Malware Protection in Amazon Inspector

**Contents**

[Scope 2](#_Toc115190395)

[Problem Statement 2](#_Toc115190396)

[Introduction 2](#_Toc115190397)

[Continuously scan your envioronment for vulnerabilities and network exposure 3](#_Toc115190408)

Assess vulnerabilities accurately with the Amazon Inspector Risk Store [3](#_Toc115190413)

[Identify high-impact findings with the Amazon Inpector dashboard 3](#_Toc115190413)

[Manage your findings using customizable views 3](#_Toc115190413)

[Monitor and process findings with other services and systems 4](#_Toc115190413)

[Scanning Amazon EC2 instances with amazon Inspector 5](#_Toc115190413)

[Implementation 6](#_Toc115190402)

[Enable Amazon Inspector 6](#_Toc115190403)

[View the Findings 7](#_Toc115190405)

[Export findings to S3 8](#_Toc115190412)

[Services Protected by Amazon Inspector 10](#_Toc115190396)

[How Inspector Protects EC2? 10](#_Toc115190412)

[How Inspector Protects ECR? 11](#_Toc115190412)

[Benefits 12](#_Toc115190413)

[Limitations 12](#_Toc115190413)

**Malware Protection in** **Amazon Inspector**

Document Name: Malware Protection in Amazon Inspector

Owner: Hema Paul

**Scope**

When vulnerabilities or open network paths are identified, Amazon Inspector produces a [*finding*](https://docs.aws.amazon.com/inspector/latest/user/findings-understanding.html)that you can investigate. The finding includes comprehensive details about the vulnerability, the impacted resource, and remediation recommendations. If you appropriately remediate a finding, Amazon Inspector automatically detects the remediation and closes the finding.

**Problem Statement**

In Amazon Inspector, a finding is a detailed report about a potential vulnerability that affects one of your resources. Amazon Inspector generates a finding whenever it detects a potential vulnerability for an Amazon EC2 instance or a potential software vulnerability in a container image within an Amazon ECR repository. Each finding is titled according to the detected vulnerability and provides a severity rating, information about the affected resource, and additional details, such as how to remediate the reported vulnerability.

**Introduction**

Amazon Inspector is a vulnerability management service that continually scans your Amazon EC2 instances and Amazon ECR container images for software vulnerabilities and unintended network exposure.

**Continuously scan your environment for vulnerabilities and network exposure**

With Amazon Inspector you do not need to manually schedule or configure assessment scans. Amazon Inspector automatically discovers and begins [*scanning your eligible resources*](https://docs.aws.amazon.com/inspector/latest/user/scanning-resources.html). Amazon Inspector continues to assess your environment throughout the lifecycle of your resources by automatically scanning resources whenever you make changes to them. Unlike traditional security scanning software, Amazon Inspector has minimal impact on the performance of your fleet.

**Assess vulnerabilities accurately with the Amazon Inspector Risk score**

As Amazon Inspector collects information about your environment through scans, it provides severity scores specifically tailored to your environment. Amazon Inspector examines the security metrics that compose the [National Vulnerability Database](https://nvd.nist.gov/vuln)(NVD) base score for a vulnerability and adjusts them according to your compute environment. For example, the service may lower the Amazon Inspector score of a finding for an Amazon EC2 instance if the vulnerability is exploitable over the network but no open network path to the internet is available from the instance. This score is in CVSS format and is a modification of the base [Common Vulnerability Scoring System](https://www.first.org/cvss/)(CVSS) score provided by NVD.

**Identify high-impact findings with the Amazon Inspector dashboard**

The [Amazon Inspector dashboard](https://docs.aws.amazon.com/inspector/latest/user/understanding-dashboard.html) offers a high-level view of findings from across your environment. From the dashboard, you can access the granular details of a finding. The newly redesigned dashboard contains streamlined information about scan coverage in your environment, your most critical findings, and which resources have the most findings. The risk-based remediation panel in the Amazon Inspector dashboard presents the findings that affect the largest number of instances and images. This panel makes it easier to identify the findings with the greatest impact on your environment, see findings details, and view suggested solutions.

