

AWS Security: Amazon Inspector



In this lab, we are going to implement Amazon Inspector in our environment. Amazon Inspector is an automated security assessment service that helps improve the security and compliance of applications deployed on AWS. Amazon Inspector automatically assesses applications for vulnerabilities or deviations from best practices. After performing an assessment, Amazon Inspector produces a detailed list of security findings prioritized by level of severity. These findings can be reviewed directly or as part of detailed assessment reports which are available via the Amazon Inspector console or API.

Below is the list of tasks:

Task 1: Create IAM Role

Task 2: Launch & Configure EC2 Instances with SSM Agent

Task 3: AWS Systems Manager: Managed Instances

Task 4: Amazon Inspector Configurations

Task 5: Amazon Inspector Troubleshooting

Task 6: Amazon Inspector-Findings

Task 1: Create IAM Role

Login to the AWS Management Console.

Navigate to IAM Service and click on Roles.

Click on Create Role.

Make sure to select the Use Case as **EC2**.

Click Next: Permissions.

aws Services Resource Groups

Console Home

Create role

1 2 3 4

Select type of trusted entity

AWS service
EC2, Lambda and others

Another AWS account
Belonging to you or 3rd party

Web identity
Cognito or any OpenID provider

SAML 2.0 federation
Your corporate directory

Allows AWS services to perform actions on your behalf. [Learn more](#)

Choose a use case

Common use cases

EC2
Allows EC2 instances to call AWS services on your behalf.

Lambda
Allows Lambda functions to call AWS services on your behalf.

Or select a service to view its use cases

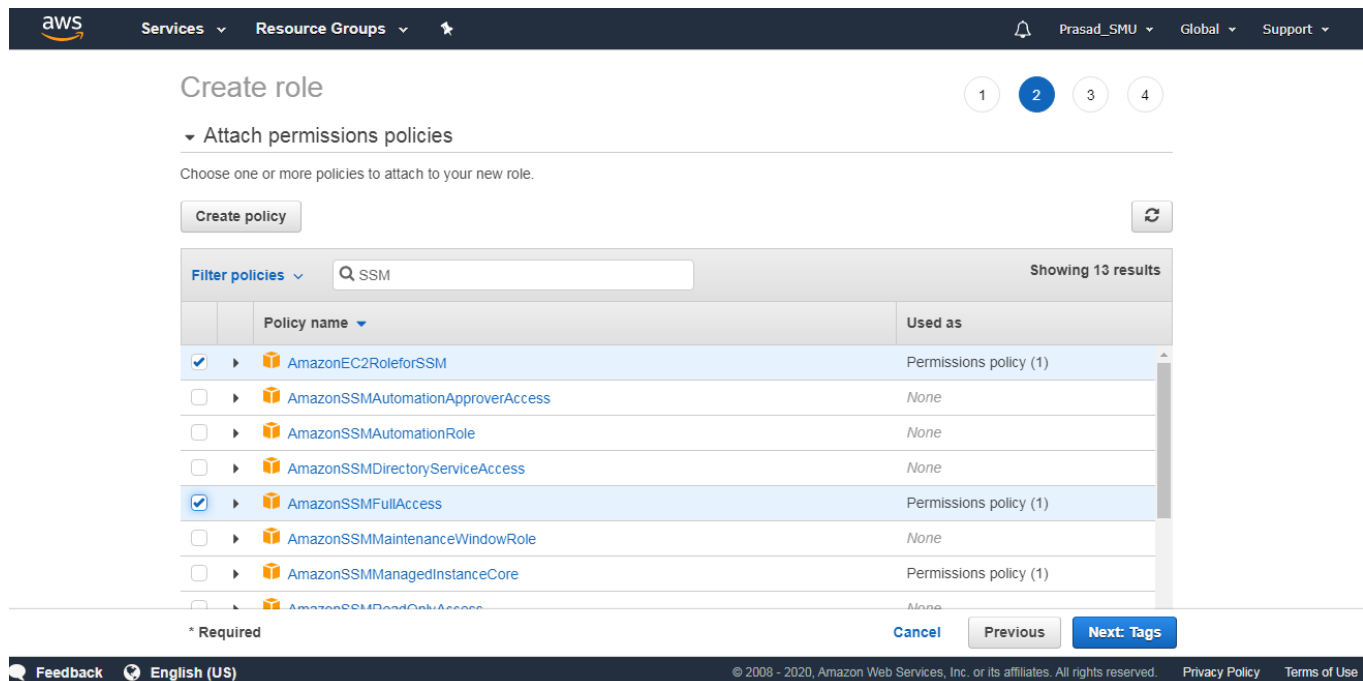
API Gateway	CodeDeploy	EMR	KMS	RoboMaker
AWS Backup	CodeGuru	ElastiCache	Kinesis	S3

* Required

Cancel **Next: Permissions**

Select the below two Default IAM Policies:

1. **AmazonEC2RoleforSSM**
2. **AmazonSSMFullAccess**
3. **AmazonEC2FullAccess**




Create role

1 2 3 4

▼ Attach permissions policies

Choose one or more policies to attach to your new role.

