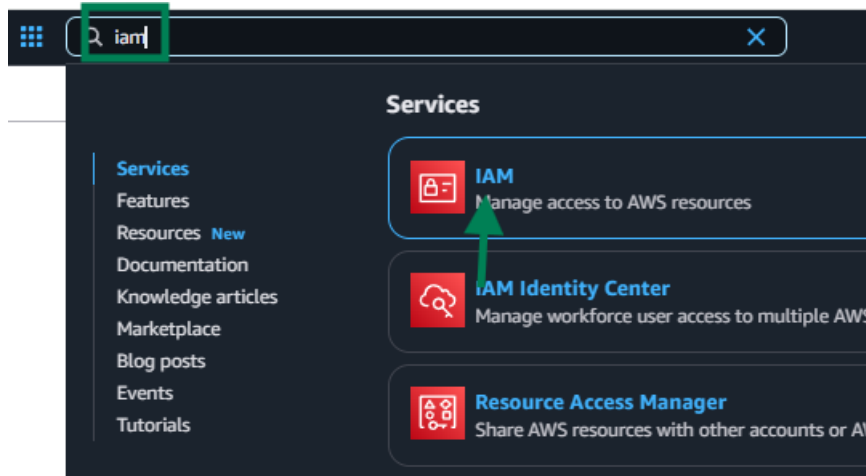
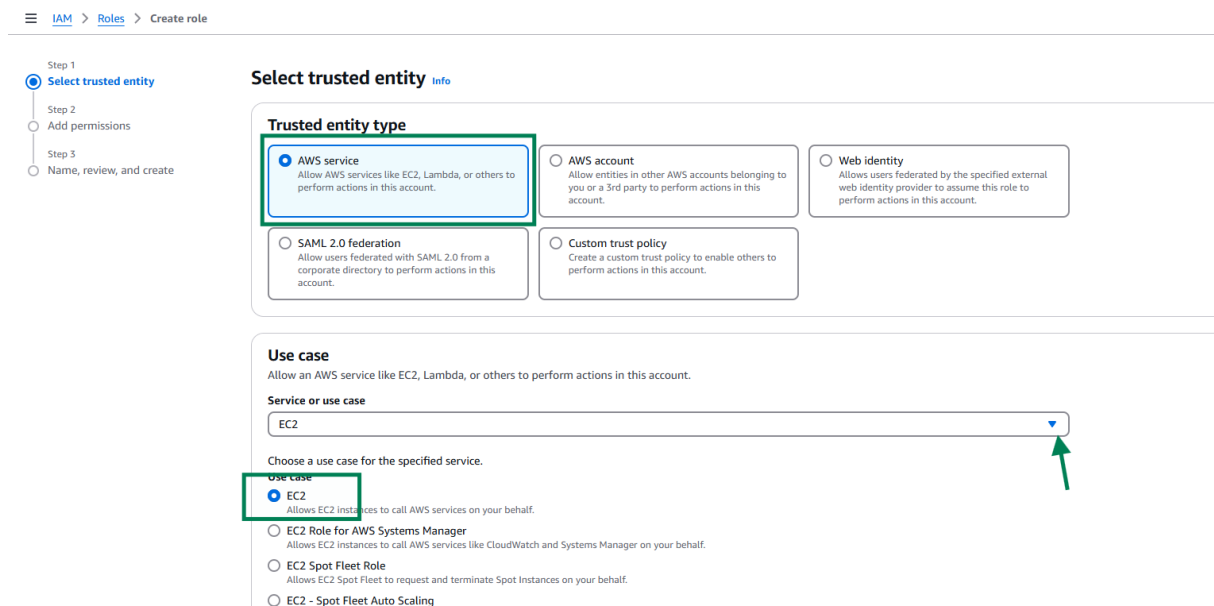
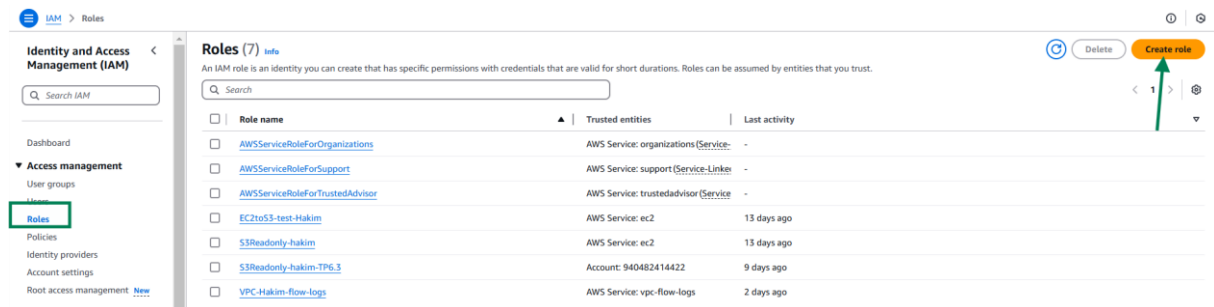


