Amazon Inspector

Amazon Inspector is an automated security assessment service to test the network accessibility of EC2 instances. 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 analyzed 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 purposes 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 the number 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 empowers both development and operations teams to make security assessments an essential part of the deployment process.

- **Network reachability price package regulations**: Assessments performed by Amazon Inspector Classic that include network reachability rules are priced per instance per assessment (instance assessment) per month. One instance assessment is one that you perform against one instance. Ten instance assessments will result from doing one assessment against ten instances. With bulk reductions, pricing can be lowered to $0.04 per instance assessment per month from the starting price of $0.15 per instance assessment per month.
- **Package prices for host assessment rules:** The host assessment rules packages for Amazon Inspector Classic employ an agent that is deployed on the Amazon EC2 Instances running the apps you want to evaluate. Each month, host rules assessments (sometimes known as “agent assessments”) are charged per agent. A single-agent assessment is one that is performed against a single agent. Ten agent assessments will result from running one assessment against ten agents.

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 and all the resources that complete the application to proceed and tested. It is followed by adding and performing 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.