**Manage your findings using customizable views**

In addition to the dashboard, the Amazon Inspector console offers a **Findings** view. This page lists all findings for your environment and provides the details of individual findings. You can view findings grouped by category or vulnerability type. In each view you can further customize your results using filters. You can also use filters to create suppression rules that hide unwanted findings from your views.

Any Amazon Inspector user can use filters and suppression rules to generate finding reports that show all findings or a customized selection of findings. Reports can be generated in CSV or JSON formats.

**Monitor and process findings with other services and systems**

To support integration with other services and systems, Amazon Inspector [publishes findings to Amazon EventBridge](https://docs.aws.amazon.com/inspector/latest/user/findings-managing-automating-responses.html) as finding events. EventBridge is a serverless event bus service that can route findings data to targets such as AWS Lambda functions and Amazon Simple Notification Service (Amazon SNS) topics. With EventBridge, you can monitor and process findings in near-real time as part of your existing security and compliance workflows.

If you have enabled [AWS Security Hub](https://docs.aws.amazon.com/inspector/latest/user/securityhub-integration.html), then Amazon Inspector will also [publish findings to Security Hub](https://docs.aws.amazon.com/inspector/latest/user/integrations.html#integrations-security-hub). Security Hub is a service that provides a comprehensive view of your security posture across your AWS environment and helps you check your environment against security industry standards and best practices. With Security Hub, you can more easily monitor and process your findings as part of a broader analysis of your organization's security posture in AWS.

**Note the following before you enable Amazon Inspector**:

* Amazon Inspector is a Regional service. Any of the configuration procedures that you complete in this tutorial must be repeated in each Region that you want to monitor with Amazon Inspector.
* Amazon Inspector gives you the flexibility to enable either EC2 scanning or ECR container image scanning, or both. You can manage the scanning types from the account management page within the Amazon Inspector console or using Amazon Inspector APIs.
* Amazon Inspector can provide common vulnerabilities and exposures (CVE) data for your Amazon EC2 instances only if the Amazon EC2 Systems Manager (SSM) agent is installed and enabled. This agent is preinstalled on [many Amazon EC2 instances](https://docs.aws.amazon.com/systems-manager/latest/userguide/prereqs-ssm-agent.html), but you might need to [enable it manually](https://docs.aws.amazon.com/systems-manager/latest/userguide/systems-manager-setting-up.html). Regardless of SSM agent status, all of your Amazon EC2 instances are scanned for network reachability issues.
* Any user with administrator permissions in an AWS account can enable Amazon Inspector. However, following the security best practice of least privilege, we recommend that you create an IAM user, role, or group specifically to manage Amazon Inspector with [*AmazonInspector2FullAccess*](https://docs.aws.amazon.com/inspector/latest/user/security-iam-awsmanpol.html#security-iam-awsmanpol-AmazonInspector2FullAccess).
* When you enable Amazon Inspector for the first time in any Region, it creates a service-linked role globally for your account called AWSServiceRoleForAmazonInspector2. This role includes the permissions and the trust policies that allow Amazon Inspector to collect software package details and analyze VPC configurations in order to generate vulnerability findings.

**Scanning Amazon EC2 instances with Amazon Inspector**

Amazon Inspector scans software applications installed on your EC2 instances for software vulnerabilities and network reachability issues.

Amazon Inspector initiates vulnerability scans of EC2 instances in the following situations:

* As soon as the EC2 instance is discovered by Amazon Inspector
* When you launch a new instance
* When you install new software on an existing instance (Linux only)
* When Amazon Inspector adds a new common vulnerabilities and exposures (CVE) item to its database (Linux only)