# AWS SSM & Inspector

## Accédez à IAM



## Créez un rôle nommé « EC2RoleforSSM ».



## TP 9 : AWS SSM & Inspector

Step 1 Select trusted entity  
Step 2 Add permissions  
Step 3 Name, review, and create

### Add permissions

Permissions policies (1/1015) [info](#)

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

Filter by Type: All types 4 matches

Policy name	Type	Description
<input type="checkbox"/> AmazonSSMMaintenanceWindowRole	AWS managed	Service Role to be used for EC2 Maintenance Window
<input type="checkbox"/> AmazonSSMManagedEC2InstanceDefaultPolicy	AWS managed	This policy enables AWS Systems Manager functionality on EC2 instances.
<input checked="" type="checkbox"/> AmazonSSMManagedInstanceCore	AWS managed	The policy for Amazon EC2 Role to enable AWS Systems Manager service core functionality.
<input type="checkbox"/> AWSQuickSetupSSMManageResourcesExecutionPolicy	AWS managed	This policy grants permissions that allow Systems Manager to create prerequisites such a...

► Set permissions boundary - optional

Cancel Previous **Next**

Step 1 Select trusted entity  
Step 2 Add permissions  
Step 3 Name, review, and create

### Name, review, and create

#### Role details

**Role name**  
Enter a meaningful name to identify this role.  
**EC2RoleforSSM**  
Maximum 64 characters. Use alphanumeric and '+,\_,@,-' characters.

**Description**  
Add a short explanation for this role.  
**Allows EC2 instances to call AWS services on your behalf.**  
Maximum 1000 characters. Use letters (A-Z and a-z), numbers (0-9), tabs, new lines, or any of the following characters: \_+., @-/[]!#\$%^&\*()~"

### Step 1: Select trusted entities

#### Trust policy

```
1 {  
2   "Version": "2012-10-17",  
3   "Statement": [  
4     {  
5       "Effect": "Allow",  
6       "Action": [  
7         "sts:AssumeRole"  
8       ],  
9       "Principal": {  
10        "Service": [  
11          "ec2.amazonaws.com"  
12        ]  
13      }  
14    ]  
15  }  
16 }
```

## TP 9 : AWS SSM & Inspector

### Step 2: Add permissions

[Edit](#)

#### Permissions policy summary

Policy name

▲ | Type

▼ | Attached as

▼

[AmazonSSMManagedInstanceCore](#)

AWS managed

Permissions policy

### Step 3: Add tags

#### Add tags - optional

Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

No tags associated with the resource.

[Add new tag](#)

You can add up to 50 more tags.

[Cancel](#)[Previous](#)[Create role](#)

Role EC2RoleforSSM created.

