

Home / AWS / Guided Lab / Find vulnerabilities on EC2 instance using Amazon Inspector

# Find vulnerabilities on EC2 instance using Amazon Inspector

Level: Intermediate

Amazon Inspector    Amazon Web Services



0h 3m 38s left



End Lab

Open Console

Validation

## Lab Credentials

User Name ⓘ

Whiz\_User\_80425.87361784



Password ⓘ

b1728cb3-a108-4f6f-a813-b379e32b30ee



Access Key ⓘ

AKIASVIAO3JRBYUQ4ZHK



Secret Key ⓘ

tf0nBocw6L2P7+udrDyZ7nuRQcjL+Xm/M5dfYlo3






## Lab Resources

No Lab Resources Found

## Support Documents

No Support Documents Found

## Need help?

-  How to use Hands on Lab
-  Troubleshooting Lab
-  FAQs

[Submit Feedback](#)[Share](#)[Lab Overview](#)[Lab Steps](#)[Lab Validation](#)[Lab FAQs](#) Cloud Security Engineer Security

# Lab Steps

## Task 1: Sign in to AWS Management Console

1. Click on the **Open Console** button, and you will get redirected to AWS Console in a new browser tab.
2. On the AWS sign-in page,
  - Leave the Account ID as default. Never edit/remove the 12 digit Account ID present in the AWS Console. otherwise, you cannot proceed with the lab.
  - Now copy your **User Name** and **Password** in the Lab Console to the **IAM Username and Password** in AWS Console and click on the **Sign in** button.
3. Once Signed In to the AWS Management Console, Make the default AWS Region as **US East (N. Virginia) us-east-1**.

## Task 2 : Launching an EC2 Instance

1. Make sure you are in the US East **(N. Virginia) us-east-1** Region.
2. Navigate to EC2 by clicking on the **Services** menu in the top, then click on **EC2** in the **Compute** section.
3. Navigate to **Instances** on the left panel and click on **Launch Instances**

- Name : *Inspector-EC2*


</

- Select **Quick Start** tab and **Amazon Linux** under it
- Amazon Machine Image (AMI) : select *Amazon Linux 2 AMI*


## Application and OS Images (Amazon Machine Image) [Info](#)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below


### Quick Start




Amazon Linux




Ubuntu



Windows



Red Hat



SUSE Linux

[Browse more AMIs](#)

Including AMIs from AWS, Marketplace and the Community

### Amazon Linux 2 AMI (HVM) - Kernel 5.10, SSD Volume Type

ami-0cff7528ff583bf9a (64-bit (x86)) / ami-00bf5f1c358708486 (64-bit (Arm))

Virtualization: hvm    ENA enabled: true    Root device type: ebs

Free tier eligible

### Description

Amazon Linux 2 Kernel 5.10 AMI 2.0.20220606.1 x86\_64 HVM gp2

Architecture

64-bit (x86)

AMI ID

ami-0cff7528ff583bf9a

- Instance Type : Select **t2.micro**

▼ Instance type [Info](#)

Instance type

t2.micro

Family: t2 1 vCPU 1 GiB Memory

On-Demand Linux pricing: 0.0116 USD per Hour

On-Demand Windows pricing: 0.0162 USD per Hour

Free tier eligible

[Compare instance types](#)

7. Under the **Key Pair (login)** section :

- Click on Create new key pair hyperlink
- Key pair name: **MyEC2Key**
- Key pair type: **RSA**
- Private key file format: **.pem** or **.ppk**
- Click on Create key pair and select the created key pair

Create key pair

×

Key pairs allow you to connect to your instance securely.

Enter the name of the key pair below. When prompted, store the private key in a secure and accessible location on your computer. **You will need it later to connect to your instance.** [Learn more](#)

Key pair name

MyEC2Key

The name can include upto 255 ASCII characters. It can't include leading or trailing spaces.

