Deploy and configure AWS inspector to scan instances

Amazon Inspector

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

**Amazon Inspector agent**

A software agent that you can install on the EC2 instances that are included in the assessment target. The agent collects a wide set of configuration data (telemetry). For more information, see [Amazon Inspector agents](https://docs.aws.amazon.com/inspector/latest/userguide/inspector_agents.html).

**Assessment run**

The process of discovering potential security issues through the analysis of your assessment target's configuration against specified rules packages. During an assessment run, Amazon Inspector monitors, collects, and analyzes configuration data (telemetry) from resources within the specified target. Next, Amazon Inspector analyzes the data and compares it against a set of security rules packages that are specified in the assessment template used during the assessment run. A completed assessment run produces a list of findings, which are potential security issues of various levels of severity. For more information, see [Amazon Inspector assessment templates and assessment runs](https://docs.aws.amazon.com/inspector/latest/userguide/inspector_assessments.html).

**Assessment target**

In the context of Amazon Inspector, a collection of AWS resources that work together as a unit to help you accomplish your business goals. Amazon Inspector evaluates the security state of the resources that constitute the assessment target.

To create an Amazon Inspector assessment target, you must first tag your EC2 instances with key-value pairs of your choice. Next, you can create a view of these tagged EC2 instances that have common keys or common values.

**Assessment template**

A configuration that is used during your assessment run. The template includes the following:

* Rules packages that Amazon Inspector uses to evaluate your assessment target
* Amazon SNS topics that you want Amazon Inspector to send notifications to about assessment run states and findings
* Tags (key-value pairs) that you can assign to findings that are generated by the assessment run
* The duration of the assessment run

**Finding**

A potential security issue that Amazon Inspector discovers during an assessment run of the specified target. Findings are displayed in the Amazon Inspector console or retrieved through the API. They contain both a detailed description of the security issue and a recommendation on how to fix it. For more information, see [Amazon Inspector findings](https://docs.aws.amazon.com/inspector/latest/userguide/inspector_findings.html).

**Rule**

In the context of Amazon Inspector, a security check performed during an assessment run. When a rule detects a potential security issue, Amazon Inspector generates a finding that describes the issue.

**Rules package**

In the context of Amazon Inspector, a collection of rules. A rules package corresponds to a security goal that you might have. You can specify your security goal by selecting the appropriate rules package when you create an Amazon Inspector assessment template. For more information, see [Amazon Inspector rules packages and rules](https://docs.aws.amazon.com/inspector/latest/userguide/inspector_rule-packages.html).