Amazon Inspector

Everyone who uses cloud-based apps understands the need for security. When we talk about cloud security, we're talking about the technologies, policies, and services that help safeguard cloud-hosted data, apps, and infrastructure from various internet threats. Amazon Inspector is an **automated security assessment service** that automatically examines applications for exposure, vulnerabilities, and deviations from best practices. It is used to improve the security of applications deployed on Amazon Web Services.

What is Amazon Inspector?

Amazon Inspector is an automated security assessment service and to test network accessibility of EC2 instance. It helps you to identify vulnerabilities within your EC2 instances and applications. And allows you to make security testing more regular occurrence as part of the development and IT operations.

Amazon Inspector provides a clear list of security and compliance findings assigned a priority by the severity level. Moreover, these findings can be analysed directly or as part of comprehensive assessment records available via the API or AWS Inspector console. AWS Inspector security assessments help you check for unintended network accessibility of EC2 instances and vulnerabilities on those EC2 instances.

Benefits of AWS Inspector

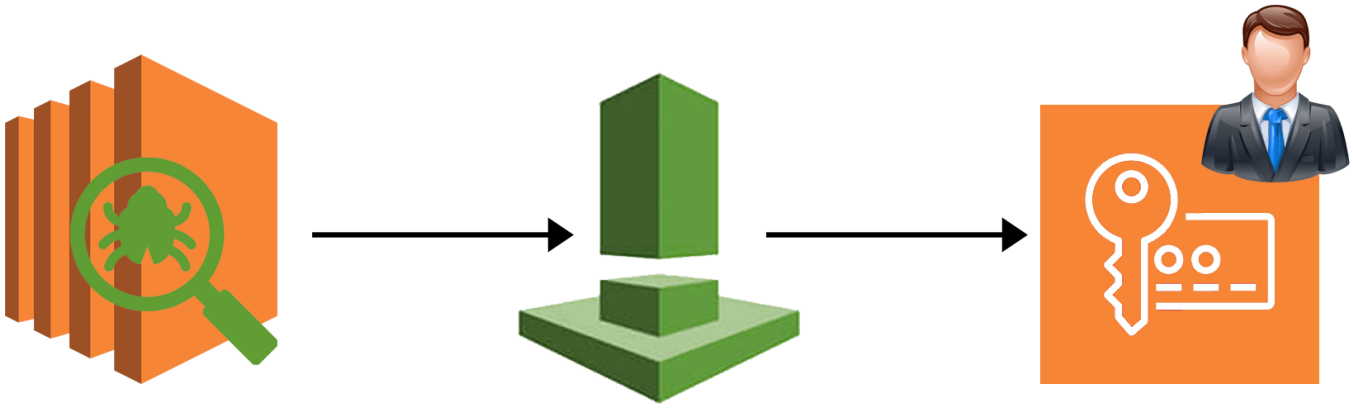
Amazon inspector is a safe and reliable service we can use for security purpose in our services, deployed applications etc. It's an automated and managed service. Let's see some key benefits of AWS Inspector.

- **Automated Service:** AWS Inspector is a beneficial service for the application's security in the AWS cloud. It can fix automatically without the interaction of human resources.
- **Regular Security Monitoring:** Amazon Inspector helps to find security vulnerabilities in applications, as well as departures from security best practices, both before they've been deployed or running in production. This improves the overall security of your AWS-hosted applications.
- **Leverage Aws Security Expertise:** AWS Inspector includes a knowledge base of numbers of rules charted to common security best practices and vulnerability definitions. It uses AWS's Security Expertise, where AWS is constantly updating the security best practices and rules, so one gets the best of both worlds.
- **Integrate Security Into DevOps:** AWS Inspector is an API-bound service that analyzes network configurations in your AWS account. Moreover, it uses an optional agent for visibility into EC2 instances. The agent makes it easy to build Inspector assessments right into your existing DevOps process and empowering both development and operations teams to make security assessments an essential part of the deployment process.

How Amazon Inspector Works?

Amazon Inspector performs an automatic assessment and generates a findings report containing steps to keep the environment safe. To use this service, you need to define the collection of AWS all the resources that complete the application to proceed and tested. It is followed by adding and

performing the security practices. You can also set the duration of that assessment which can vary from 15 Min to 12 Hrs or last for one day.



An Inspector Agent runs on the EC2 machines hosting the application that monitors the network, file system, and process activity. After collecting all the required data, it is compared with the built-in security rules to identify security or compliance issues.

Read: SDLC Automation: Everything You Need To Know

Getting Started With Amazon Inspector

AWS Inspector is a security service that helps to monitor and improve the security and compliance of web applications running inside AWS. So in this guide, we have a production EC2 instance for which we need to perform a network accessibility check.

We will set up an EC2 instance to use with Amazon Inspector and induce a security thread, and we will open port 21 on EC2. Port 21 is generally not recommended to keep open on your instances. Follow the steps mentioned below.