



AWS  
re:Start  
LAB

# Network Hardening



**WEEK 4**





# Overview

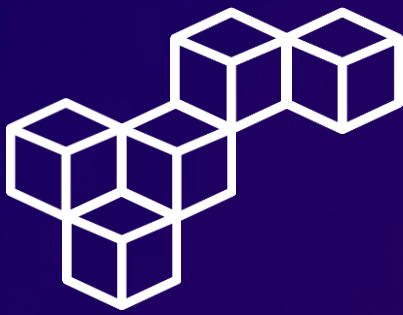
---

Securing an infrastructure can be a challenge for any company. Companies use many tools to audit networks and find vulnerabilities in systems and applications. This process takes significant time and effort.

In this lab, you are a new security engineer for AnyCompany. You need to identify weak areas in the company's network security and update AnyCompany's environment for better efficiency and optimization. You will use Amazon Inspector to do this.

**Amazon Inspector** runs scans that analyze all your network configurations—such as security groups, network access control lists (network ACLs), route tables, and internet gateways—together to infer reachability. You don't need to send packets across the virtual private cloud (VPC) network or connect to Amazon Elastic Compute Cloud (Amazon EC2) instance network ports. It's like packetless network mapping and reconnaissance.

From Amazon Inspector, you will use the **network reachability package** to analyze your network configurations to find security vulnerabilities in your EC2 instances. The findings that Amazon Inspector generates also provide guidance about restricting access that is not secure.

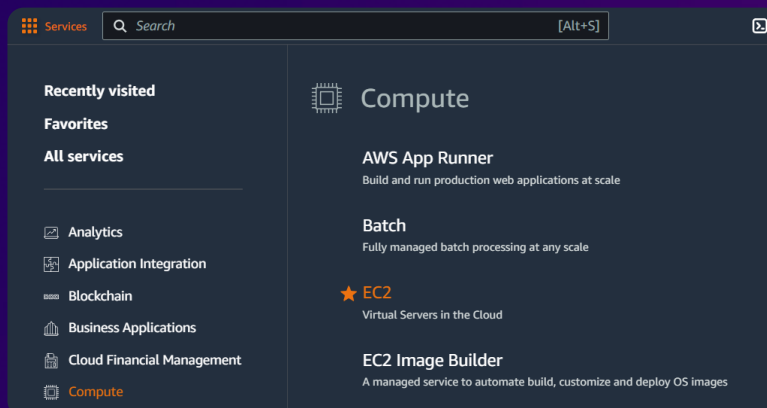


# Task 1

## View EC2 instances and add tags

### Step 1: Access the EC2 Management Console

Open the AWS Management Console, and select EC2.



### Step 2: Review running instances

Navigate to the **Instances** section. The running BastionServer and AppServer EC2 instances are listed.

Instances (2) Info

Find Instance by attribute or tag (case-sensitive)

All states

< 1 > ⚙

Connect

Instance state

Actions

Launch instances

<input type="checkbox"/>	Name	Instance ID	Instance state	Status check	Availability Zone	Public IPv4 ...	Security group name
<input type="checkbox"/>	BastionServer	i-0871a0c91e93a7996	<span>Running</span>	<span>2/2 checks passed</span>	us-west-2a	54.202.172.54	c117085a27900861646...
<input type="checkbox"/>	AppServer	i-0d4e329c3ec0c5df3	<span>Running</span>	<span>2/2 checks passed</span>	us-west-2a	35.160.239.71	c117085a27900861646...