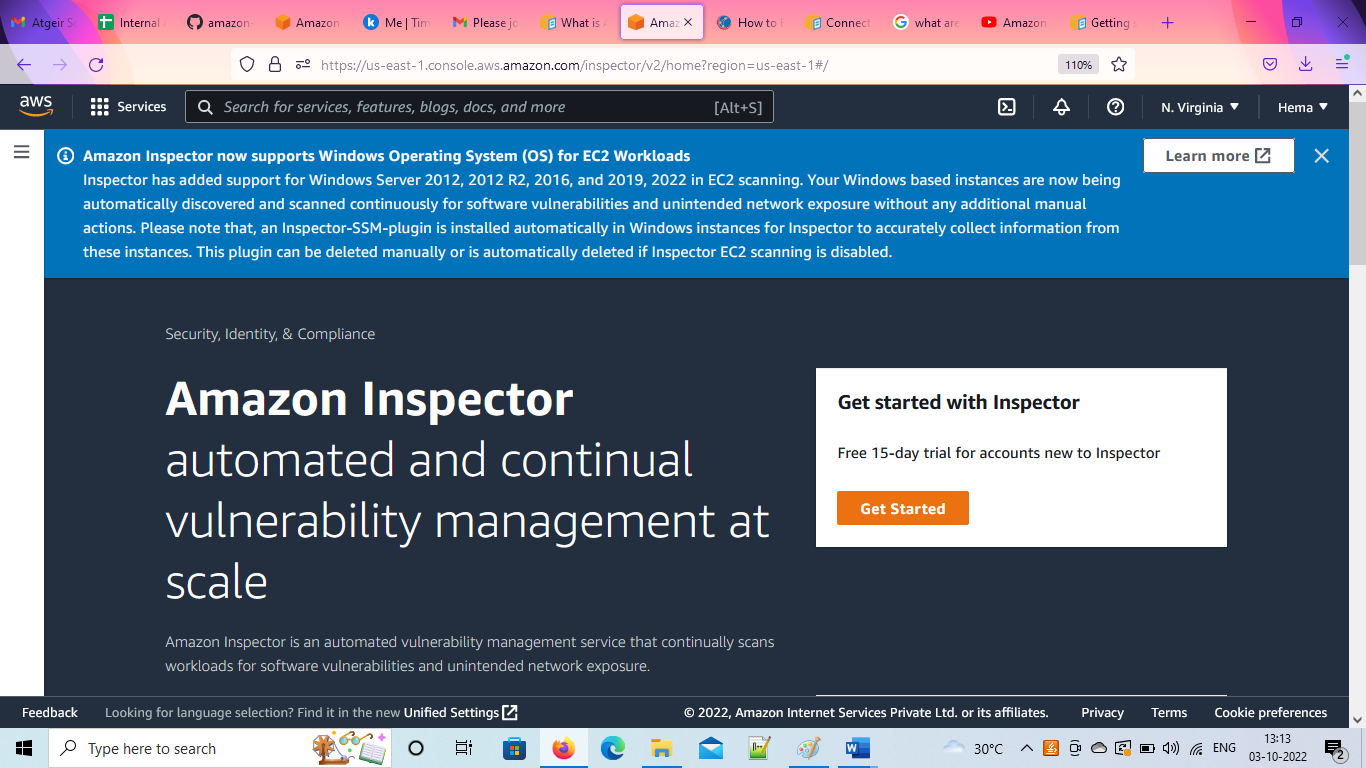
Network reachability scans for EC2 instances are performed once every 24 hours.

Amazon Inspector uses [AWS Systems Manager](https://docs.aws.amazon.com/systems-manager/latest/userguide/what-is-systems-manager.html) (SSM) and the SSM Agent to collect information about the software application inventory of your EC2 instances, this data is then scanned by Amazon Inspector for software vulnerabilities. Amazon Inspector can only scan for software vulnerabilities in [operating systems supported by Systems Manager](https://docs.aws.amazon.com/systems-manager/latest/userguide/prereqs-operating-systems.html).

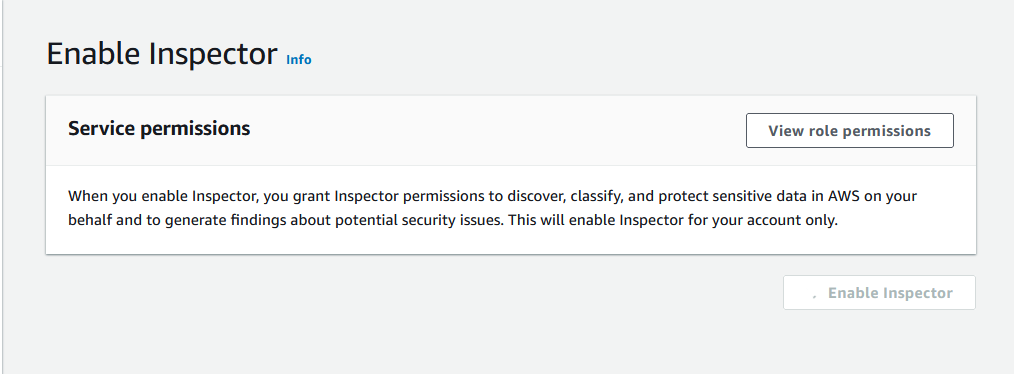
Amazon Inspector does not require the SSM Agent to scan Amazon EC2 instances for open network paths. There are no prerequisites for this type of scanning.