Create policy 

Filter policies Showing 13 results

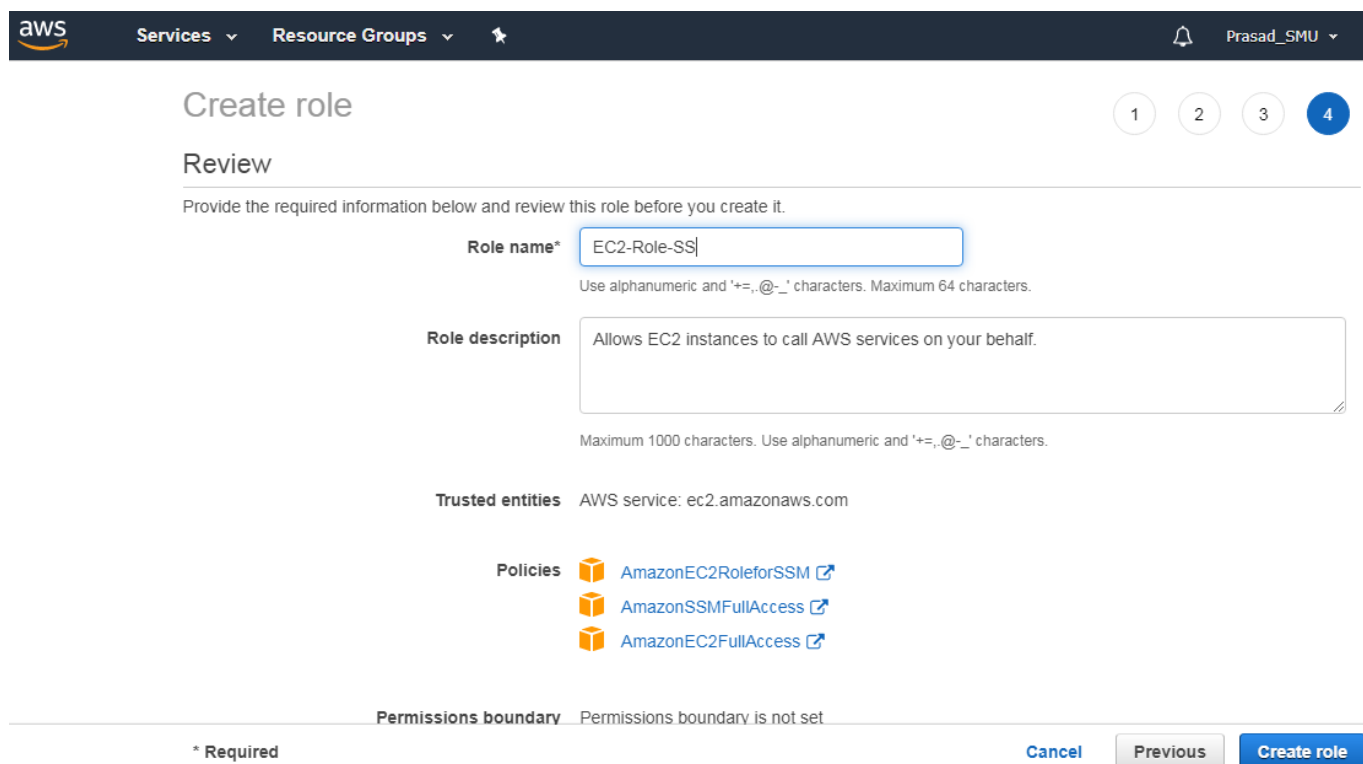
	Policy name	Used as
<input checked="" type="checkbox"/>	AmazonEC2RoleforSSM	Permissions policy (1)
<input type="checkbox"/>	AmazonSSMAutomationApproverAccess	None
<input type="checkbox"/>	AmazonSSMAutomationRole	None
<input type="checkbox"/>	AmazonSSMDirectoryServiceAccess	None
<input checked="" type="checkbox"/>	AmazonSSMFullAccess	Permissions policy (1)
<input type="checkbox"/>	AmazonSSMMaintenanceWindowRole	None
<input type="checkbox"/>	AmazonSSManagedInstanceCore	Permissions policy (1)
<input type="checkbox"/>	AmazonSSMDocOnlyAccess	None

* Required

Cancel Previous **Next: Tags**

Feedback English (US) © 2008 - 2020, Amazon Web Services, Inc. or its affiliates. All rights reserved. Privacy Policy Terms of Use

Give the Role Name as per your Choice and click on Create Role.



Create role

1 2 3 4

Review

Provide the required information below and review this role before you create it.

Role name*
Use alphanumeric and '+,=, @, _' characters. Maximum 64 characters.

Role description
Maximum 1000 characters. Use alphanumeric and '+,=, @, _' characters.

Trusted entities AWS service: ec2.amazonaws.com

Policies

- AmazonEC2RoleforSSM
- AmazonSSMFullAccess
- AmazonEC2FullAccess

Permissions boundary Permissions boundary is not set

* Required

Cancel Previous **Create role**

Task 2: Launch & Configure EC2 Instances with SSM Agent

Login to the AWS Management Console.

Navigate to EC2 Service and click on Launch Instance.

Select the **Amazon Linux AMI**.

Step 1: Choose an Amazon Machine Image (AMI)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

Search for an AMI by entering a search term e.g. "Windows"

Quick Start

- My AMIs
- AWS Marketplace
- Community AMIs
- ☐ Free tier only

Amazon Linux 2 AMI (HVM), SSD Volume Type - ami-0323c3dd2da7fb37d (64-bit x86) / ami-0ce2e5b7d27317779 (64-bit Arm)

Amazon Linux 2 comes with five years support. It provides Linux kernel 4.14 tuned for optimal performance on Amazon EC2, systemd 219, GCC 7.3, Glibc 2.26, Binutils 2.29.1, and the latest software packages through extras.

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

Amazon Linux AMI 2018.03.0 (HVM), SSD Volume Type - ami-0915e09cc7ceee3ab

The Amazon Linux AMI is an EBS-backed, AWS-supported image. The default image includes AWS command line tools, Python, Ruby, Perl, and Java. The repositories include Docker, PHP, MySQL, PostgreSQL, and other packages.

Root device type: ebs Virtualization type: hvm ENA Enabled: Yes

Select the Number of Instances as 1, select the Network as our Custom VPC, Select Subnet as Public Subnet 1 and select the IAM Role which you configured in the Task 1.

Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances 1 [Launch into Auto Scaling Group](#)

Purchasing option ☐ Request Spot instances

Network vpc-062814d035612343e | Custom VPC [Create new VPC](#)

Subnet subnet-01ee44283bcd09e5c | Public Subnet 1 | us-e [Create new subnet](#)
245 IP Addresses available

Auto-assign Public IP Use subnet setting (Enable)

Placement group ☐ Add instance to placement group

Capacity Reservation Open [Create new Capacity Reservation](#)

IAM role EC2-Role-SSM [Create new IAM role](#)

Since AWS Systems Manager is AGENTLESS, we need to install Packages for Systems Manager (SSM) to connect with Target Instances.

Scroll down on the same page, click on Advanced Details and in User Data field bootstrap the below commands.

I've provided the Commands in text file.

▼ Advanced Details

Metadata accessible	<input type="text" value="Enabled"/>
Metadata version	<input type="text" value="V1 and V2 (token optional)"/>
Metadata token response hop limit	<input type="text" value="1"/>
User data	<input checked="" type="radio"/> As text <input type="radio"/> As file <input type="checkbox"/> Input is already base64 encoded

```
#!/bin/bash
cd /tmp
sudo yum install -y https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/latest/linux_amd64/amazon-ssm-agent.rpm
sudo systemctl start amazon-ssm-agent
sudo systemctl enable amazon-ssm-agent
```

You can mention Tags as per your choice.

Services ▼ Resource Groups ▼

Prasad_SMU ▼ N. Virginia ▼ Support ▼

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 5: Add Tags

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver.
A copy of a tag can be applied to volumes, instances or both.
Tags will be applied to all instances and volumes. [Learn more](#) about tagging your Amazon EC2 resources.

Key (128 characters maximum)	Value (256 characters maximum)	Instances	Volumes
Name	EC2-Amazon Inspector	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Add another tag (Up to 50 tags maximum)

Click Next: Security Groups.

Create a new Security Group. Give the Name & Discription as per your choice. Allow SSH, HTTPS, HTTP Inbound traffic from Anywhere.

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
HTTP	TCP	80	Anywhere (0.0.0.0/0, :::/0)	e.g. SSH for Admin Desktop

[Add Rule](#)

Warning

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

Click on Review and Launch.

Select the existing Key Pair which you've using for previous labs.

Click on Launch Instances.

Step 7: Review Instance Launch

Please review your instance launch details. You can [Edit security groups](#) or [Edit AMI](#).