## Roles (8)

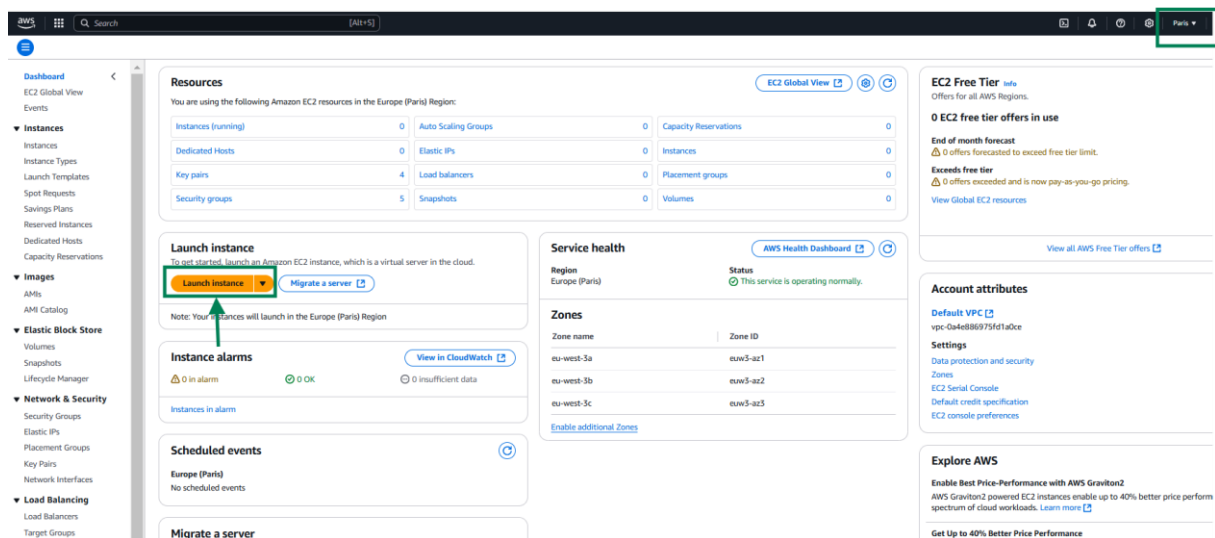
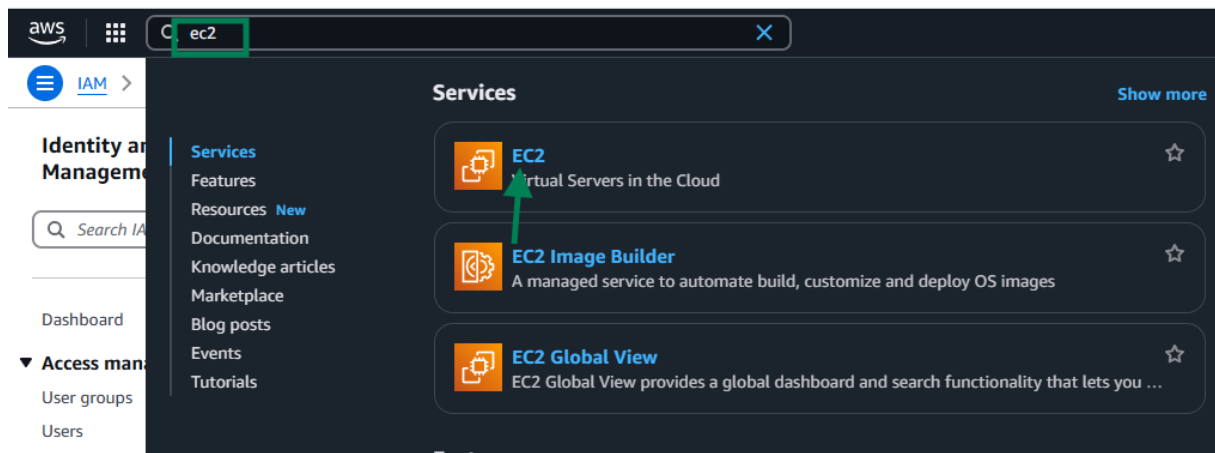
An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that yo

Search

<input type="checkbox"/>	Role name	▲   Trusted entities	Last activity
<input type="checkbox"/>	<a href="#">AWSServiceRoleForOrganizations</a>	AWS Service: organizations (Service-	-
<input type="checkbox"/>	<a href="#">AWSServiceRoleForSupport</a>	AWS Service: support (Service-Linker	-
<input type="checkbox"/>	<a href="#">AWSServiceRoleForTrustedAdvisor</a>	AWS Service: trustedadvisor (Service	-
<input type="checkbox"/>	<a href="#">EC2RoleforSSM</a>	AWS Service: ec2	-
<input type="checkbox"/>	<a href="#">EC2toS3-test-Hakim</a>	AWS Service: ec2	13 days ago
<input type="checkbox"/>	<a href="#">S3Readonly-hakim</a>	AWS Service: ec2	13 days ago
<input type="checkbox"/>	<a href="#">S3Readonly-hakim-TP6.3</a>	Account: 940482414422	9 days ago
<input type="checkbox"/>	<a href="#">VPC-Hakim-flow-logs</a>	AWS Service: vpc-flow-logs	2 days ago

Vous allez lancer une instance Linux (T2.micro), qui dispose par défaut de l'agent **Systems Manager** préinstallé.

## TP 9 : AWS SSM & Inspector



Nommez l'instance « **EC2 Linux VotreNom Inspector** » (par exemple : EC2 Linux Hakim Inspector).

## TP 9 : AWS SSM & Inspector

### Launch an instance [Info](#)

Amazon EC2 allows you to create virtual machines, or instances, that run on the AWS Cloud. Quickly get started by following the simple steps below.