Key pair type

☒ RSA

RSA encrypted private and public key pair

☐ ED25519

ED25519 encrypted private and public key pair (Not supported for Windows instances)

Private key file format

☒ .pem

For use with OpenSSH

☐ .ppk

For use with PuTTY

Cancel

Create key pair

8. Under the **Network Settings** section :

- Click on **Edit** button
- Auto-assign public IP: select **Enable**
- Firewall (security groups) : Select **Create a new security group**
  - Security group name : Enter **Inspector-SG**
  - Description : Enter **Security group for Inspector EC2**
  - To add **SSH**:
    - Choose Type: **SSH**
    - Source: **Anywhere** (From ALL IP addresses accessible).
  - For **Custom TCP Rule**, click on **Add security group rule**,
    - Choose Type: **Custom TCP**
    - Port range : **21**
    - Source: **Anywhere** (From ALL IP addresses accessible).
  - For **Custom TCP Rule**, click on **Add security group rule**,
    - Choose Type: **Custom TCP**
    - Port range : **23**
    - Source: **Anywhere** (From ALL IP addresses accessible).
  - For **Custom TCP Rule**, click on **Add security group rule**,
    - Choose Type: **Custom TCP**
    - Port range : **20**
    - Source: **Anywhere** (From ALL IP addresses accessible).

**Firewall (security groups)** [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

☒ Create security group ☐ Select existing security group

Security group name - *required*

Inspector-SG

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and .\_-:/()#,@[]+=&;{}!\$\*

Description - *required* [Info](#)

Security group for Inspector EC2

▼ Security group rule 1 (TCP, 22, 0.0.0.0/0)

Type [Info](#)

ssh

Protocol [Info](#)

TCP

Port range [Info](#)

22

Source type [Info](#)

Anywhere

Source [Info](#)

Q Add CIDR, prefix list or security

0.0.0.0/0 X

Description - optional [Info](#)

e.g. SSH for admin desktop

Remove

▼ Security group rule 2 (TCP, 21, 0.0.0.0/0)

Type [Info](#)

Custom TCP

Protocol [Info](#)

TCP

Port range [Info](#)

21

Source type [Info](#)

Anywhere

Source [Info](#)

Q Add CIDR, prefix list or security

0.0.0.0/0 X

Description - optional [Info](#)

e.g. SSH for admin desktop

Remove

▼ Security group rule 3 (TCP, 23, 0.0.0.0/0)

Type [Info](#)

Custom TCP

Protocol [Info](#)

TCP

Port range [Info](#)

23

Source type [Info](#)

Anywhere

Source [Info](#)

Q Add CIDR, prefix list or security

0.0.0.0/0 X

Description - optional [Info](#)

Remove

9. Keep everything else as default and click on the **Launch instance** button.
10. **Launch Status:** Your instance is now launching, Navigate to **Instances** page from the left menu and wait until the status of the EC2 Instance changes to **running**.
11. Note down the sample IPv4 Public IP Address of the EC2 instance. A sample is shown in the screenshot below.

Instance: i-0cf858079998f5bef (Inspector-EC2)

Details

Security

Networking

Storage

Status checks

Monitoring

Tags

▼ Instance summary [Info](#)

Instance ID

i-0cf858079998f5bef (Inspector-EC2)

Public IPv4 address

34.204.171.197 | [open address](#)

Task 3 : SSH into EC2 Instance

- Please follow the steps in [SSH into EC2 Instance](#) using **putty tool**, or you can use **Ec2 instance connect**.

Task 4: Install an AWS Agent

1. Switch to root user:



```
sudo su
```



2. Download the agent installation script by running one of the following commands:

```
wget https://inspector-agent.amazonaws.com/linux/latest/install
```



```
curl -O https://inspector-agent.amazonaws.com/linux/latest/install
```



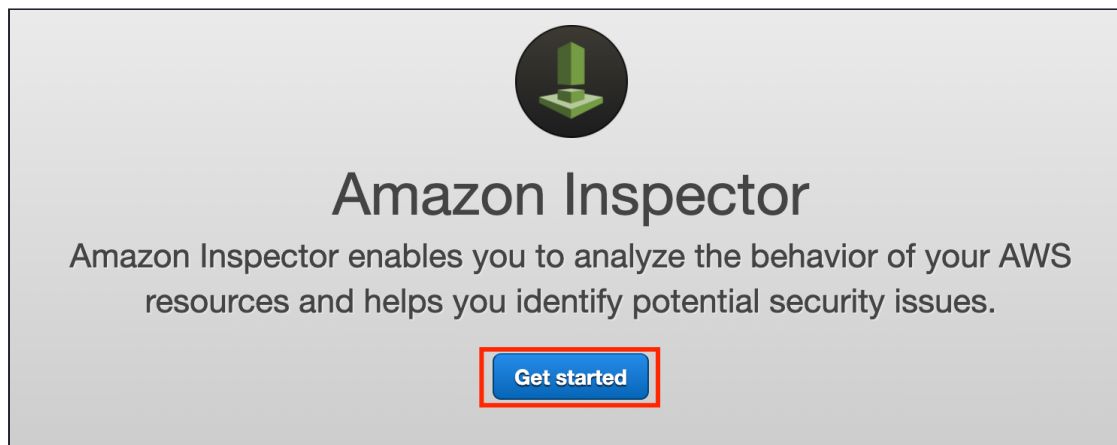
3. To install the agent, run the following command:

```
sudo bash install
```



