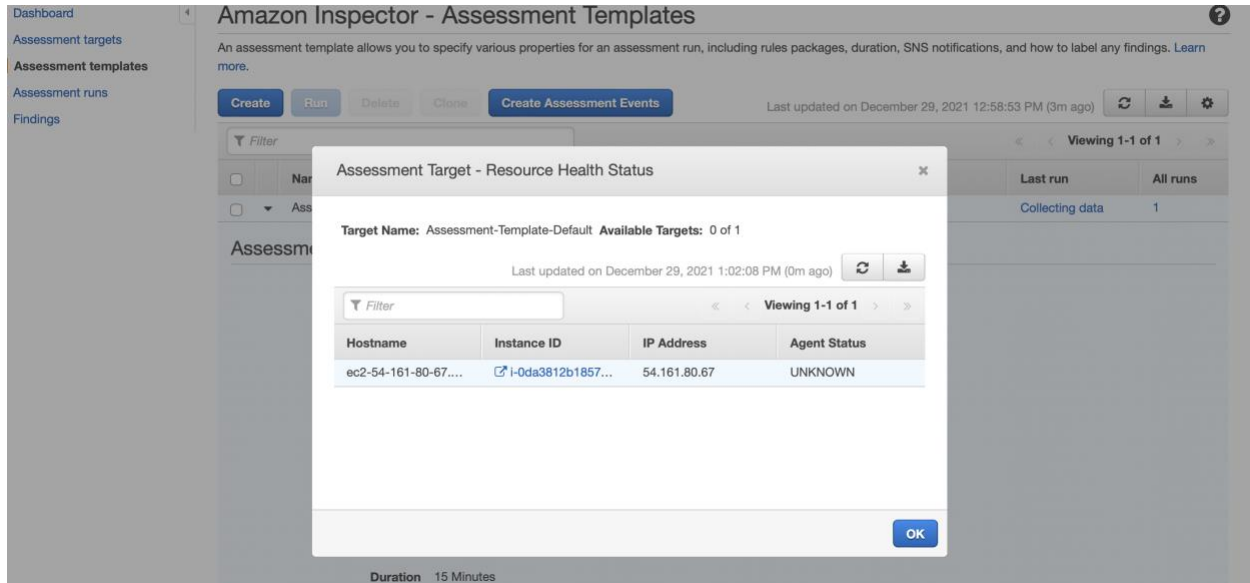
Max records per page:

25

\*

\* refresh browser to reflect change

- 3) Check the agent status if it is unknown for 5 mins then go to Assessment targets and install agent with run command. Run the templates if you want see the results or else it will run based on run time configurations.



- 4) As you can see below SS we can go finding and check for Severity based on that we can go fix the problems.

Dashboard
Assessment targets
Assessment templates
Assessment runs
Findings

## 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 December 29, 2021 1:12:32 PM (0m ago)

Filter

	Start time	Status	Template name	Findings	Findings by sev...	Exclusions	Reports
	Today at 1:04 PM...	Analysis complete	Assessment-Tem...	3	High   Medium   L...	1	Download report
	Today at 12:58 P...	Analysis complete	Assessment-Tem...	3	High   Medium   L...	1	Download report

Max records per page: 25

\* refresh browser to reflect change

Dashboard
Assessment targets
Assessment templates
Assessment runs
Findings

## 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 December 29, 2021 1:13:06 PM (0m ago)

Filter

Severity Filter

- High
- Medium
- Low
- Informational

	Severity	Date	Finding	Target	Template	Rules Package
	Medium	Today at 1:0...	On instance i-0da3812b1857c4c48, TCP port 22 ...	Assessment-Targe...	Assessment-Temp...	Network Reachability-
	Medium	Today at 1:0...	On instance i-0da3812b1857c4c48, TCP port 22 ...	Assessment-Targe...	Assessment-Temp...	Network Reachability-
	Low	Today at 1:0...	On instance i-0da3812b1857c4c48, TCP port 80 ...	Assessment-Targe...	Assessment-Temp...	Network Reachability-
	Low	Today at 1:0...	On instance i-0da3812b1857c4c48, TCP port 80 ...	Assessment-Targe...	Assessment-Temp...	Network Reachability-
	Informational	Today at 1:0...	Aggregate network exposure: On instance i-0da38...	Assessment-Targe...	Assessment-Temp...	Network Reachability-
	Informational	Today at 1:0...	Aggregate network exposure: On instance i-0da38...	Assessment-Targe...	Assessment-Temp...	Network Reachability-

Max records per page: 25

\* refresh browser to reflect change

5) We can find all the information in the Dashboard.

Dashboard
Assessment targets
Assessment templates
Assessment runs
Findings

## 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
- 6 Recent findings

Assessment status

- 0 Assessments running
- 2 Assessment runs completed
- 0 Assessment runs failed

Account settings
[Manage Amazon Inspector Service-Linked Role](#)

Recent Assessment Runs (Last 10)

Name	Date Run	Status
Run - Assessment-Template-Default - 2021-12-29T18:04:21.984Z	Today at 1:04 PM (GMT-5)	Analysis complete
Run - Assessment-Template-Default - 2021-12-29T17:58:51.650Z	Today at 12:58 PM (GMT-5)	Analysis complete