#### Name and tags [Info](#)

Name

EC2 linux Hakim inspector

[Add additional tags](#)

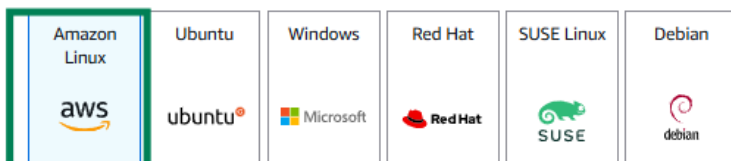
#### ▼ Application and OS Images (Amazon Machine Image) [Info](#)

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

Q Search our full catalog including 1000s of application and OS images

Recents

**Quick Start**



[Browse more AMIs](#)

Including AMIs from  
AWS, Marketplace and  
the Community

#### Amazon Machine Image (AMI)

Amazon Linux 2023 AMI

ami-03216a20ecc5d72ee (64-bit (x86), uefi-preferred) / ami-07ee183bb1314209b (64-bit (Arm), uefi)  
Virtualization: hvm ENA enabled: true Root device type: ebs

Free tier eligible

#### Description

Amazon Linux 2023 is a modern, general purpose Linux-based OS that comes with 5 years of long term support. It is optimized for AWS and designed to provide a secure, stable and high-performance execution environment to develop and run your cloud applications.

Amazon Linux 2023 AMI 2023.6.20241121.0 x86\_64 HVM kernel-6.1

Architecture

64-bit (x86)

Boot mode

uefi-preferred

AMI ID

ami-  
03216a20ecc5d72ee

Username

ec2-user



Verified provider

## TP 9 : AWS SSM & Inspector

Vous allez lancer l'instance dans le VPC par défaut de la région Paris.

**▼ Key pair (login)** [Info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

**Key pair name - required**

Hakim-Key ▼ [Create new key pair](#)

**▼ Network settings** [Info](#) [Edit](#)

**Network** [Info](#)

vpc-0a4e886975fd1a0ce

**Subnet** [Info](#)

No preference (Default subnet in any availability zone)

**Auto-assign public IP** [Info](#)

Enable

Additional charges apply when outside of free tier allowance

**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**

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

Select security groups ▼ [Compare security group rules](#)

Security groups that you add or remove here will be added to or removed from all your network interfaces

N'oubliez pas d'ajouter le rôle **EC2RoleforSSM**.

**▼ Advanced details** [Info](#)

**Domain join directory** [Info](#)

Select ▼ [Create new directory](#)

**IAM instance profile** [Info](#)

EC2RoleforSSM  
arn:aws:iam::940482414422:instance-profile/EC2RoleforSSM ▼ [Create new IAM profile](#)

**Hostname type** [Info](#)

IP name ▼

**DNS Hostname** [Info](#)

☒ Enable IP name IPv4 (A record) DNS requests

☒ Enable resource-based IPv4 (A record) DNS requests

☐ Enable resource-based IPv6 (AAAA record) DNS requests

**Instance auto-recovery** [Info](#)

Select ▼

**Shutdown behavior** [Info](#)

Stop ▼

**Stop - Hibernate behavior** [Info](#)

## TP 9 : AWS SSM & Inspector

Additional charges apply when outside of free tier allowance

**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

**Common security groups** [Info](#)  
Select security groups

default sg-0d472b7f0b0f234a1 [X](#)  
VPC: vpc-0a4e886975fd1a0ce

[Compare security group rules](#)

**Configure storage** [Info](#) [Advanced](#)  
1x 8 GiB gp3 Root volume (Not encrypted)

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage

[Add new volume](#)

Click refresh to view backup information  
The tags that you assign determine whether the instance will be backed up by any Data Lifecycle Manager policies.

0 x File systems [Edit](#)

[Advanced details](#) [Info](#)

**Virtual server type (instance type)**  
t2.micro

**Firewall (security group)**  
default

**Storage (volumes)**  
1 volume(s) - 8 GiB

**Free tier:** In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4 address usage per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

[Cancel](#) [Launch instance](#) [Preview code](#)

Vérifiez qu'aucune communication n'est autorisée, sauf celles au sein du même groupe de sécurité.

### Compare security group rules [Info](#)

Amazon EC2 evaluates all the rules of the selected security groups to control inbound and outbound traffic. You can select more security groups to view their inbound rules to help you to decide how to secure your instance from incoming traffic.

**Common security groups**  
Select security groups

default sg-0d472b7f0b0f234a1 [X](#)  
VPC: vpc-0a4e886975fd1a0ce

Security groups that you add or remove here will be added to or removed from all your network interfaces.

**Inbound rules (1)**

Security group name	Security group ID	Type	Protocol	Port range	Source	Description
default	sg-0d472b7f0b0f234a1	All traffic	All	All	sg-0d472b7f0b0f234a1	-

Cliquez sur « Cancel » pour revenir en arrière, puis relancez l'instance.

Security groups that you add or remove here will be added to or removed from all your network interfaces.