## Task 5: Create an assessment target

1. Navigate to **Inspector** by clicking on the Services menu in the top, then click on **Inspector** in the **Security, Identity & Compliance** section.
2. Expand the left side column and switch to **Amazon Inspector Classic**.
3. On the home page, click on the **Get started** button.



4. Click on the **Cancel** button present on the right bottom corner, to see the options. Run weekly, Run once and Advanced setup is for quick setup.



Welcome to Amazon Inspector

Amazon Inspector assessments check for security exposures and vulnerabilities in your EC2 instances. Learn more about [how Inspector functions](#).

Inspector uses a [Service-linked Role](#) to describe your EC2 instances and network configuration.

### Assessment Setup

You can use the options below to get the following assessments on all of your EC2 instances in this AWS region. Click **Run weekly** for the assessment to run at this time once a week starting now, **Run once** for a one-time assessment, or **Advanced setup** for custom assessments.

☒ **Network Assessments** (Inspector Agent is not required)

- Assessments performed:** Network configuration analysis to checks for ports reachable from outside the VPC. [Learn more](#)
- Optional Agent:** If the Inspector Agent is installed on your EC2 instances, the assessment also finds processes reachable on port. Learn more about [Inspector Agent](#)
- Pricing:** Pricing for **network assessments** is based on the monthly volume of instance-assessments, where an instance-assessment denotes a successful assessment of an instance. For example, for 100 instances assessed weekly, the monthly cost would be around \$61/month. [Learn more](#)

☒ **Host Assessments** (Inspector Agent is required)

- Assessments performed:** Vulnerable software (CVE), host hardening (CIS benchmarks), and security best practices. [Learn more](#)
- Agent Deployment:** Inspector assessments require an agent to be installed on your EC2 instances. We will automatically install the agent for instances that allow [System Manager Run Command](#). Learn more about [Inspector Agent](#) and [how to manually install agent](#).
- Pricing:** Pricing for **host assessments** is based on the monthly volume of agent-assessments, where an agent-assessment denotes a successful assessment of an instance. For example, for 100 instances assessed weekly, the monthly cost would be around \$120/month. [Learn more](#)

Run weekly (recommended) Run once Advanced setup **Cancel**

- On the left side bar, click on the **Assessment targets**.
- Click on the **Create**.
- Fill in the details, Name: **Demo**
- All instances: Select **Include all EC2 instances in this AWS account and region**.
- Install Agents: **Selected by Default**
- Click on the **Save** button, to create an Assessment Target.

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 March 11, 2021 12:07:14 PM (1m ago) Refresh Download Settings

Filter < Viewing 1-1 of 1 >

	Name	Tags	Templates
<input type="checkbox"/>	Demo		

**Assessment Target - Demo**

Name\*

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.