AMI Details

Red Hat Enterprise Linux 8 (H)
 Free tier eligible
 Red Hat Enterprise Linux version 8 (H)
 Root Device Type: ebs Virtualization type: x86_64

Instance Type

Instance Type	ECUs
t2.micro	Variable

Network Performance

Low to Moderate

Select an existing key pair or create a new key pair

A key pair consists of a **public key** that AWS stores, and a **private key file** that you store. Together, they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to securely SSH into your instance.

Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about [removing existing key pairs from a public AMI](#).

Choose an existing key pair
 Select a key pair
 LinuxServer

☒ I acknowledge that I have access to the selected private key file (LinuxServer.pem), and that without this file, I won't be able to log into my instance.

[Cancel](#) [Launch Instances](#)

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

You can see that the Highlighted Instance has been launched Successfully!!!!

Instances Table:

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)
	i-04d960bbddffc81ee	t2.micro	us-east-1d	running	2/2 checks ...	None	ec2-3-90-163-174.com...
	i-05308de4d1fe34b24	t2.micro	us-east-1a	running	2/2 checks ...	None	ec2-54-196-114-17.co...
	i-056010c787acae7db	t2.micro	us-east-1a	running	2/2 checks ...	None	ec2-3-89-202-180.com...
	i-06fc6c6f2400143e8	t2.micro	us-east-1a	running	2/2 checks ...	None	
EC2-Amazo...	i-0a25233378569135c	t2.micro	us-east-1a	running	2/2 checks ...	None	ec2-54-165-239-253.co...

Instance Details: i-0a25233378569135c (EC2-Amazon Inspector)

Public DNS: ec2-54-165-239-253.compute-1.amazonaws.com

Description

Instance ID	i-0a25233378569135c	Public DNS (IPv4)	ec2-54-165-239-253.compute-1.amazonaws.com
Instance state	running	IPv4 Public IP	54.165.239.253
Instance type	t2.micro	IPv6 IPs	-
Finding	Opt-in to AWS Compute Optimizer for recommendations. Learn more	Elastic IPs	
Private DNS	ip-10-192-10-197.ec2.internal	Availability zone	us-east-1a
Private IPs	10.192.10.197	Security groups	RHEL8-SG, view inbound rules , view outbound rules

Task 3: AWS Systems Manager: Managed Instances

Navigate to AWS Systems Manager Service.

AWS Systems Manager

MANAGEMENT TOOLS

AWS Systems Manager

Gain Operational Insight and Take Action on AWS Resources.

[Get Started with Systems Manager](#)

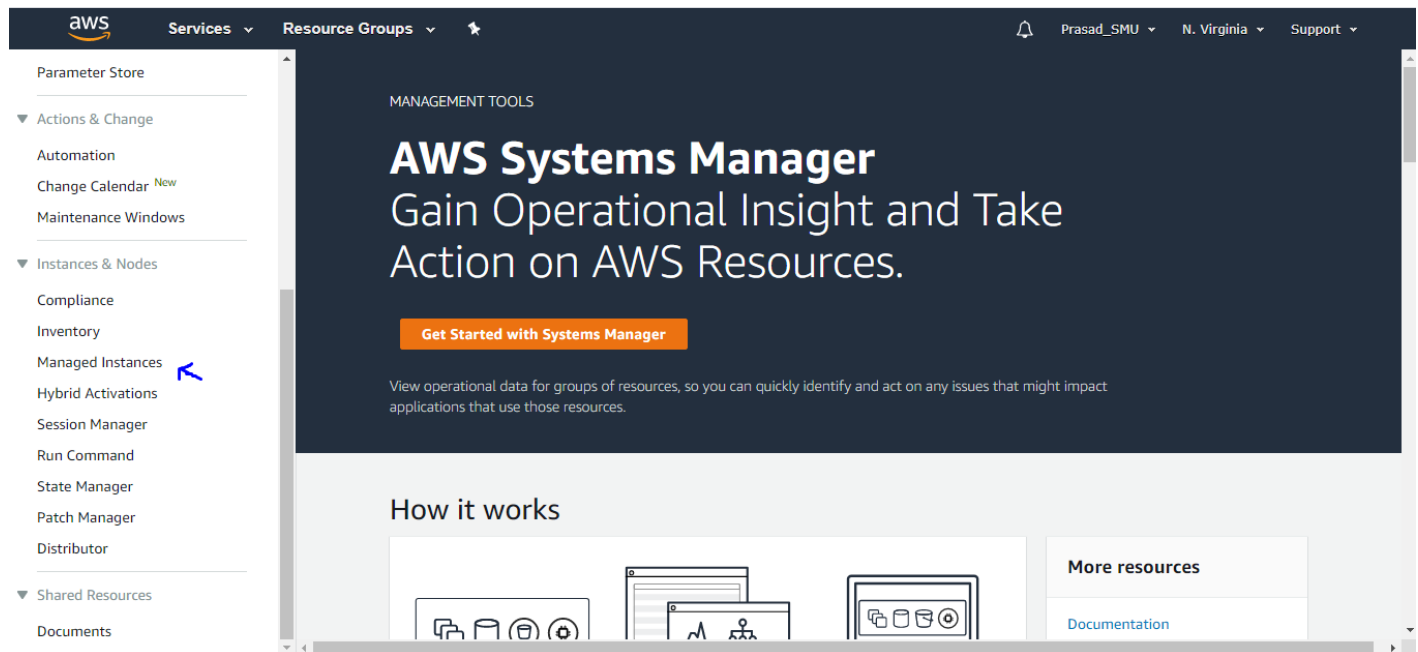
View operational data for groups of resources, so you can quickly identify and act on any issues that might impact applications that use those resources.