**Configure storage** [Info](#) [Advanced](#)  
1x 8 GiB gp3 Root volume (Not encrypted)

Free tier eligible customers can get up to 30 GB of EBS General Purpose (SSD) or Magnetic storage

[Add new volume](#)

Click refresh to view backup information  
The tags that you assign determine whether the instance will be backed up by any Data Lifecycle Manager policies.

0 x File systems [Edit](#)

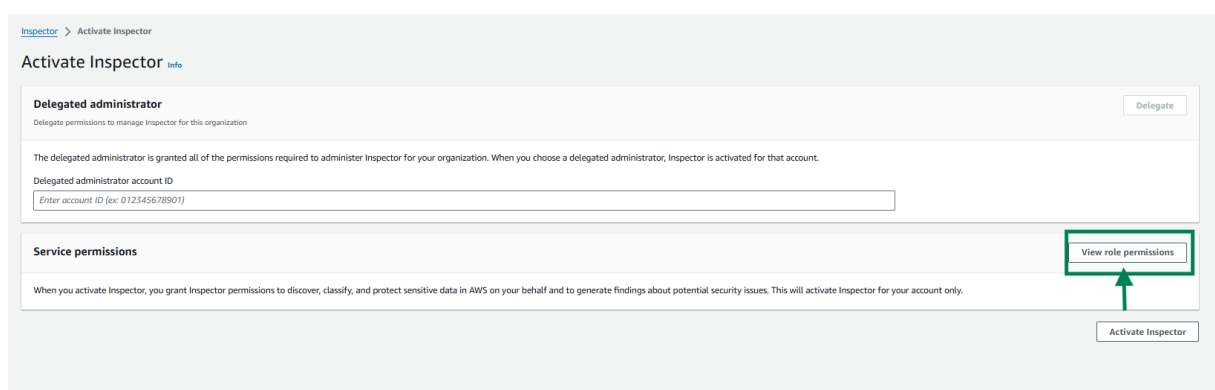
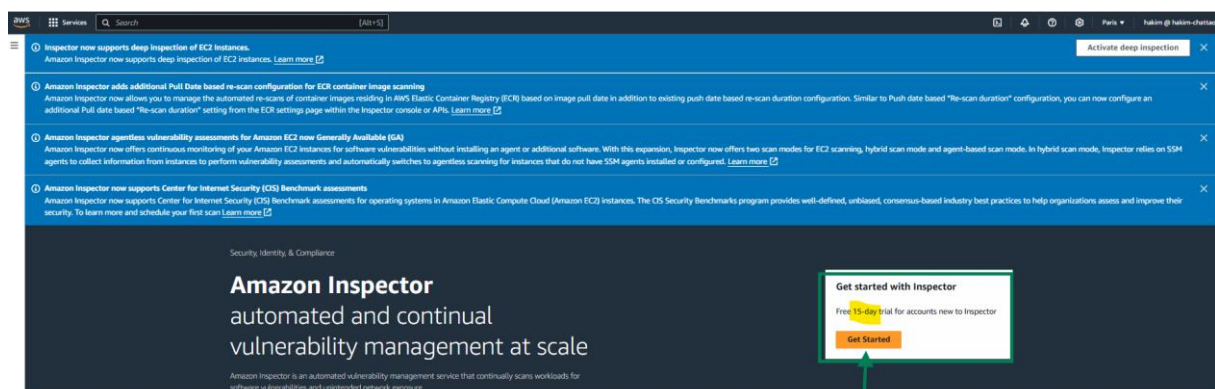
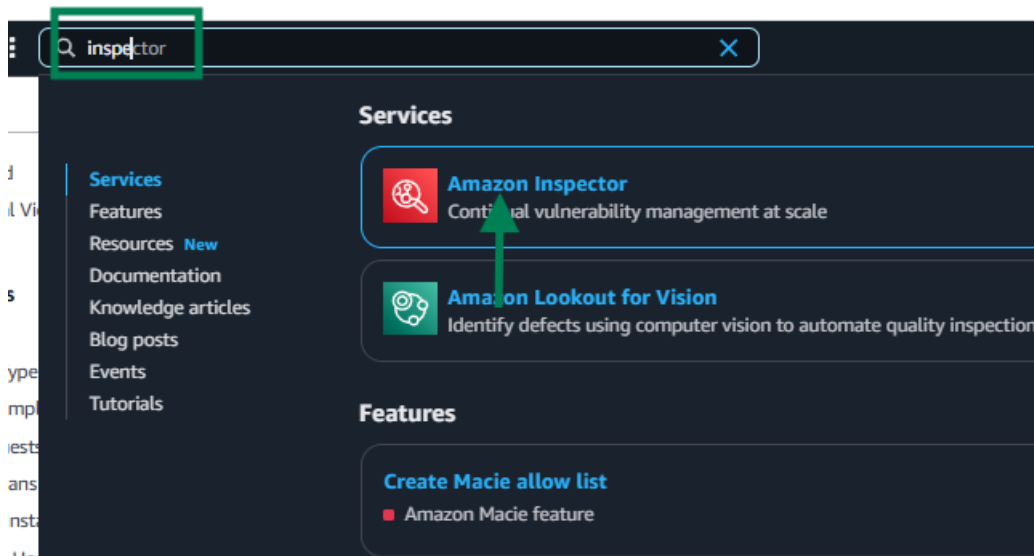
[Advanced details](#) [Info](#)

