Overview

1. What is an Amazon Inspector?
    - Amazon Inspector is an **automated security assessment service**
    - Amazon Inspector tests the **network accessibility of your Amazon EC2 instances and the security state of your applications that run on those instances**.

2. What does Amazon Inspector do?
    a. Analyze the behavior of your AWS resources
    b. Test network accessibility and security state
    c. helps **improve the security and compliance of applications deployed on AWS.** It assesses applications for:
        - Exposure
        - Vulnerabilities
        - Deviations from best practices

    This allows you to do the **security assessment against your infrastructure**

3. What is the severity of a finding?
    After performing an assessment, Amazon Inspector produces a **detailed list of security findings that is organized by level of severity.**

4. Is Amazon Inspector a HIPAA eligible service? YES

Let's say your security teams wants to know which processes are running on open port

Create an Assessment

Amazon inspector assessments check for security exposure and vulnerabilities in your EC2 instances.

1. Network assessment (Inspector agent **is not required**) :
    Assessment performed: Network configuration analysis to checks for ports reachable from outside the VPC

2. Host assessment (**Inspector agent is REQUIRED**) :
    Assessment performed: Vulnerability software, Host hardening (CIS Benchmark), and security best practices

You can create assessment to run weekly (Recommended) or Run once

Key Concepts for Inspector

1. What is an assessment template?

An assessment template is a configuration that you create in Amazon Inspector to define your assessment run.
This assessment template includes a rules package against which you want Amazon Inspector to evaluate your assessment target, the duration of the assessment run, Amazon Simple Notification Service (SNS) topics to which you want Amazon Inspector to send notifications about assessment run states and findings, and Amazon Inspector-specific attributes (key/value pairs) that you can assign to findings generated by the assessment run.

2. What is an assessment run?

An assessment run is the process of discovering potential security issues through the analysis of your assessment target's configuration, installed software, and behavior against specified rule packages.
If the network reachability rules package is included, Inspector analyzes your network configurations in AWS to find accessibility of your EC2 instances over the network.
If the Inspector agent is installed on the instance, the agent collects and sends on-host software and configuration data.
Next, the Inspector service analyzes the data and compares it against the rule packages specified.
A completed assessment run produces a list of findings for potential security issues.

3. What is an assessment target?

An assessment target represents a collection of Amazon EC2 instances that you want assessed, typically a set of instances that work together as a unit to help you accomplish your business goal(s).
Amazon Inspector evaluates the security state of these EC2 instances.
You can include all of your instances in an assessment target or specify a subset of instances by using Amazon EC2 tags.

3.What is a rules package?

Types of checks you want to run. What security vulnerability or exposure that I want to run to check.

4. Inspector Agent:

To gather data from all of your EC2 instance to analyze and determine what vulnerability they have

5. Triggers and Run:

Inspectors can be set up on a recurrence schedule. This can run on a schedule for you

6. Findings and Reports:

This produce our findings in reports

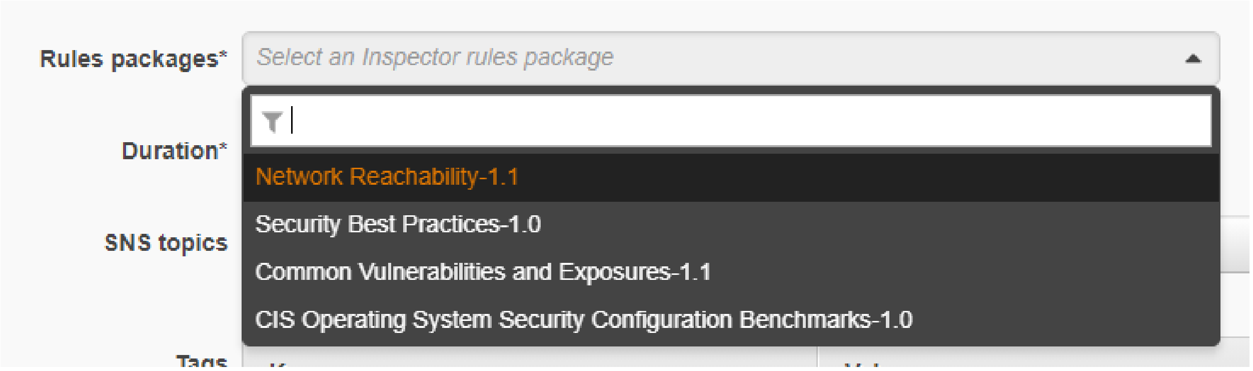
Inspector Rules Packages:

Amazon Inspector has two types of rules packages:

- **Network reachability rules package** that checks for network accessibility of your Amazon EC2 instances
- **Host assessment rules packages** that check for vulnerabilities and insecure configurations on the Amazon EC2 instance.