How it works

More resources

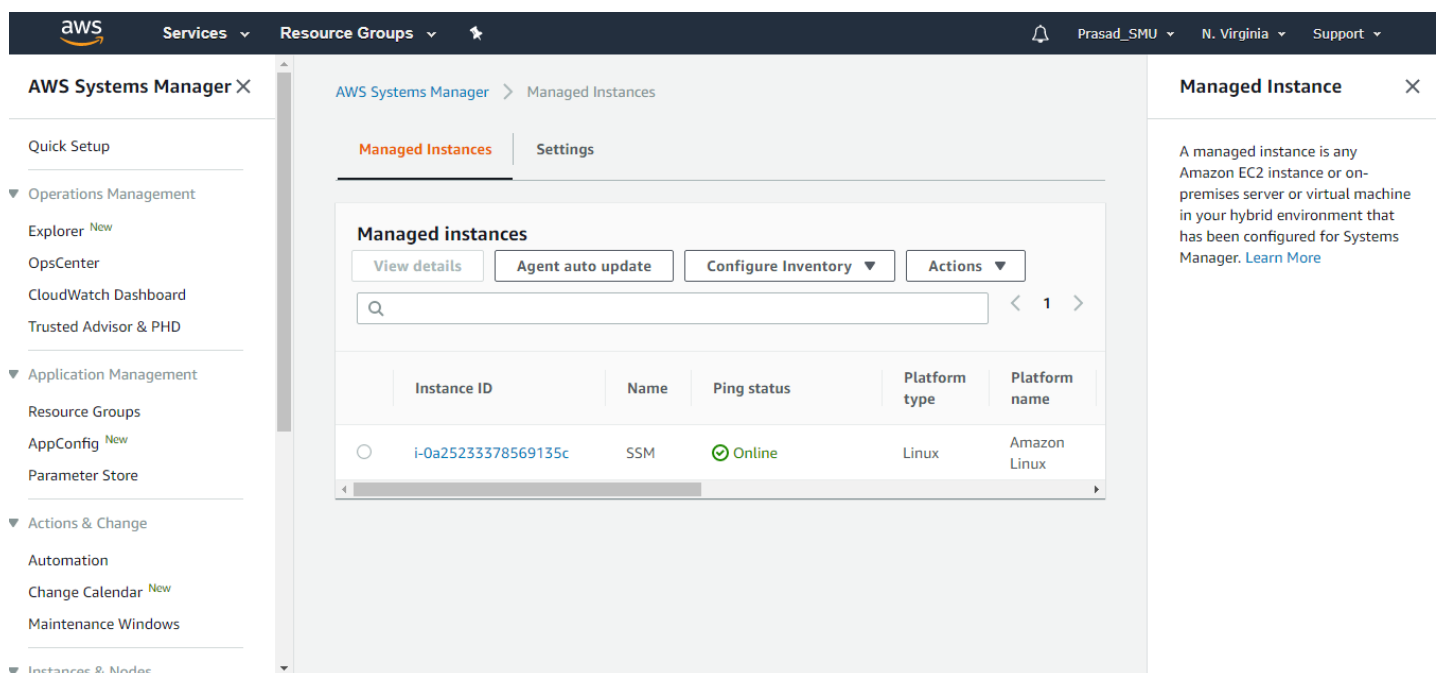
[Documentation](#)

One the left-hand side, click on Managed Instances.



You should see the Instance which we launched in Task 2.

If you do not see any Instance in Managed Instances tab, it means Systems Manager Agent is not Installed on the EC2 Instance.



You can also verify the Instance IDs from EC2 Service Dashboard.

aws Services Resource Groups

Prasad_SMU N. Virginia Support

New EC2 Experience Tell us what you think

EC2 Dashboard **New**

Events **New**

Tags

Reports

Limits

▼ INSTANCES

Instances

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts **New**

Scheduled Instances

Capacity Reservations

▼ IMAGES

AMIs

Launch Instance Connect Actions

Filter by tags and attributes or search by keyword

Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)
	i-04d960bbddffc81ee	t2.micro	us-east-1d	running	2/2 checks ...	None	ec2-3-90-163-174.com...
	i-05308de4d1fe34b24	t2.micro	us-east-1a	running	2/2 checks ...	None	ec2-54-196-114-17.co...
	i-056010c787acae7db	t2.micro	us-east-1a	running	2/2 checks ...	None	ec2-3-89-202-180.com...
	i-06fc6c6f2400143e8	t2.micro	us-east-1a	running	2/2 checks ...	None	
EC2-Amazo...	i-0a25233378569135c	t2.micro	us-east-1a	running	2/2 checks ...	None	ec2-54-165-239-253.co...

Instance: **i-0a25233378569135c (EC2-Amazon Inspector)** Public DNS: **ec2-54-165-239-253.compute-1.amazonaws.com**

Description Status Checks Monitoring Tags

Instance ID i-0a25233378569135c

Instance state running

Instance type t2.micro

Finding Opt-in to AWS Compute Optimizer for recommendations. [Learn more](#)

Private DNS ip-10-192-10-197.ec2.internal

Private IPs 10.192.10.197

Public DNS (IPv4) ec2-54-165-239-253.compute-1.amazonaws.com

IPv4 Public IP 54.165.239.253

IPv6 IPs -

Elastic IPs

Availability zone us-east-1a

Security groups [RHEL8-SG](#) [view inbound rules](#) [view outbound rules](#)

Task 4: Amazon Inspector Configurations

Navigate to Amazon Inspector Service.

aws Services Resource Groups

Prasad_SMU N. Virginia Support

Amazon Inspector

Amazon Inspector enables you to analyze the behavior of your AWS resources and helps you identify potential security issues.

[Get started](#)

Install

Install the AWS agent on your EC2 instances.

Run

Run an assessment for your assessment target.

Analyze

Review your findings and remediate security issues.

Go ahead and click on Get Started. Click on Advanced 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



Give the Assessment Target Name as per your choice.

Unselect the All Instances and specify Tag of your EC2 Instance.

Check on Install Agents. Amazon Inspector will now Install Amazon Inspector Agent on Target Instances using Systems Manager Service-Run Command.

Services

Resource Groups

Prasad_SMU

N. Virginia

Support

Get started with Amazon Inspector

Step 1: Define an assessment target
Step 2: Define an assessment template
Step 3: Review

Define an assessment target

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

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](#)

Tags*

Key	Value
Name	EC2-Amazon Inspector
Add a new key	

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

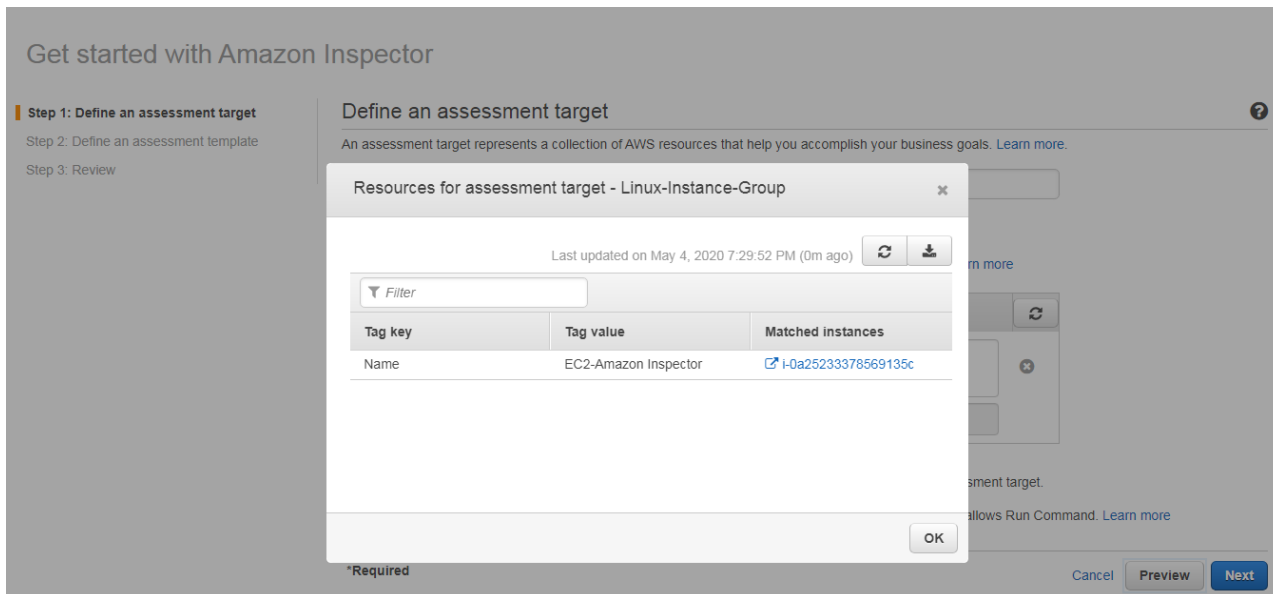
To use this option, make sure that your EC2 instances have the SSM Agent installed and an IAM role that allows Run Command. [Learn more](#)

*Required

Cancel Preview Next

Click on Preview. You should see the Instance which you've configured in Task 2.