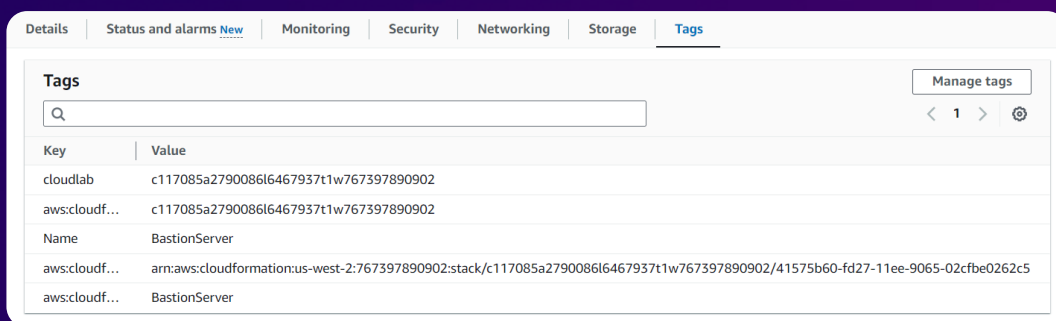


# Task 1

## View EC2 instances and add tags

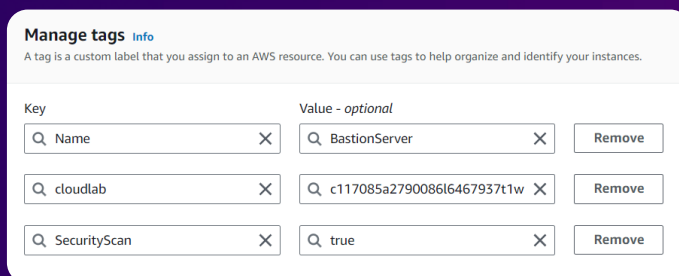
### Step 3: Manage instance tags

Select the BastionServer instance and go to the **Tags** tab, then select [Manage tags](#).



### Step 4: Add a tag to an instance

Add a new tag with the key [SecurityScan](#) and the value [true](#).



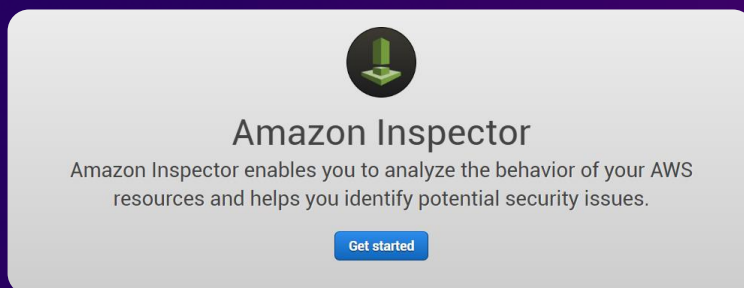


# Task 2

## Configure and run Amazon Inspector

### Step 1: Access Amazon Inspector Classic

On the AWS Management Console, navigate to the **Amazon Inspector** service, choose [Switch to Inspector Classic](#), click on [Get started](#) and select [Advanced setup](#).



### Step 2: Define an assessment target

In the **Define an assessment target** section, configure the following options.

Define an assessment target

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

Name\*

Network-Audit

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
SecurityScan	true

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](#)



# Task 2

## Configure and run Amazon Inspector

### Step 3: Define an assessment template

In the **Define an assessment template** section, configure the following options.

#### 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\***

**Rules packages\***  ✕

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

**Duration\***

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  days. The first run starts on create. [Learn more](#)

### Step 4: Create the assessment

Review the setup and choose [Create](#). Once the Assessment Run status changes to Analysis complete, go to **Findings**.

# 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 April 17, 2024 6:23:36 PM (0m ago)

?

↺

⬇️

⚙️

▼ Filter

«

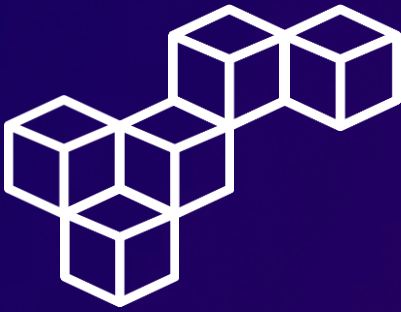
<

Viewing 1-1 of 1

>

»

<input type="checkbox"/>	Start time	Status	Template name	Findings	Findings by severity	Exclusions	Reports
<input type="checkbox"/>	▶ Today at 6:22 PM (G...	Analysis complete	Assessment-Templ...	3	High   Medium   Low...	2	📄 Download report



# Task 3

## Analyze Amazon Inspector findings

### Review the high-severity finding

Expand the high-severity finding and review key details.