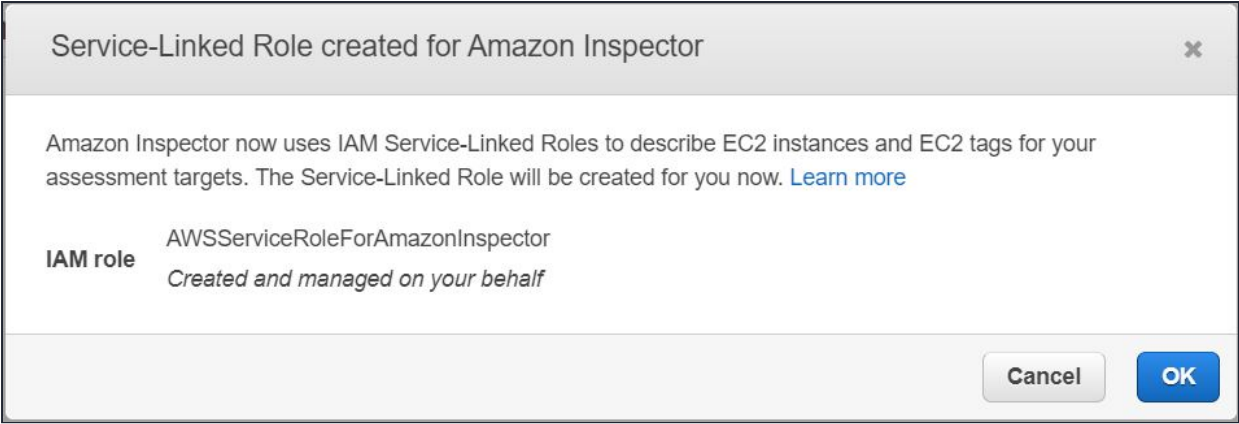
To use this option, make sure that your EC2 instances have the SSM Agent installed and an IAM role that allows Run Command. [Learn more](#)

\*Required

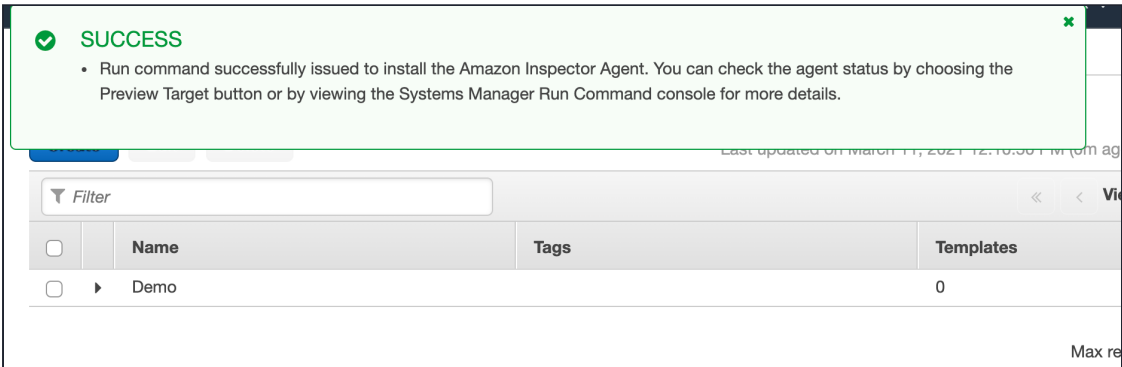
**Save** Cancel Preview

- Click the **OK** button on the pop-up menu.





11. The assessment target is now created.



Task 6: Create an assessment template

1. On the left side bar, click on the **Assessment templates**.
2. Click on the **Create**.
3. Fill in the below details, as follows:
- Name: Enter **Whiz**

• Target Name: Select **Demo**

• Rules packages: **Select all four rules, one-by-one**

Name\*

Whiz

Target name\*

Demo

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: **15 Minutes**
- Keep all other options as default.
- Click on the **Create** button.

Duration\* 15 Minutes

SNS topics Select a new SNS topic to notify of events

Tags

Key

Value

Add a new key

Attributes added to findings

Key

Value

Add a new key

Add a new value

Assessment Schedule

Set up recurring assessment runs once every 7 days. The first run starts on create. Learn more

\*Required

Create and run

Create

Cancel

4. Assessment template **Whiz** is now getting created.

Working

Saving assessment template

Attaching rules packages

5. It's created, in the next step you will run the template to find the vulnerabilities on the created EC2 instance.

CreateRunDeleteCloneCreate Assessment Events

Last updated on March 11, 2021 2:35:01 PM (7m ago)

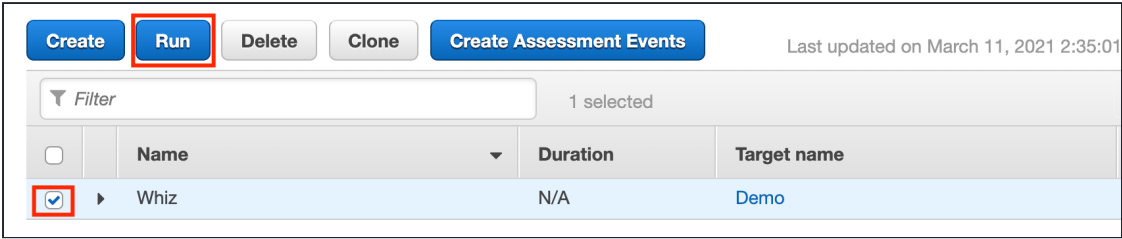
Filter

Viewing 1-1 of 1

	Name	Duration	Target name	Last run	All runs
<input type="checkbox"/>	Whiz	N/A	Demo		