You can also verify the Instance ID from the EC2 Service Dashboard.



Click on Next.

Give the Assessment Template Name as CVE-Template.

Remove all the existing Rule Packages & from the dropdown select the **Common Vulnerabilities and Exposure-1.1** Rule Package.

Set the scan duration to 15 Minutes. Amazon Inspector will scan the Target Instances for every 15 Minutes to detect the Vulnerabilities.

You can also set up the recurring schedule if you want. Click Next.

Get started with Amazon Inspector

Step 1: Define an assessment target

Step 2: Define an assessment template

Step 3: Review

Define an assessment template

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.](#)

Name* CVE-Template

Rules packages* Common Vulnerabilities and Exposures-1.1

Select an Inspector rules package

Amazon Inspector runs assessments for the assessment target against selected rules package(s). [Learn more.](#)

Duration* 15 Minutes

The default Amazon Inspector assessment template duration is 1 hour. You can modify the duration, but note that assessment templates with longer durations can deliver fuller sets of findings.

Assessment Schedule ☐ Set up recurring assessment runs once every 7 days. The first run starts on create. [Learn more](#)

*Required

Cancel Previous Next

Finally review the configurations and click on Create.

Assessment has been deployed successfully.

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 May 4, 2020 7:39:47 PM (0m ago)

Filter

	Start time	Status	Template name	Findings	Findings by s...	Exclusions	Reports
<input type="checkbox"/>	Today at 7:39 P...	Collecting data	CVE-Template	0		0	

Click and expand the current Assessment.

You'll notice that the Scanning for the Vulnerabilities on the EC2 Instance has been started automatically. You can see the scanning Status as **Collecting Data**.

The entire scanning process will take approximately 15-30 Minutes.

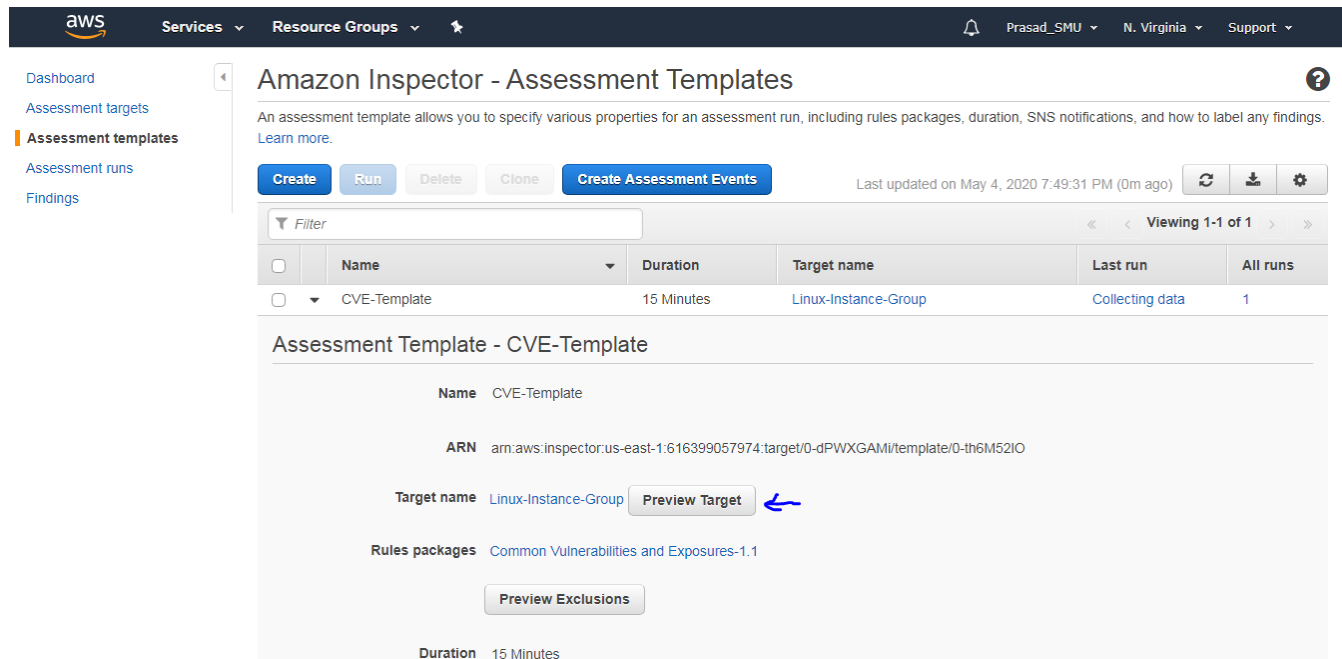
The screenshot displays the AWS Inspector 'Assessment runs' page. At the top, there are buttons for 'Run', 'Cancel', and 'Delete'. A status bar indicates 'Last updated on May 4, 2020 7:41:45 PM (0m ago)'. Below this is a table with columns: Start time, Status, Template name, Findings, Findings by s..., Exclusions, and Reports. A single row is visible with the status 'Collecting data' highlighted by a blue arrow. Below the table, the details for the assessment run 'Assessment - Run - CVE-Template - 2020-05-05T00:39:35.743Z' are shown. These details include: ARN (arn:aws:inspector:us-east-1:616399057974:target/0-dPWXGAMi/template/0-th6M52IO/run/0-YtvFAe6e), Start time (Today at 7:39 PM (GMT-5) (2 minutes ago)), Target name (Linux-Instance-Group), Template name (CVE-Template), Rules packages (Common Vulnerabilities and Exposures-1.1), Duration (15 Minutes), Status (Collecting data, highlighted by a blue arrow), and Findings (0). At the bottom, there are buttons for 'Show AWS agents' and 'Show status'.

Task 5: Amazon Inspector-Troubleshooting

In some cases, the Inspector Agent may not get installed on the Target Instances successfully. In-such cases, if you Run the Scanning Process, you may get the below error message.



In this case, on the right-hand side, click on Assessment Template. Expand the Assessment Template and click on Preview Targets.