**Free tier:** In your first year includes 750 hours of t2.micro (or t3.micro in the Regions in which t2.micro is unavailable) instance usage on free tier AMIs per month, 750 hours of public IPv4 address usage per month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

[Cancel](#) [Launch instance](#) [Preview code](#)

## TP 9 : AWS SSM & Inspector

Vous allez maintenant activer **AWS Inspector** (ce service est gratuit pendant 15 jours).





Amazon Inspector service-linked role

×

Role name: `AWSServiceRoleForAmazonInspector2`

The following policy document contains the permissions that Inspector requires to detect and protect resources in your AWS environment.

Read-only

Permissions

Trust relationships

```

1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": [
7         "directconnect:DescribeConnections",
8         "directconnect:DescribeDirectConnectGatewayAssociations",
9         "directconnect:DescribeDirectConnectGatewayAttachments",
10        "directconnect:DescribeDirectConnectGateways",
11        "directconnect:DescribeVirtualGateways",
12        "directconnect:DescribeVirtualInterfaces",
13        "directconnect:DescribeTags",
14        "ec2:DescribeTags",
15        "ec2:DescribeAvailabilityZones",
16        "ec2:DescribeCustomerGateways",
17        "ec2:DescribeInstances",
18        "ec2:DescribeInternetGateways",
19        "ec2:DescribeManagedPrefixLists",
20        "ec2:DescribeNatGateways",
21        "ec2:DescribeNetworkAcls",
22        "ec2:DescribeNetworkInterfaces",
23        "ec2:DescribePrefixLists",
24        "ec2:DescribeRegions",
25        "ec2:DescribeRouteTables",
26        "ec2:DescribeSecurityGroups",
27        "ec2:DescribeSubnets",
28        "ec2:DescribeTransitGatewayAttachments",
29        "ec2:DescribeTransitGatewayConnects",
30        "ec2:DescribeTransitGatewayPeeringAttachments",
31        "ec2:DescribeTransitGatewayRouteTables",
32        "ec2:DescribeTransitGatewayVpcAttachments",
33        "ec2:DescribeTransitGateways",

```

Close

## TP 9 : AWS SSM & Inspector

Inspector > Activate Inspector

### Activate Inspector Info

**Delegated administrator** Delegate  
Delegate permissions to manage Inspector for this organization.

The delegated administrator is granted all of the permissions required to administer Inspector for your organization. When you choose a delegated administrator, Inspector is activated for that account.

Delegated administrator account ID

**Service permissions** View role permissions

When you activate Inspector, you grant Inspector permissions to discover, classify, and protect sensitive data in AWS on your behalf and to generate findings about potential security issues. This will activate Inspector for your account only.

**Activate Inspector**

1 Welcome to Inspector  
To get started, activate Amazon EC2, Amazon ECR, AWS Lambda scanning for your member accounts. Manage all accounts

2 Welcome to Inspector. Your first scan is underway.

3 Inspector now supports deep inspection of EC2 instances. Activate deep inspection

4 Amazon Inspector adds additional Pull Date based re-scan configuration for ECR container image scanning  
Amazon Inspector now allows you to manage the automated re-scans of container images residing in AWS Elastic Container Registry (ECR) based on image pull date in addition to existing push date based re-scan duration configuration. Similar to Push date based "Re-scan duration" configuration, you can now configure an additional Pull date based "Re-scan duration" setting from the ECR settings page within the Inspector console or APIs. [Learn more](#)

5 Amazon Inspector agentless vulnerability assessments for Amazon EC2 now Generally Available (GA)  
Amazon Inspector now offers continuous monitoring of your Amazon EC2 instances for software vulnerabilities without installing an agent or additional software. With this expansion, Inspector now offers two scan modes for EC2 scanning, hybrid scan mode and agent-based scan mode. In hybrid scan mode, Inspector relies on SSM agents to collect information from instances to perform vulnerability assessments and automatically switches to agentless scanning for instances that do not have SSM agents installed or configured. [Learn more](#)