**Implementation**

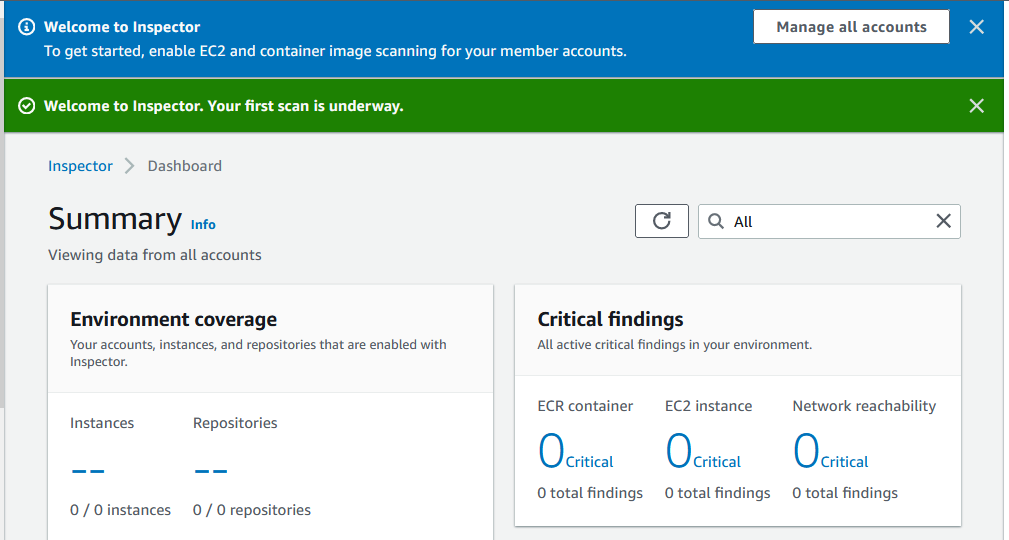
Go to Amazon Inspector services panel which is a paid service available for 15 day trial.