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 May 4, 2020 7:49:31 PM (0m ago) [Refresh](#) [Download](#) [Settings](#)

Viewing 1-1 of 1

<input type="checkbox"/>	Name	Duration	Target name	Last run	All runs
<input type="checkbox"/>	CVE-Template	15 Minutes	Linux-Instance-Group	Collecting data	1

Assessment Template - CVE-Template

Name CVE-Template

ARN [arn:aws:inspector:us-east-1:616399057974:target/0-dPWXGAMi/template/0-th6M52IO](#)

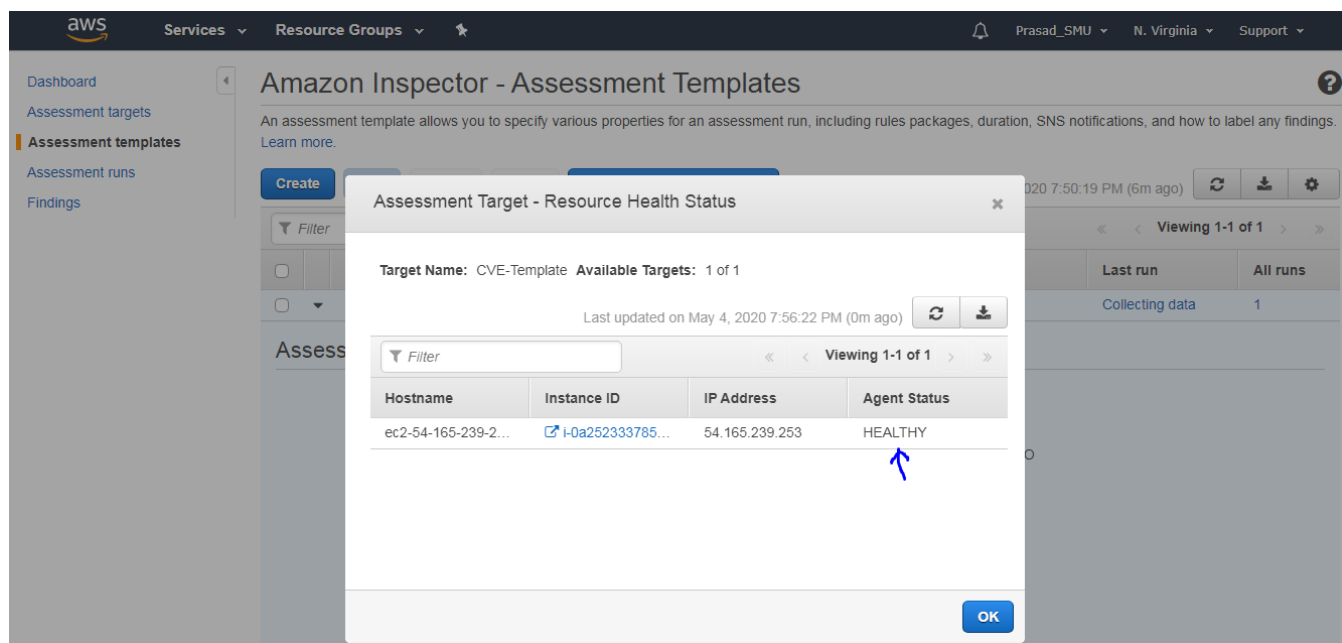
Target name [Linux-Instance-Group](#) [Preview Target](#)

Rules packages [Common Vulnerabilities and Exposures-1.1](#)

[Preview Exclusions](#)

Duration 15 Minutes

Agent Status is currently Healthy, you do not have to worry about it.



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.](#)

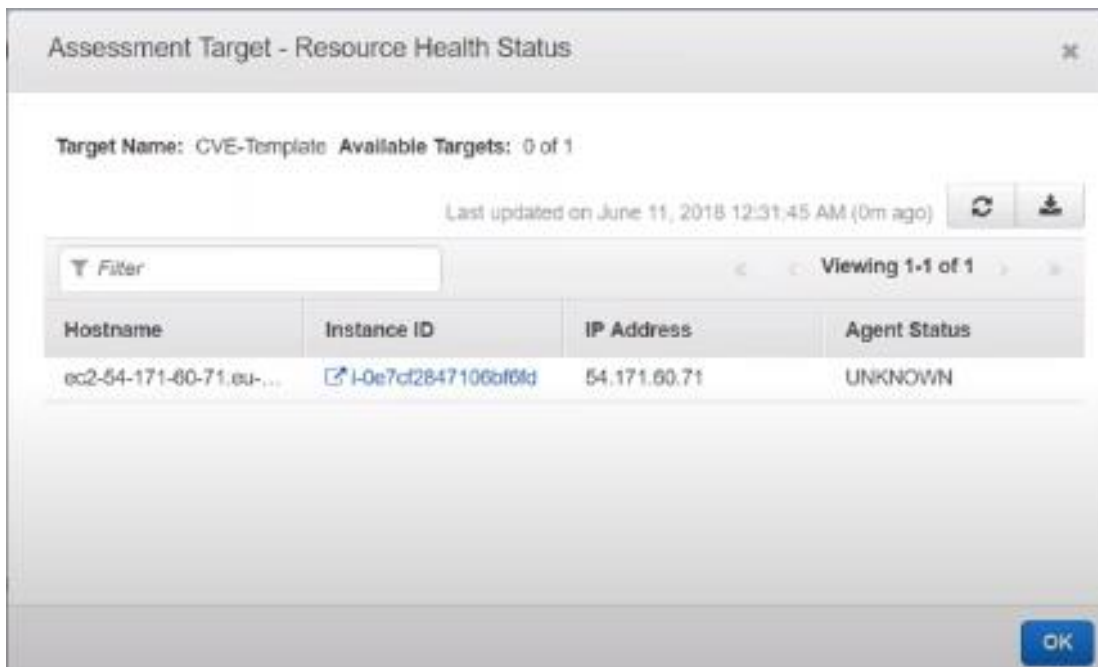
[Create](#) [Run](#) [Delete](#) [Clone](#) [Create Assessment Events](#) Last updated on May 4, 2020 7:50:19 PM (6m ago) [Refresh](#) [Download](#) [Settings](#)

Viewing 1-1 of 1

Hostname	Instance ID	IP Address	Agent Status
ec2-54-165-239-2...	i-0a252333785...	54.165.239.253	HEALTHY

[OK](#)

But in-case of above error, the Agent Status will be Unknown.