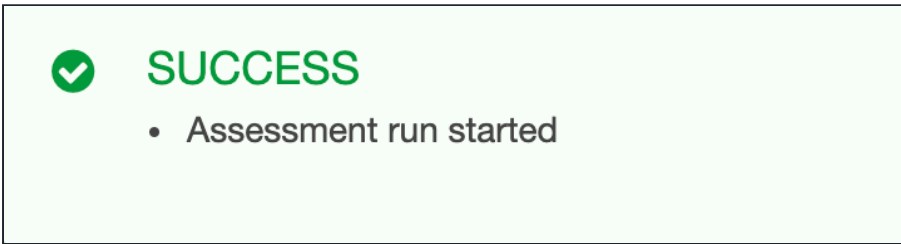
Task 7: Run the assessment template

1. Select Assessment templates **Whiz**, and click on the **Run** button.(If any error pops up stating error, ignore it.)



	Name	Duration	Target name
<input checked="" type="checkbox"/>	Whiz	N/A	Demo

2. The assessment run has started.

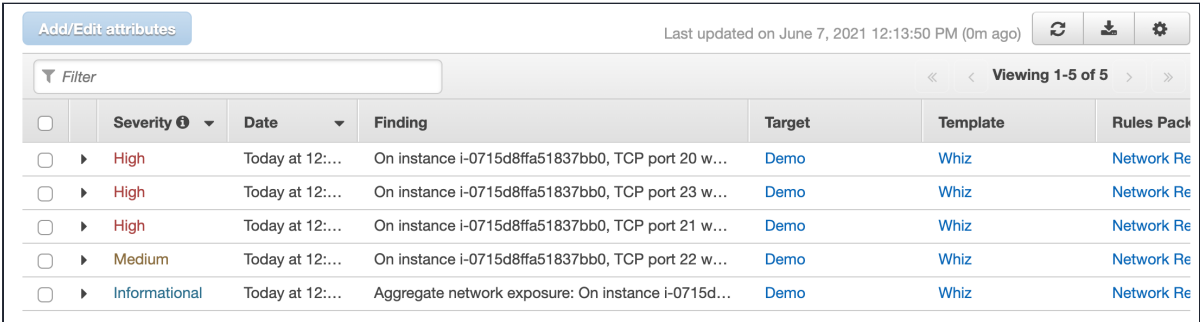


3. To see the Assessment Run and its result, click on the **Assessment runs** present on the left sidebar.
4. Click on the number of findings to know about the vulnerabilities found by Inspector on the EC2 instance.



	Start time	Status	Template name	Findings	Findings by s...	Exclusions	Reports
<input type="checkbox"/>	Today at 12:09 ...	Analysis complete	Whiz	5	High   Medium  ...	1	Download re...

5. There are currently 5 findings.



	Severity	Date	Finding	Target	Template	Rules Pack
<input type="checkbox"/>	High	Today at 12:...	On instance i-0715d8ffa51837bb0, TCP port 20 w...	Demo	Whiz	Network Re
<input type="checkbox"/>	High	Today at 12:...	On instance i-0715d8ffa51837bb0, TCP port 23 w...	Demo	Whiz	Network Re
<input type="checkbox"/>	High	Today at 12:...	On instance i-0715d8ffa51837bb0, TCP port 21 w...	Demo	Whiz	Network Re
<input type="checkbox"/>	Medium	Today at 12:...	On instance i-0715d8ffa51837bb0, TCP port 22 w...	Demo	Whiz	Network Re
<input type="checkbox"/>	Informational	Today at 12:...	Aggregate network exposure: On instance i-0715d...	Demo	Whiz	Network Re

6. Click on the expand button for the first finding, to see the details.

Run name [Run - Whiz - 2021-06-07T06:39:10.948Z](#)

Target name [Demo](#)

Template name [Whiz](#)

Start Today at 12:09 PM (GMT+5) (6 minutes ago)