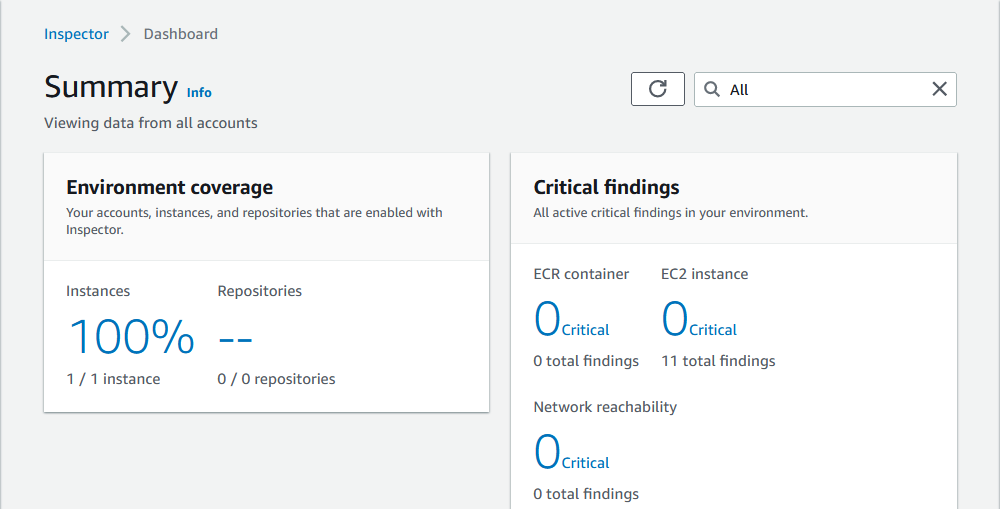
Get started and Enable Inspector



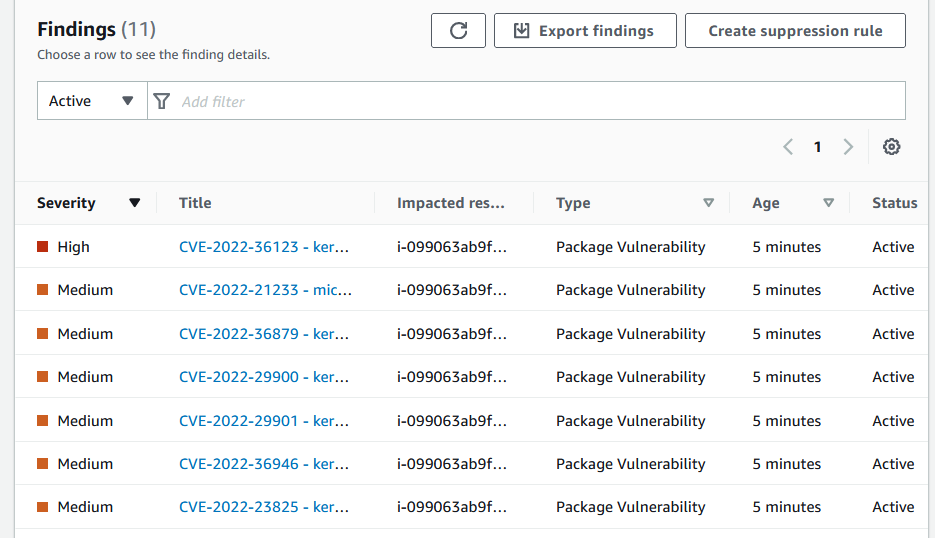
The **Summary** dashboard provides a snapshot view of aggregated statistics for your resources in the current AWS Region. If you are the Amazon Inspector administrator for your organization, the dashboard includes information for all of the member accounts in your organization