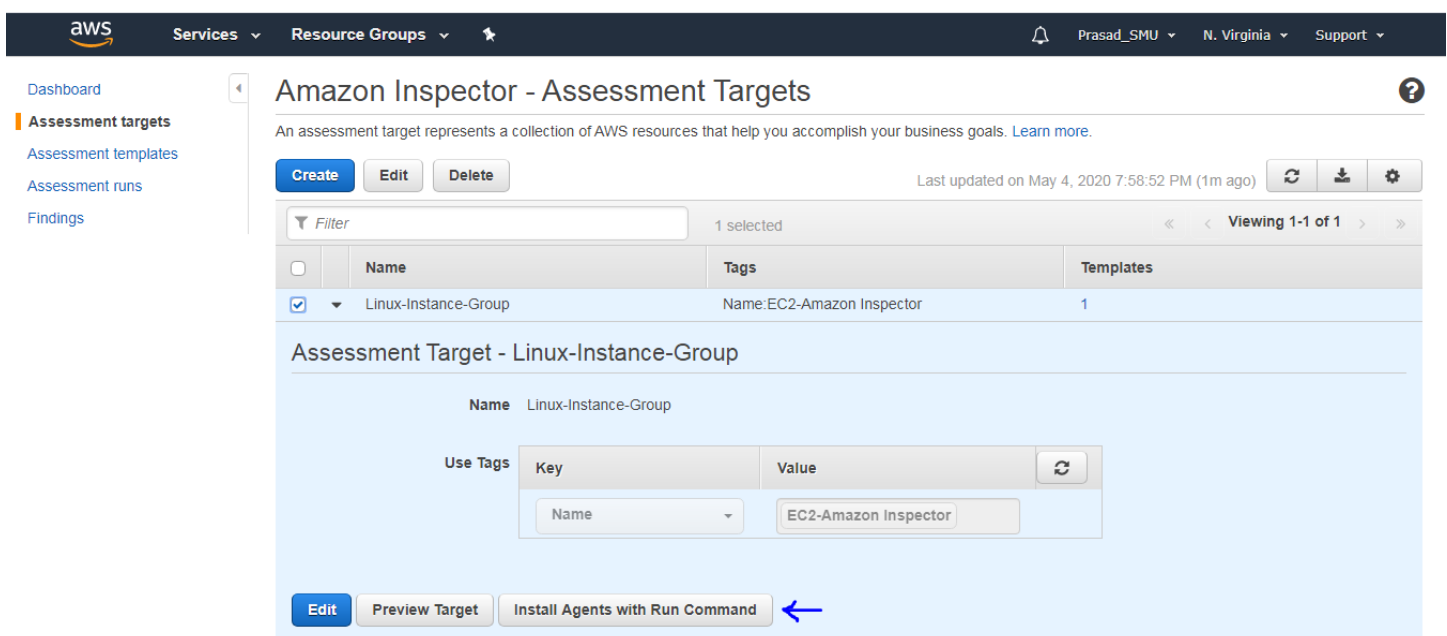


If the Agent Status is Unknown, then it is possible to Install the Inspector Agent Remotely on the EC2 Instances.

On right-hand side. Click on Assessment Targets.

Select the Assessment Target and click on **Install Agents with Run Command**.

This will Install the Amazon Inspector Agent on EC2 Instances remotely.



Now if you navigate to AWS Systems Manager Service, click on Run Command and click on Command History, you'll observe the Command has been executed successfully.

The screenshot shows the AWS Systems Manager console. On the left, the 'AWS Systems Manager' sidebar is visible with a blue arrow pointing to the 'Command history' link under the 'Commands' section. The main content area shows the 'Command history' tab selected. A table lists command execution details:

Command ID	Status	Request ed date	Document name	Comment	# targets	# error	# delin time out
45bbe31b-d0a5-4511-ba51-4244cce71c52	Success	Tue, 05 May 2020 01:02:01 GMT	AmazonInspector-ManageAWSAgent		1	0	0

Now if you click on Assessment Template, expand the Assessment Template and click on Preview Targets, the Agent Status will be HEALTHY.

Now again click on Assessment Templates.

Select the Template and click on Run.

The screenshot shows the 'Amazon Inspector - Assessment Templates' page. A blue arrow points to the 'Run' button. Below the buttons, a table lists the available assessment templates:

Name	Duration	Target name	Last run	All runs
CVE-Template	15 Minutes	Linux-Instance-Group	Analysis complete	1

Scanning Process will get started.

The screenshot shows the 'Amazon Inspector - Assessment Runs' page. A table lists the active assessment runs:

Start time	Status	Template name	Findings	Findings by s...	Exclusions	Reports
Today at 7:39 P...	Collecting data	CVE-Template	0		0	

Task 6: Amazon Inspector-Findings

Now you can see that the Assessment analysis has been completed.

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 May 4, 2020 8:12:33 PM (0m ago) [Refresh](#) [Download](#) [Settings](#)

Filter

	Start time	Status	Template name	Findings	Findings by s...	Exclusions	Reports
<input type="checkbox"/>	Today at 7:39 P...	Analysis complete	CVE-Template	0	High Medium ...	0	Download re...

You can download the Vulnerability Report if you want.

Now click on Findings.

You'll observe the list of Vulnerability exists in your EC2 Instance.

I do not have any findings for my EC2 Instance, it means my EC2 Instance is 0% vulnerable and highly secured.

Amazon Inspector - Findings

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

[Add/Edit attributes](#) Last updated on May 4, 2020 8:20:23 PM (0m ago) [Refresh](#) [Download](#) [Settings](#)

Filter

	Severity	Date	Finding	Target	Template	Rules Pac
No Results						

Max records per page: 25 [* refresh browser to reflect change](#)

Below is the list of Findings & example of Amazon Inspector Finding which provides Description of the Vulnerability and Steps or recommendations to remove the **Vulnerability**.

Amazon Inspector - Findings ?

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

[Add/Edit attributes](#) Last updated on June 11, 2018 12:26:06 AM (7m ago) ↺ ⬇ ⚙

Viewing 1-10 of 10

<input type="checkbox"/>	Severity ⓘ	Date	Finding	Target	Template	Rules Package
<input type="checkbox"/>	High	Today at 12:...	Instance i-00c9fb87895e81f7d is vulnerable to CV...	Latest-Assessment	CVE-Assessment-...	Common Vulne
<input type="checkbox"/>	High	Today at 12:...	Instance i-00c9fb87895e81f7d is vulnerable to CV...	Latest-Assessment	CVE-Assessment-...	Common Vulne
<input type="checkbox"/>	High	Today at 12:...	Instance i-00c9fb87895e81f7d is vulnerable to CV...	Latest-Assessment	CVE-Assessment-...	Common Vulne
<input type="checkbox"/>	High	Today at 12:...	Instance i-00c9fb87895e81f7d is vulnerable to CV...	Latest-Assessment	CVE-Assessment-...	Common Vulne
<input type="checkbox"/>	Medium	Today at 12:...	Instance i-00c9fb87895e81f7d is vulnerable to CV...	Latest-Assessment	CVE-Assessment-...	Common Vulne
<input type="checkbox"/>	Medium	Today at 12:...	Instance i-00c9fb87895e81f7d is vulnerable to CV...	Latest-Assessment	CVE-Assessment-...	Common Vulne
<input type="checkbox"/>	Medium	Today at 12:...	Instance i-00c9fb87895e81f7d is vulnerable to CV...	Latest-Assessment	CVE-Assessment-...	Common Vulne
<input type="checkbox"/>	Medium	Today at 12:...	Instance i-00c9fb87895e81f7d is vulnerable to CV...	Latest-Assessment	CVE-Assessment-...	Common Vulne
<input type="checkbox"/>	Medium	Today at 12:...	Instance i-00c9fb87895e81f7d is vulnerable to CV...	Latest-Assessment	CVE-Assessment-...	Common Vulne
<input type="checkbox"/>	Medium	Today at 12:...	Instance i-00c9fb87895e81f7d is vulnerable to CV...	Latest-Assessment	CVE-Assessment-...	Common Vulne

Amazon Inspector - Findings ?

