

Amazon Inspector

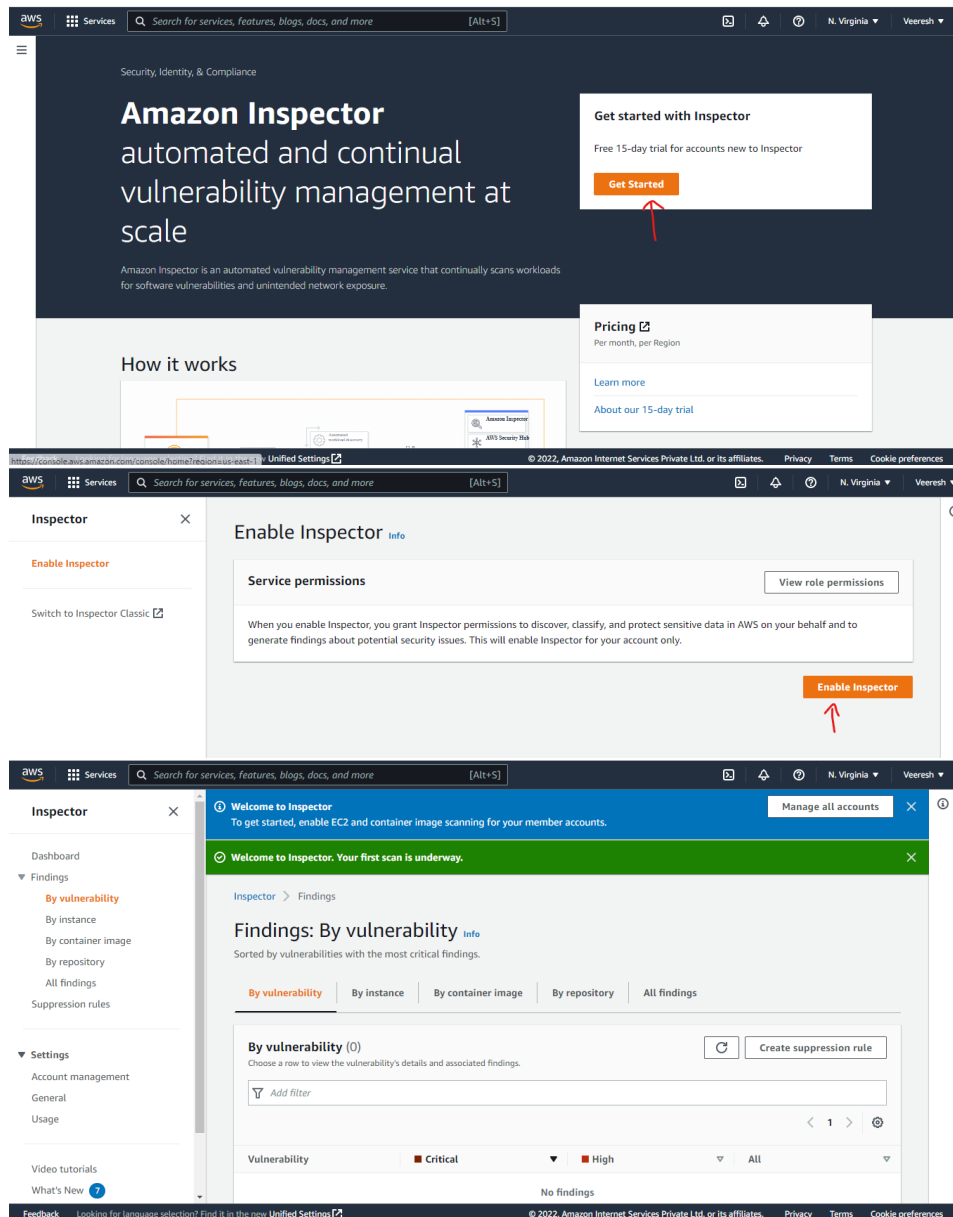
Amazon Inspector is an automated security assessment service and to test network accessibility of EC2 instance. It helps you to identify vulnerabilities within your EC2 instances and applications. And allows you to make security testing more regular occurrence as part of the development and IT operations.

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.

Hands on:

Step 1 :

- Goto amazon inspector dashboard, select get started.
- Next enable the inspector.



Step 2: Launch an EC2 instance with security group ports , 21,22, 443 at source everywhere. This is for we can track the vulnerabilities.

Step 6: Configure Security Group

A security group is a set of firewall rules that control the traffic for your instance. On this page, you can add rules to allow specific traffic to reach your instance. For example, if you want to set up a web server and allow internet traffic to reach your instance, add rules that allow unrestricted access to the HTTP and HTTPS ports. You can create a new security group or select from an existing one below. [Learn more](#) about Amazon EC2 security groups.