High

Today ...

On instance i-0871a0c91e93a7996, TCP port 23 w...

Network-Audit

Assessment-Temp...

Network Reachability-1.1

AWS agent ID

i-0871a0c91e93a7996

Finding

On instance i-0871a0c91e93a7996, TCP port 23 which is associated with 'Telnet' is reachable from the internet

Description

On this instance, TCP port 23, which is associated with Telnet, 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-0871a0c91e93a7996 is located in VPC vpc-0da2cfb0cbfa60012 and has an attached ENI eni-00b8c28e15358dee1 which uses network ACL acl-0942d0d37042ee103. The port is reachable from the internet through Security Group sg-0179ad25f9f7858f5 and IGW igw-043f31e0a82e29bca

Recommendation

You can edit the Security Group sg-0179ad25f9f7858f5 to remove access from the internet on port 23

### Review the medium-severity finding

Expand the medium-severity finding and review key details.

Medium

Today ...

On instance i-0871a0c91e93a7996, TCP port 22 w...

Network-Audit

Assessment-Temp...

Network Reachability-1.1

AWS agent ID

i-0871a0c91e93a7996

Finding

On instance i-0871a0c91e93a7996, TCP port 22 which is associated with 'SSH' is reachable from the internet

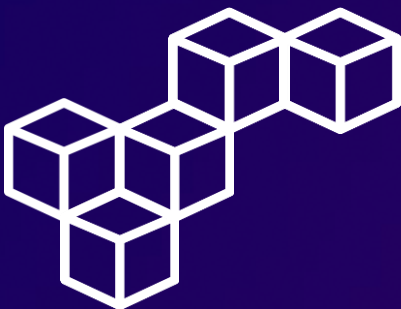
Description

On this instance, TCP port 22, which is associated with SSH, 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-0871a0c91e93a7996 is located in VPC vpc-0da2cfb0cbfa60012 and has an attached ENI eni-00b8c28e15358dee1 which uses network ACL acl-0942d0d37042ee103. The port is reachable from the internet through Security Group sg-0179ad25f9f7858f5 and IGW igw-043f31e0a82e29bca

Recommendation

You can edit the Security Group sg-0179ad25f9f7858f5 to remove access from the internet on port 22





# Task 4

## Update security groups

### Step 1: Follow the Recommendation link

On the high-severity finding, [follow the Recommendation link](#) to the security group attached to the BastionServer instance.

Security Groups (1) [Info](#)

Find resources by attribute or tag

Security group ID = sg-0179ad25f9f7858f5

X

Clear filters

Actions

Export security groups to CSV

Create security group

<input type="checkbox"/>	Name	Security group ID	Security group name	VPC ID	Description
<input type="checkbox"/>	BastionServerSG	<a href="#">sg-0179ad25f9f7858f5</a>	c117085a279008616467937t1w767...	<a href="#">vpc-0da2cfb0cbfa60012</a>	security group

### Step 2: Check current inbound rules

Select the **Inbound rules** tab of the BastionServerSG security group and click on [Edit inbound rules](#).

Inbound rules [Info](#)

Security group rule ID	Type <a href="#">Info</a>	Protocol <a href="#">Info</a>	Port range <a href="#">Info</a>	Source <a href="#">Info</a>	Description - optional <a href="#">Info</a>	
sg-0688aea27f378ce0c	SSH	TCP	22	Cust... <div><div>Q</div><div>0.0.0.0/0 X</div></div>		Delete
sg-006e396390dabeb39	Custom TCP	TCP	23	Cust... <div><div>Q</div><div>0.0.0.0/0 X</div></div>		Delete





# Task 4

## Update security groups

### Step 3: Edit inbound rules

Delete the inbound rule associated with port range 23 and change the Source of the SSH rule to My IP.