Host assessment rules packages include:

- Common Vulnerabilities and Exposures (CVE)
  - Are my instances exposed to the latest vulnerabilities?
- Center for Internet Security (CIS) Operating System configuration benchmarks
  - Are my instances hardened for security?
- Security best practices.
  - Are my password policies in line with best practices?
  - Does my application use insecure protocols?



Rules packages* Select an Inspector rules package

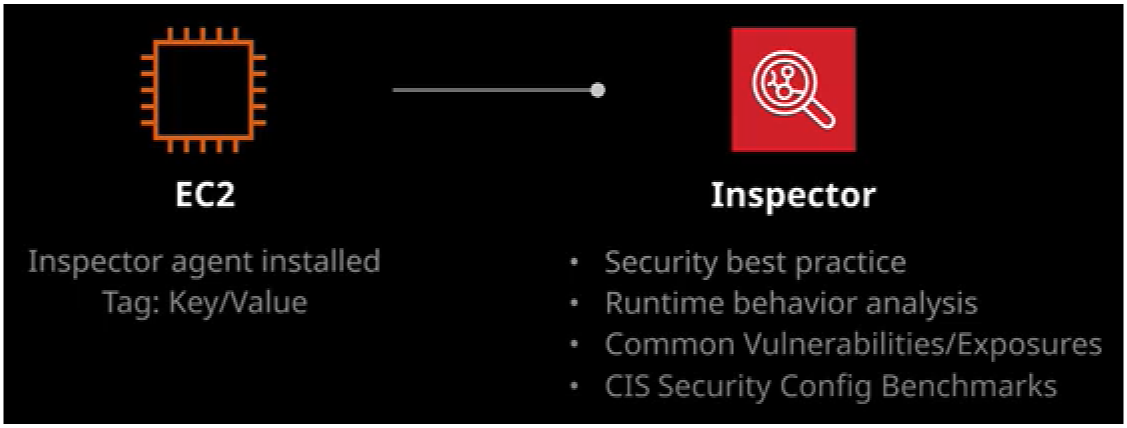
Network Reachability-1.1

Security Best Practices-1.0

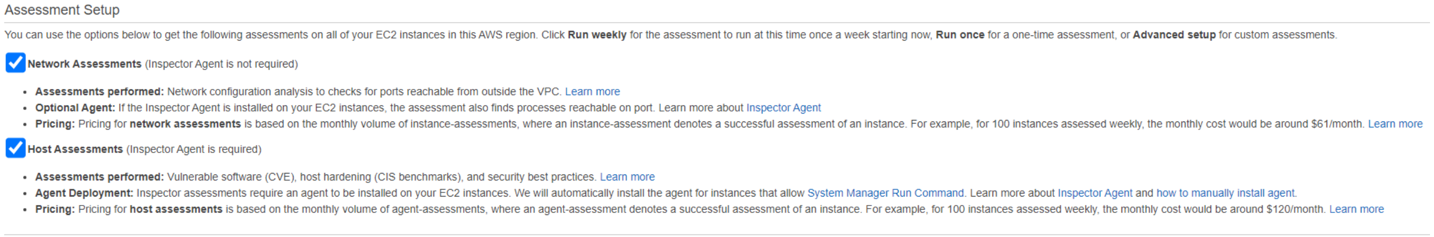
Common Vulnerabilities and Exposures-1.1

CIS Operating System Security Configuration Benchmarks-1.0

Can I define my own rules for assessment templates? No. Only the pre-defined rules are currently allowed for assessment runs.



EC2
Inspector agent installed
Tag: Key/Value
Inspector
• Security best practice
• Runtime behavior analysis
• Common Vulnerabilities/Exposures
• CIS Security Config Benchmarks



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

Types of Reports

Findings-Report : High level report that contains an executive summary of the findings from the scan. In other words this gives a basic report

Full-Report: Detailed Report that is perfect for IT and InfoSec team

Is Amazon Inspector a HIPAA eligible service? YES

Read: https://aws.amazon.com/inspector/faqs/