End Today at 12:09 PM (GMT+5) (6 minutes ago)

Status Analysis complete

Rules package [Network Reachability-1.1](#)

AWS agent ID [i-0715d8ffa51837bb0](#)

**Finding** On instance [i-0715d8ffa51837bb0](#), TCP port 20 which is associated with 'FTP' is reachable from the internet

Severity High 


**Description** On this instance, TCP port 20, which is associated with FTP, is reachable from the internet. You can install the Inspector agent on this instance and re-run the assessment to check for any process listening on this port. The instance [i-0715d8ffa51837bb0](#) is located in VPC [vpc-3418934e](#) and has an attached ENI [eni-064aa887dd0271e5](#) which uses network ACL [acl-5754a62a](#). The port is reachable from the internet through Security Group [sg-0493299d8801804aa](#) and IGW [igw-6627d91d](#).

**Recommendation** You can edit the Security Group [sg-0493299d8801804aa](#) to remove access from the internet on port 20.




7. The **description** field has details about the finding, while the **Recommendation** field has the message to solve the issue and avoid this finding.

## Task 8: Download the assessment run report

1. Click on the Assessment runs, present on the left sidebar.
2. Wait for Collection status in Assessment to become Analysis Completed. It may take 10 minutes to complete Otherwise you can't download report
3. Choose the **Download report** button.

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 June 7, 2021 12:18:27 PM (0m ago)   



<< < Viewing 1-1 of 1 > >>

<input type="checkbox"/>	Start time	Status	Template name	Findings	Findings by sev...	Exclusions	Reports
<input type="checkbox"/>	Today at 12:09 P...	Analysis complete	Whiz	5	High   Medium   L...	1	<a href="#">Download report</a>

4. After you click on the **Download report** option, you will be prompted with a screen to select the report type and format.
5. Keep the option default, Report type as **Findings report**, and report format as **PDF**. Click on the **Generate Report** button.

Assessment report

 WHIZLABS

  K ▼

☒ Findings report

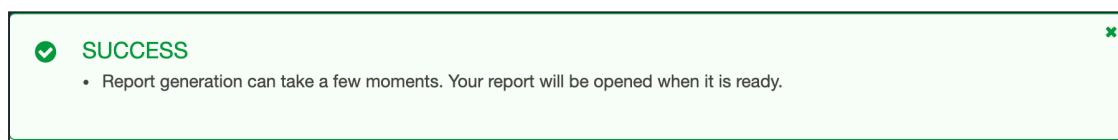
☐ Full report

Select report format:

☐ HTML ☒ PDF

**Generate report** Close

6. It would take a couple of seconds to generate the report.



7. Once ready, it will open in the new tab of your browser.



8. **Note: Vulnerabilities of Informational severity will not be shown in the report. To see that regenerate the report with the Full report option.**

9. If there are more than 3 vulnerabilities found, it is recommended to generate the report and check the issue.



## Do You Know ?


Amazon Inspector supports not only system-level vulnerability assessments but also offers specific rules packages for assessing compliance with industry standards and best practices.

### Task 9: Validation Test

1. Once the lab steps are completed, please click on the **Validate** button on the left side panel.
2. This will validate the resources in the AWS account and displays whether you have completed this lab successfully or not.
3. Sample output :

#### Check your Validation

If any checks fail  , you can use the remaining time in the Lab to work on making the checks pass  . Click Validate My Lab again to rerun the checks at any time.

Validate My Lab 

##### Launch an Amazon EC2 Instance

Check whether an Amazon Linux 2 Instance is created or not.

##### Create Assessment Target

Check whether an Inspector Assessment target is created or not

##### Create Assessment Template

Check whether an Inspector Assessment template is created or not

##### Add Assessment Template Rules Packages

## Completion and Conclusion

1. You have successfully created and launched Amazon EC2 Instance.
2. You have successfully created an Inspector assessment target and template.
3. You have successfully found the vulnerabilities on the configured EC2 instance.

## End Lab

1. Sign out of AWS Account.
2. You have successfully completed the lab.

3. Once you have completed the steps, click on **End Lab** from your whizlabs lab console and wait till the process gets completed.

[About Us](#)   [Subscription](#)   [Instructions and Guidelines](#)   [FAQ's](#)   [Contact Us](#)



© 2024, Whizlabs Software Pvt. Ltd.

