**How to setup Amazon inspector through the console**

# **What is Amazon inspector?**

It is a vulnerability management service, which can scan for software vulnerabilities and network exposure.  
When it discovers an issue, it creates a finding which can be checked through the Amazon Inspector console.  
Findings can be in the following 3 categories:

* Package vulnerability
* Code vulnerability
* Network reachability

# **Why Amazon inspector?**

* Monitor your application for vulnerabilities
* Crosschecks for Security compliance & exposure to attack.
* Secure your EC2 for zero day vulnerability.
* Low Cost are few of the benefits using Amazon Inspector

# **Enabling Amazon Inspector:**

There are two ways it can be done. One is easy the other requires more advanced knowledge.

1. Through the console (*easy*)
   1. Log-in into AWS Console
   2. Navigate to the Amazon Inspector Service
   3. Click on the “Get Started” button.
   4. Click on the “Activate Inspector”.  
      This will create the necessary role permissions for you (*you can view it by clicking on the “View role permissions”*)

Notes:   
Read more here:   
<https://docs.aws.amazon.com/inspector/latest/user/getting_started_tutorial.html#tutorial_activate_scans>

1. Through AWS CLI (*advanced*)
   1. First you will need to have an access token set up to your account which you can use from your local machine. Also make sure that your AWS user has the necessary permissions here.
   2. Have AWS CLI version 2 installed on your local computer
   3. Open up a command line session
   4. Type the following command:  
      [enable — AWS CLI 2.13.25 Command Reference (amazonaws.com)](https://awscli.amazonaws.com/v2/documentation/api/latest/reference/inspector2/enable.html)  
      Example for enabling it only for EC2, assuming you are using the default AWS profile.  
      *aws inspector2 enable --resource-types "EC2" --region eu-central-1*

# **Setting up Amazon inspector:**

If you enabled AWS Inspector from the console you will have all the supported service scanning enabled.  
In order to have them properly working, there are a few keynotes to take:

## **EC2 Scanning:**

To have the Amazon Inspector EC2 scanning functionality working, it is not enough to just enable the ECS in Amazon Inspector, but you will need to have Amazon SSM Agent installed on the EC2 instances.  
To do so please check if your desired OS version is supported, and then on the end of the page click on the supported OS version you want to have it installed and follow the instructions to install the SSM Agent.  
<https://docs.aws.amazon.com/systems-manager/latest/userguide/sysman-manual-agent-install.html>  
  
TLDR;  
Quick install example on Linux:  
*wget* [*https://inspector-agent.amazonaws.com/linux/latest/install*](https://inspector-agent.amazonaws.com/linux/latest/install)  
or  
*curl -O* [*https://inspector-agent.amazonaws.com/linux/latest/install*](https://inspector-agent.amazonaws.com/linux/latest/install)  
then   
sudo bash install  
  
Quick install example on For Windows:  
Download .exe file from this [link](https://inspector-agent.amazonaws.com/windows/installer/latest/AWSAgentInstall.exe)

**ECR Scanning:**  
There are no extra actions to do after you enable ECR scanning in Amazon Inspector but it is important to know that when you set Amazon Inspector as your preferred scanning service for your private registry, this replaces the default basic scanning which is provided at no charge by Amazon ECR. Enhanced scanning, which is provided and billed through Amazon Inspector.

## **Lambda Scanning**

When activated Amazon Inspector scans all Lambda functions invoked or updated in the last 90 days in your account.  
Lambdas will be scanned when:

* Inspector find an existing Lambda function
* New lambda deployment
* Updating the lambda function application code or its dependencies (in lambda or in layer)
* Whenever Inspector adds a new CVE item to its database

Scan only runs if the following criteria are met:

* Lambda function is marked $LATEST
* Function was invoked or updated in the last 90 days
* Lambda is not excluded from scan by Tags

## **Vulnerability database search:**

If you find a CVE (*Common Vulnerabilities and Exposures*) you have the option to look it up through the Amazon Inspector AWS Console page, under the “Vulnerability database search” sidebar menu item.   
Searching for a CVE in this list gives you detailed information and references to learn more about a specific CVE.

## **Video tutorials:**

[Video tutorials | Amazon Inspector | eu-central-1](https://eu-central-1.console.aws.amazon.com/inspector/v2/home?region=eu-central-1#/video-tutorials)