Inbound rules

Security group rule ID

Type

Protocol

Port range

Source

Description - optional

sgr-0688aea27f378ce0c

SSH

TCP

22

My IP

Delete

190.117.58.32/32

### Step 4: Re-scan the environment

Re-run the assessment and go to **Findings**. The high-severity finding is now gone, but the medium-severity finding remains.

Amazon Inspector - Findings

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

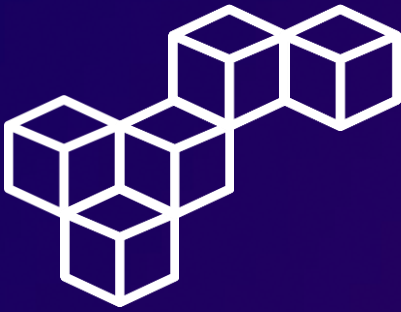
Add/Edit attributes

Last updated on April 17, 2024 6:39:50 PM (1m ago)

Filter

Viewing 1-5 of 5

	Severity	Date	Finding	Target	Template	Rules Package
<input type="checkbox"/>	Informational	Today at 6:39 P...	Aggregate network exposure: On instance i-0871a0...	Network-Audit	Assessment-Temp...	Network Reachability-1.1
<input type="checkbox"/>	Medium	Today at 6:39 P...	On instance i-0871a0c91e93a7996, TCP port 22 w...	Network-Audit	Assessment-Temp...	Network Reachability-1.1
<input type="checkbox"/>	Informational	Today at 6:23 P...	Aggregate network exposure: On instance i-0871a0...	Network-Audit	Assessment-Temp...	Network Reachability-1.1
<input type="checkbox"/>	Medium	Today at 6:23 P...	On instance i-0871a0c91e93a7996, TCP port 22 w...	Network-Audit	Assessment-Temp...	Network Reachability-1.1
<input type="checkbox"/>	High	Today at 6:23 P...	On instance i-0871a0c91e93a7996, TCP port 23 w...	Network-Audit	Assessment-Temp...	Network Reachability-1.1



# Task 5

## Replace BastionServer with Systems Manager

### Step 1: Edit inbound rules

In the EC2 dashboard, go to **Security Groups**. Select the BastionServerSG security group and choose [Edit inbound rules](#).

Security Groups (4) <a href="#">Info</a>					
<div><div><div>Q Find resources by attribute or tag</div></div><div><div>&lt; 1 &gt;</div><div></div></div></div>					
<input type="checkbox"/>	Name	Security group ID	Security group name	VPC ID	Description
<input type="checkbox"/>	BastionServerSG	<a href="#">sg-0179ad25f9f7858f5</a>	c117085a279008616467937t1w767...	<a href="#">vpc-0da2cfb0cbfa60012</a>	security group
<input type="checkbox"/>	AppSG	<a href="#">sg-01ae975ee3f4fd561</a>	c117085a279008616467937t1w767...	<a href="#">vpc-0da2cfb0cbfa60012</a>	security group

Inbound rules <a href="#">Info</a>					
Security group rule ID	Type <a href="#">Info</a>	Protocol <a href="#">Info</a>	Port range <a href="#">Info</a>	Source <a href="#">Info</a>	Description - optional <a href="#">Info</a>
sg-0688aea27f378ce0c	SSH	TCP	22	Cust... <div><div>Q</div><div>190.117.58.32/32 X</div></div>	<div></div> <div>Delete</div>

### Step 2: Remove the SSH inbound rule

Delete the SSH rule of the BastionServerSG security group.

Inbound rules <a href="#">Info</a>					
This security group has no inbound rules.					



# Task 5

## Replace BastionServer with Systems Manager

### Step 3: Stop the BastionServer instance

Go to the **Instances** section and stop the BastionServer instance.