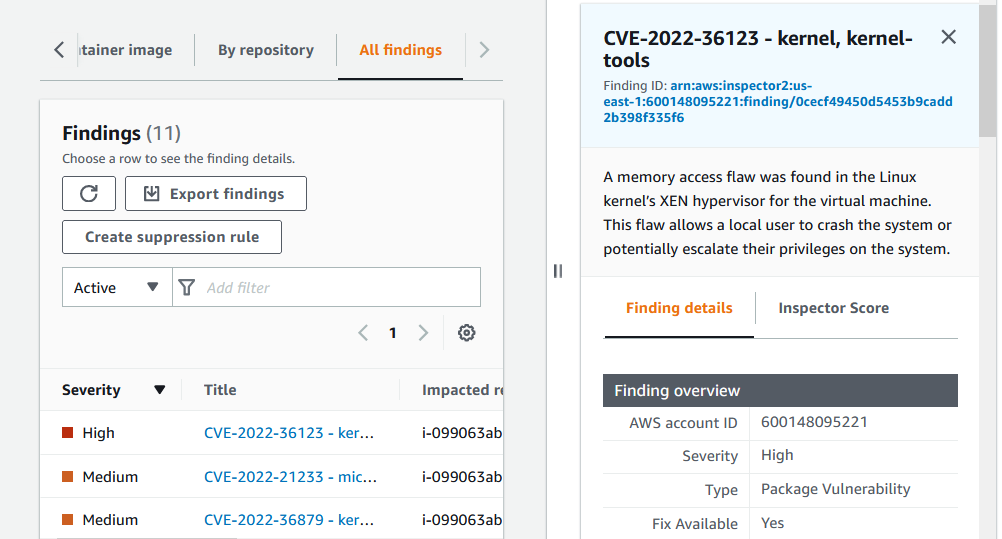
After scanning



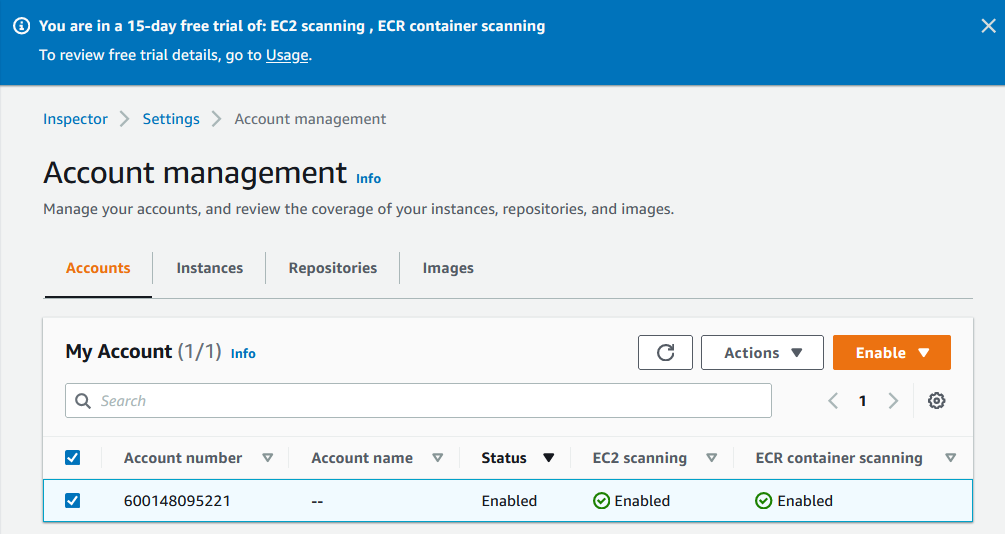
The findings are then listed in the findings page



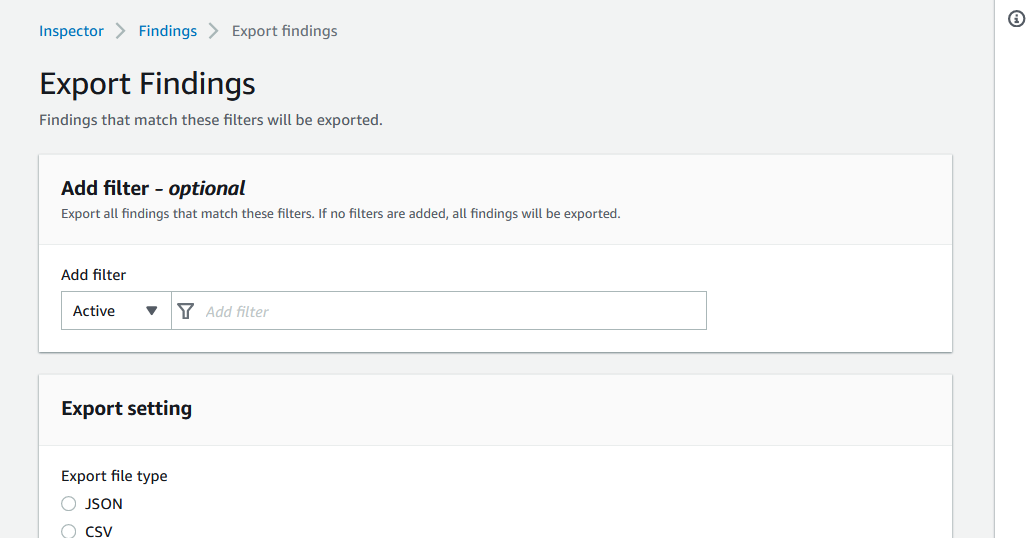
Choose a vulnerability to view the details related to that.

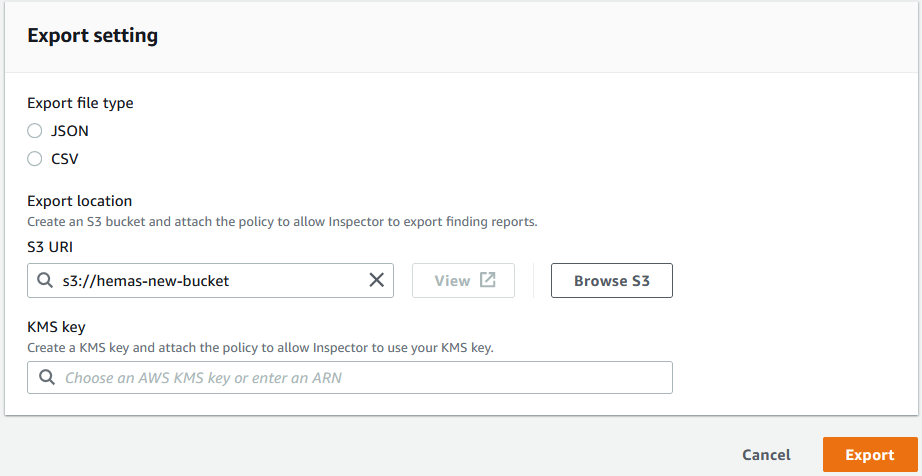


If you have multiple accounts, you can enable all scanning or EC2 scanning or ECR scanning