Assign a security group: ☒ Create a new security group
☐ Select an existing security group

Security group name:
Description:

| Type | Protocol | Port Range | Source | Description |
|------------|----------|------------|--------------------------|----------------------------|
| SSH | TCP | 22 | Anywhere 0.0.0.0/0, ::/0 | e.g. SSH for Admin Desktop |
| HTTPS | TCP | 443 | Anywhere 0.0.0.0/0, ::/0 | e.g. SSH for Admin Desktop |
| Custom TCP | TCP | 21 | Anywhere 0.0.0.0/0, ::/0 | e.g. SSH for Admin Desktop |

[Add Rule](#)

Warning

[Cancel](#) [Previous](#) [Review and Launch](#)

Step 3 :

- Goto the inspector assessment targets, create the target with all instances.
- Create and run assessment templates with the assessment target which are previously created.
- We can get the data of vulnerabilities as TCP port 21 for High risk, TCP port 22 for medium risk.

Inspector

Search results for 'inspe'

Services

- Inspector** ☆
Analyze Application Security
- Amazon Lookout for Vision** ☆
Identify defects using computer vision to automate quality inspection.
- Systems Manager** ☆
AWS Systems Manager is a Central Place to View and Manage AWS Resources

Top features

- Assessment targets
- Assessment templates
- Assessment findings

Features

Introducing the new Amazon Inspector

The new Amazon Inspector is a completely rearchitected version of the existing Inspector Classic. The new Inspector is an automated vulnerability management service that continually scans your EC2 and Container workloads for software vulnerabilities and unintended network exposure. [Learn more](#) [Start your free trial](#)

Amazon Inspector - Assessment Targets

An assessment target represents a collection of AWS resources that help you accomplish your business goals. [Learn more](#).

[Create](#) [Edit](#) [Delete](#)

Last updated on October 4, 2022 5:16:28 PM (0m ago)

☐ **Name** **Tags** **Templates**

No Results

Max records per page: 25

* refresh browser to reflect change

awsServicesSearch for services, features, blogs, docs, and more[Alt+S]

FeedbackFeedback (1/3)

© 2022 Amazon Internet Services Private Ltd. or its affiliates. PrivacyTerms

Name

Tags

Templates

myassessment

Assessment Target - myassessment

Name*myassessment

All instances

☒

Include all EC2 instances in this AWS account and region.

Note: The limit on the maximum number of agents that can be included in an assessment run applies. [Learn more](#)

Install Agents

☒

Install the Amazon Inspector Agent on all EC2 instances in this assessment target.

To use this option, make sure that your EC2 instances have the SSM Agent installed and an IAM role that allows Run Command. [Learn more](#)

*Required

Save

Cancel

Preview

awsServicesSearch for services, features, blogs, docs, and more[Alt+S]

FeedbackFeedback (1/3)

© 2022 Amazon Internet Services Private Ltd. or its affiliates. PrivacyTerms

Dashboard

Assessment targets

Assessment templates

Assessment runs

Findings

Switch to Inspector V2

Introducing the new Amazon Inspector

The new Amazon Inspector is a completely rearchitected version of the existing Inspector Classic. The new Inspector is an automated vulnerability management service that continually scans your EC2 and Container workloads for software vulnerabilities and unintended network exposure. [Learn more](#) [Start your free trial](#)

Amazon Inspector - Assessment Templates

An assessment template allows you to specify various properties for an assessment run, including rules packages, duration, SNS notifications, and how to label any findings. [Learn more](#).

CreateRunDeleteCloneCreate Assessment Events

Last updated on October 4, 2022 5:18:40 PM (0m ago)

Filter

Viewing 0-0 of 0

| | Name | Duration | Target name | Last run | All runs |
|--|------|----------|-------------|----------|----------|
| | | | | | |

No Results

Max records per page: 25

* refresh browser to reflect change

awsServicesSearch for services, features, blogs, docs, and more[Alt+S]

FeedbackFeedback (1/3)

© 2022 Amazon Internet Services Private Ltd. or its affiliates. PrivacyTerms

CreateRunDeleteCloneCreate Assessment Events

Last updated on October 4, 2022 5:18:40 PM (0m ago)

Filter

Viewing 1-1 of 1

| | Name | Duration | Target name | Last run | All runs |
|--|--------------|----------|--------------|----------|----------|
| | myassessment | N/A | myassessment | | |

Assessment Template - myassessment

Name*myassessment

Target name*myassessment

Rules packages*

Network Reachability-1.1

Security Best Practices-1.0

Common Vulnerabilities and Exposures-1.1

CIS Operating System Security Configuration Benchmarks-1.0

Duration*1 Hour (Recommended)

SNS topics

Select a new SNS topic to notify of events

The first screenshot shows the 'Create and run' button in the AWS IAM console. The page includes fields for 'SNS topics', 'Tags', 'Attributes added to findings', and 'Assessment Schedule'. The 'Assessment Schedule' is set to '7' days. The 'Create and run' button is highlighted.