Instances (2) <a href="#">Info</a>							
<input type="text" value="Find Instance by attribute or tag (case-sensitive)"/>				All states ▾		< 1 > ⚙	
<input type="checkbox"/>	Name ↗ ▾	Instance ID	Instance state ▾	Status check	Availability Zone ▾	Public IPv4 ... ▾	Security group name ▾
<input type="checkbox"/>	BastionServer	i-0871a0c91e93a7996	⏹ Stopped 🔍	-	us-west-2a	-	c117085a27900861646...
<input type="checkbox"/>	AppServer	i-0d4e329c3ec0c5df3	✅ Running 🔍	🟢 2/2 checks passed	us-west-2a	35.160.239.71	c117085a27900861646...

### Step 4: Connect to the AppServer instance

Connect to the AppServer instance using Session Manager.

#### Connect to instance [Info](#)

Connect to your instance i-0d4e329c3ec0c5df3 (AppServer) using any of these options

EC2 Instance Connect

**Session Manager**

SSH client

EC2 serial console

Session Manager usage:

- Connect to your instance without SSH keys, a bastion host, or opening any inbound ports.
- Sessions are secured using an AWS Key Management Service key.
- You can log session commands and details in an Amazon S3 bucket or CloudWatch Logs log group.
- Configure sessions on the Session Manager [Preferences](#) page.

Cancel

Connect



# Task 5

## Replace BastionServer with Systems Manager

### Step 5: Run commands in the Session Manager

Enter the commands `cd ~` and `pwd` to change the directory and to view the current working directory of the AppServer.

Session ID: user3195341=Cristhian\_Becerra-0348f81ed564d21b6Instance ID: i-0d4e329c3ec0c5df3

```
sh-4.2$ cd ~
sh-4.2$ pwd
/home/ssm-user
sh-4.2$
```

### Step 6: Final scan of the environment

Re-run the assessment and verify that there are zero Findings.

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.](#)

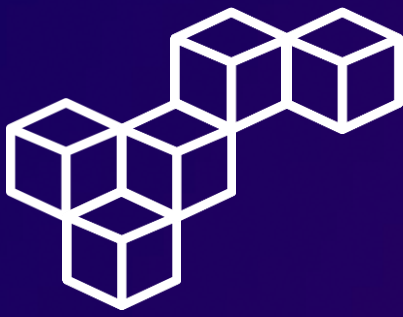
RunCancelDelete

Last updated on April 17, 2024 6:49:47 PM (0m ago)

Filter

Viewing 1-3 of 3

	Start time	Status	Template name	Findings	Findings by severity	Exclusions	Reports
<input type="checkbox"/>	Today at 6:49 PM (G...)	Analysis complete	Assessment-Templ...	0	High   Medium   Low...	1	<a href="#">Download report</a>
<input type="checkbox"/>	Today at 6:39 PM (G...)	Analysis complete	Assessment-Templ...	2	High   Medium   Low...	2	<a href="#">Download report</a>
<input type="checkbox"/>	Today at 6:22 PM (G...)	Analysis complete	Assessment-Templ...	3	High   Medium   Low...	2	<a href="#">Download report</a>



# Conclusions

---

## **Network Hardening**

Network hardening enhances security by implementing robust measures like firewall rules and access controls.

## **Amazon Inspector**

Amazon Inspector automates security assessments to identify vulnerabilities and compliance issues within AWS resources.

## **Amazon Inspector Classic**

Amazon Inspector Classic focuses on security assessments for EC2 instances and applications, offering a detailed analysis of vulnerabilities and compliance issues within AWS environments.

## **Amazon Inspector Assessments**

Amazon Inspector assessments provide actionable insights to improve security posture and meet regulatory requirements.

## **Amazon Inspector Findings**

Amazon Inspector findings highlight specific security issues, enabling targeted remediation efforts.

## **Connecting to instances using Session Manager**

Connecting to instances using Session Manager enhances security by providing secure, auditable access without the need for direct SSH access.



**Cristhian Becerra**



[cristhian-becerra-espinoza](#)



+51 951 634 354



[cristhianbecerra99@gmail.com](mailto:cristhianbecerra99@gmail.com)



Lima, Peru