We can export and save the findings to S3 bucket





**Note** : Disable the Amazon Inspector feature for not getting charged.

**Services Protected by Amazon Inspector**

The one service protected by Amazon Inspector is Elastic Compute Cloud (EC2) Instances of AWS and Amazon Elastic Container Registry (ECR).

**How Inspector Protects EC2?**

Amazon Inspector is a service that automates security assessments and network accessibility testing for[**AWS EC2**](https://intellipaat.com/blog/what-is-amazon-ec2-in-aws/) instances. It aids in the detection of vulnerabilities in your EC2 instances and apps. Furthermore, it enables you to make security testing a more frequent event as part of the development and IT operations.

Amazon Inspector displays a clear list of security and compliance issues that have been prioritized by severity level. Furthermore, these discoveries may be analysed directly or as part of full evaluation records accessible through the API or the AWS Inspector UI. AWS Inspector security evaluations assist you in detecting unauthorized network access to EC2 instances as well as vulnerabilities on those EC2 instances.

It operates by first defining a target set of resources using tags, then configuring an assessment template that defines what we’re looking for (common vulnerabilities and exploits (CVEs), PCI requirements, and so on) and running an assessment against our target resources, examining the research results and reducing the issues discovered.

Amazon Inspector conducts an automated examination and delivers results reports with recommendations for environmental protection. To utilize this service, you must establish an AWS collection containing all the resources required for the application to progress and be tested.

It is then followed by the addition and execution of [**cloud security**](https://intellipaat.com/blog/what-is-cloud-security/) practices. You may also specify the length of the exam, which can range from 15 minutes to 12 hours or last for one day.

On the EC2 computers that host the application, an Inspector Agent observes the network, file system, and process activities. After gathering all of the necessary information, it is compared to the built-in security rules to discover security or compliance concerns.

**How Inspector Protects ECR?**

Amazon Inspector scans container images stored in Amazon ECR for software vulnerabilities to generate **Package Vulnerability** findings. For more information, see [Finding types in Amazon Inspector](https://docs.aws.amazon.com/inspector/latest/user/findings-types.html).

When you enable Amazon Inspector scans for Amazon ECR, you set Amazon Inspector as your preferred scanning service for your private registry. This replaces the default [**Basic scanning**](https://docs.aws.amazon.com/AmazonECR/latest/userguide/image-scanning.html), which is provided as a free service by Amazon ECR, with **Enhanced scanning**, which is provided and billed through Amazon Inspector.

The enhanced scanning provided by Amazon Inspector gives you the benefit of vulnerability scanning for both operating system and programming language packages at the registry level. You can review findings discovered using enhanced scanning at the image level, at each layer of the image, and on the Amazon ECR console. Additionally, you can review and work with these findings in other services not available for basic scanning findings, including AWS Security Hub and Amazon EventBridge.

Enhanced scanning gives you a choice between continuous scanning or on-push scanning at the repository level. Continuous scanning includes on-push scans and automated rescans. On-push scanning scans only when you push an image. For both options you can refine the scanning scope through inclusion filters.

Automated rescans are triggered for container images based on whether you use the continuous or on-push option in your **Enhanced scanning** settings. Whenever Amazon Inspector adds a new Common Vulnerabilities and Exposures (CVE) item to its database, eligible container images in Amazon ECR repositories configured with continuous scanning are scanned in response.

**List of common Vulnerabilities found by Inspector**

You must use very specific keywords, such as an application name, when searching the CVE List. For example: **Sendmail, wu-ftp, ToolTalk, ps**, etc.

**Benefits**

Automate the security assessment of your applications and proactively identify vulnerabilities. This allows you to develop and iterate on new applications quickly, and assess compliance with best practices and policies.

**Limitations**

Amazon Inspector is a Regional service. Inspector requires Systems Manager (SSM) agent to be installed and enabled.