The second screenshot shows the 'Amazon Inspector - Findings' page. The page displays a list of findings with columns for 'Severity', 'Date', 'Finding', 'Target', and 'Template'. The findings are filtered by 'Severity' and 'Date'. The findings are as follows:

| Severity | Date | Finding | Target | Template |
|---------------|--------------------|--|--------------|----------|
| High | Today at 5:21 P... | On instance i-0f73a702e4c73fed9, TCP port 21 which is associated with '... | myassessment | myassesm |
| High | Today at 5:20 P... | On instance i-0f73a702e4c73fed9, TCP port 21 which is associated with '... | myassessment | myassesm |
| Medium | Today at 5:21 P... | On instance i-0f73a702e4c73fed9, TCP port 22 which is associated with '... | myassessment | myassesm |
| Medium | Today at 5:20 P... | On instance i-0f73a702e4c73fed9, TCP port 22 which is associated with '... | myassessment | myassesm |
| Low | Today at 5:21 P... | On instance i-0f73a702e4c73fed9, TCP port 443 which is associated with... | myassessment | myassesm |
| Low | Today at 5:20 P... | On instance i-0f73a702e4c73fed9, TCP port 443 which is associated with... | myassessment | myassesm |
| Informational | Today at 5:21 P... | Aggregate network exposure: On instance i-0f73a702e4c73fed9, ports ar... | myassessment | myassesm |
| Informational | Today at 5:20 P... | Aggregate network exposure: On instance i-0f73a702e4c73fed9, ports ar... | myassessment | myassesm |

Step 4 : now get back to the EC2 instance security group and remove all previously created protocols and add the ssh 22 custom source and save it.

- Then goto the assessment templets select and run the templets.
- Then we will find the medium and informational severity.

EC2 > Security Groups > sg-076444ae48ab91d5e - inspector > Edit inbound rules

Edit inbound rules [Info](#)

Inbound rules control the incoming traffic that's allowed to reach the instance.

Inbound rules [Info](#)

| Security group rule ID | Type Info | Protocol Info | Port range Info | Source Info | Description - optional Info | |
|------------------------|---------------------------|-------------------------------|---------------------------------|-----------------------------|---|------------------------|
| - | SSH | TCP | 22 | Custom | | Delete |

[Add rule](#)

[Cancel](#) [Preview changes](#) [Save rules](#)

Dashboard
Assessment targets
Assessment templates
Assessment runs
Findings
Switch to Inspector V2

Amazon Inspector - Assessment Templates

An assessment template allows you to specify various properties for an assessment run, including rules packages, duration, SNS notifications, and how to label any findings. [Learn more.](#)

[Create](#) [Run](#) [Delete](#) [Clone](#) [Create Assessment Events](#) Last updated on October 4, 2022 5:24:19 PM (0m ago)

Filter 1 selected

| Name | Duration | Target name | Last run | All runs |
|--------------|----------|--------------|-----------------|----------|
| myassessment | 1 Hour | myassessment | Collecting data | 2 |

Max records per page: 25
* refresh browser to reflect change

Dashboard
Assessment targets
Assessment templates
Assessment runs
Findings
Switch to Inspector V2

Amazon Inspector - Assessment Runs

An assessment run is the process of discovering potential security issues through the analysis of your assessment target's behavior against selected rules packages. [Learn more.](#)

[Run](#) [Cancel](#) [Delete](#) Last updated on October 4, 2022 5:25:16 PM (0m ago)

Filter 1 selected

| Start time | Status | Template name | Findings | Findings by s... | Exclusions | Reports |
|--------------------|-------------------|---------------|----------|---------------------|------------|--------------------------------|
| Today at 5:24 P... | Analysis complete | myassessment | 2 | High Medium ... | 1 | Download re... |
| Today at 5:21 P... | Analysis complete | myassessment | 4 | High Medium ... | 1 | Download re... |
| Today at 5:20 P... | Analysis complete | myassessment | 4 | High Medium ... | 1 | Download re... |

Max records per page: 25
* refresh browser to reflect change

Feedback English (US) © 2022, Amazon Internet Services Private Ltd. or its affiliates. Privacy Terms

Dashboard
Assessment targets
Assessment templates
Assessment runs
Findings
Severity Filter
High
Medium
Low
Informational
Switch to Inspector V2

Amazon Inspector - Findings

Findings are potential security issues discovered after Amazon Inspector runs an assessment against a specified assessment target. [Learn more.](#)

Filters: ("assessmentRuns": {"arn": "aws:inspector:us-east-1:881832161071:target/0-xb6nf3Qu/template/0-K9fmCKv/run/0-Uvk124tg"})

[Add/Edit attributes](#) Last updated on October 4, 2022 5:26:06 PM (0m ago)

Filter Viewing 1-2 of 2

| Severity | Date | Finding | Target | Template | Rules Pac |
|---------------|-----------------|--|--------------|--------------|------------|
| Medium | Today at 5:2... | On instance i-073a702e4c73fed9, TCP port 22 whi... | myassessment | myassessment | Network Ri |
| Informational | Today at 5:2... | Aggregate network exposure: On instance i-073a7... | myassessment | myassessment | Network Ri |

Max records per page: 25
* refresh browser to reflect change