Inspector > Dashboard

### Summary Info

Viewing data from all accounts

**Environment coverage**  
Your accounts, instances, and repositories that are activated with Inspector.

Instances	Repositories
—	—
0 / 0 instances	0 / 0 repositories
Lambda functions	
—	
0 / 0 Lambda functions	

**Critical findings**  
All active critical findings in your environment.

ECR container	EC2 Instance	Lambda functions
0 Critical 0 total findings	0 Critical 0 total findings	0 Critical 0 total findings

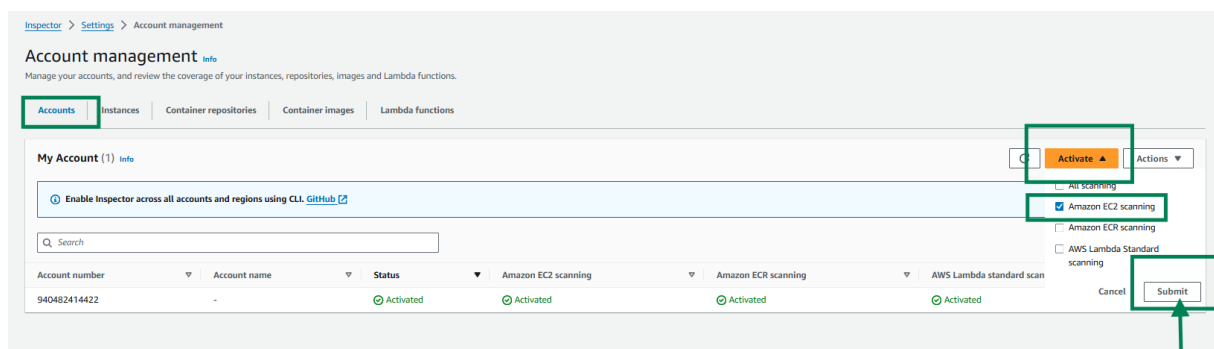
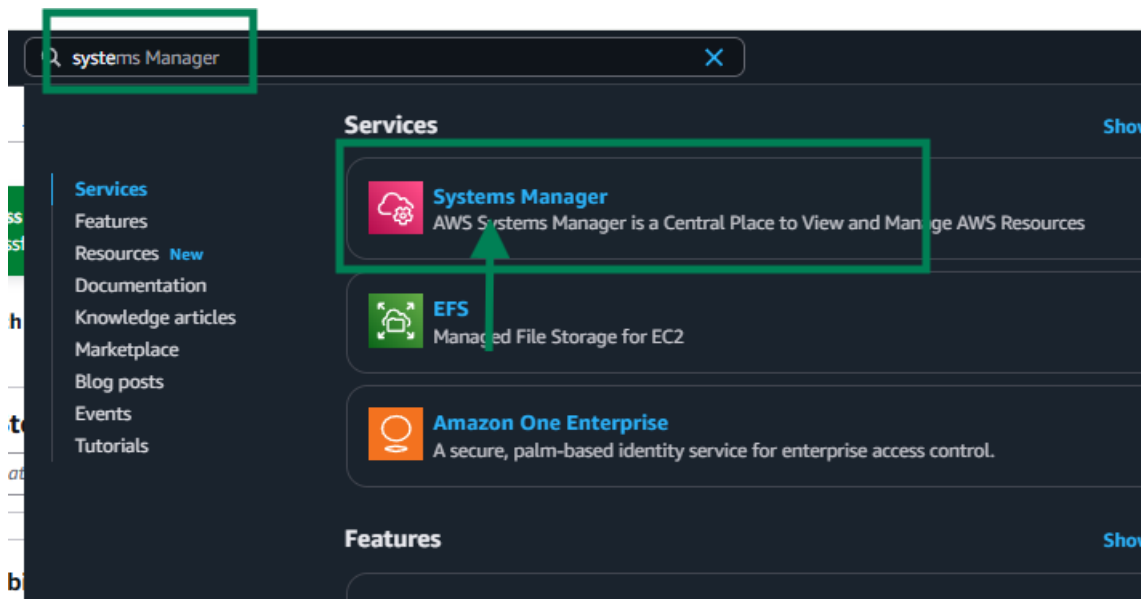
**Findings with exploit available and fix available**  
View the findings with exploit available and fix available coverage.