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

[Add/Edit attributes](#) Last updated on June 11, 2018 12:26:06 AM (7m ago) ↺ ⬇ ⚙

Viewing 1-10 of 10

<input type="checkbox"/>	Severity ⓘ	Date	Finding	Target	Template	Rules Package
<input type="checkbox"/>	High	Today at 12:...	Instance i-00c9fb87895e81f7d is vulnerable to CV...	Latest-Assessment	CVE-Assessment-...	Common Vulne

Finding for assessment target 'Latest-Assessment' and template 'CVE-Assessment-Template'

ARN [arn:aws:inspector:eu-central-1:579807160478:target/0-CSxvLZm2/template/0-pFkcnkk3/run/0-n3njZG9N/finding/0-AounH0RJ](#)

Run name [Run - CVE-Assessment-Template - 2018-06-10T22:02:47.574Z](#)

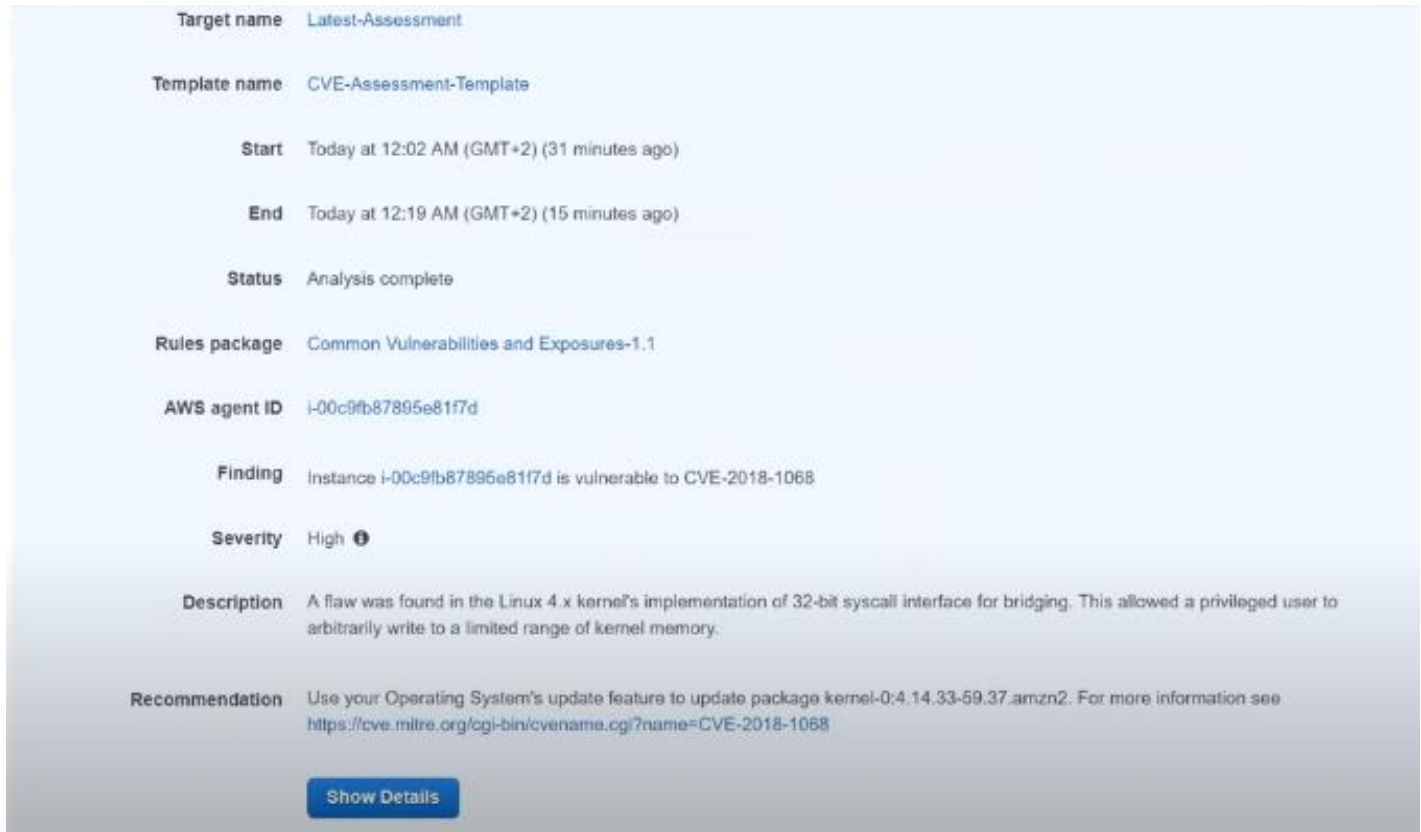
Target name [Latest-Assessment](#)

Template name [CVE-Assessment-Template](#)

Start Today at 12:02 AM (GMT+2) (31 minutes ago)

End Today at 12:19 AM (GMT+2) (15 minutes ago)

Status Analysis complete



The screenshot displays the AWS Inspector findings interface. It shows a list of findings for the target 'Latest-Assessment' using the 'CVE-Assessment-Template'. The finding is for CVE-2018-1068, which is a high-severity vulnerability in the Linux 4.x kernel's syscalls interface. The description states that a privileged user could write to kernel memory. The recommendation is to update the kernel package to version 0:4.14.33-59.37.amzn2. A 'Show Details' button is located at the bottom of the finding card.

Target name	Latest-Assessment
Template name	CVE-Assessment-Template
Start	Today at 12:02 AM (GMT+2) (31 minutes ago)
End	Today at 12:19 AM (GMT+2) (15 minutes ago)
Status	Analysis complete
Rules package	Common Vulnerabilities and Exposures-1.1
AWS agent ID	i-00c9fb87895e81f7d
Finding	Instance i-00c9fb87895e81f7d is vulnerable to CVE-2018-1068
Severity	High ⓘ
Description	A flaw was found in the Linux 4.x kernel's implementation of 32-bit syscall interface for bridging. This allowed a privileged user to arbitrarily write to a limited range of kernel memory.
Recommendation	Use your Operating System's update feature to update package kernel-0:4.14.33-59.37.amzn2. For more information see https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-1068

Show Details

This completes the Lab on AWS Security-AWS Inspector.

For questions. Contact me on pbhavsar@smu.edu .