Environments with neither exploit nor fix available

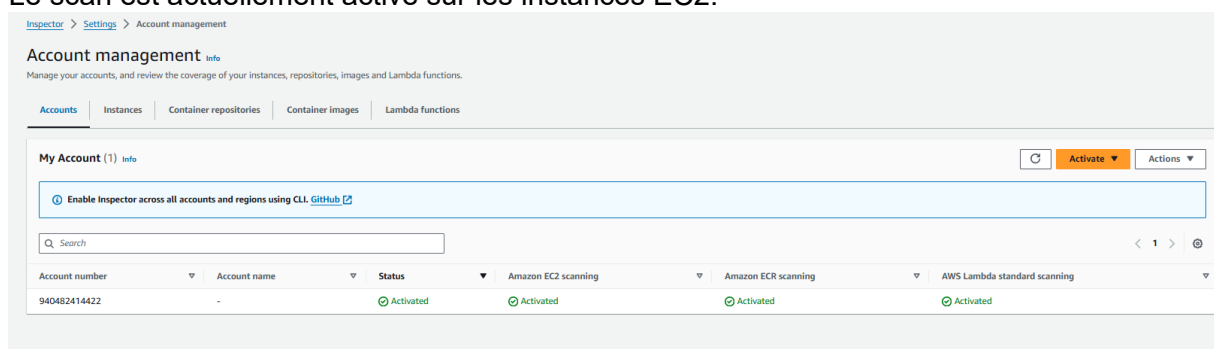
Environments with fix available

Activation de **Systems Manager**.

## TP 9 : AWS SSM & Inspector

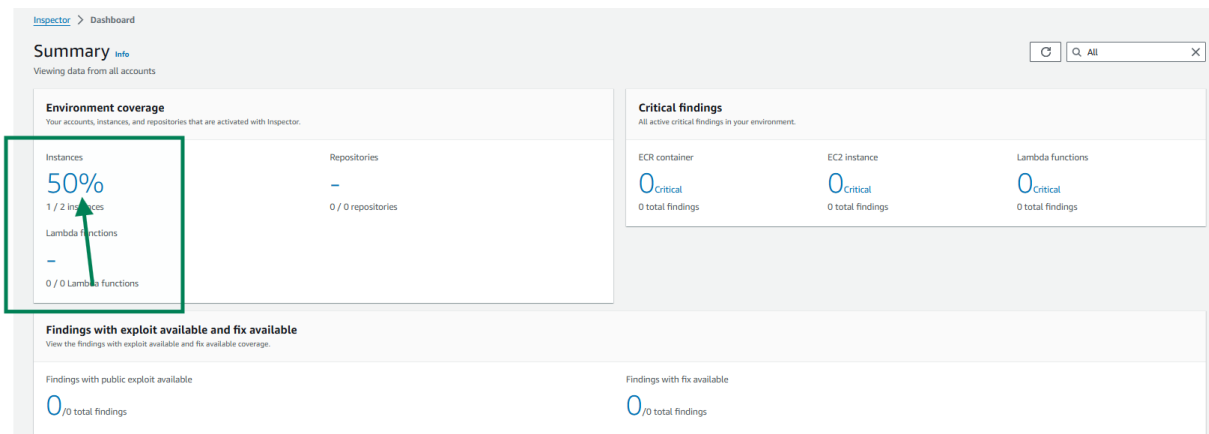


Le scan est actuellement activé sur les instances EC2.



Après un certain temps, vous obtiendrez des résultats comme suit.

## TP 9 : AWS SSM & Inspector



The AWS Inspector Account management Instances view displays the following information:

- Accounts:** All (2), Scanning (1), Not scanning (1). A green arrow points to the 'Scanning' tab.
- Instances (2):** Info. A green arrow points to the 'Instances (2)' header.
- Filters:** Resource type EQUALS Amazon EC2 Instance. Clear filters.
- Table:**

EC2 instance	EC2 instance tags	Account	AMI	Operating system	Last scanned	Status
i-002c0c0b164fdb4a	Name:EC2 Windows Hakim ins...	abdelhakim-chattaoui (940482414	ami-0579db1599727b2c3	WINDOWS	-	Unmanaged EC2 instance
i-069439dc2b5e65048...	Name:EC2 linux Hakim inspec...	abdelhakim-chattaoui (940482414	ami-03216a20ecc5d72ee	LINUX	December 4, 2024 10:20 A...	Actively monitoring

Aws Inspector a terminé de scanner l'instance Linux.

The AWS Inspector Account management Instances view displays the following information:

- Accounts:** All (2), Scanning (1), Not scanning (1). A green box highlights the 'Scanning' tab.
- Instances (1):** Info. A green arrow points to the 'Instances (1)' header.
- Filters:** Resource type EQUALS Amazon EC2 Instance, Scan status code EQUALS Active. Clear filters.
- Table:**

EC2 instance	EC2 instance tags	Account	AMI	Operating system	Last scanned	Monitored using
i-069439dc2b5e65048...	Name:EC2 linux Hakim inspec...	abdelhakim-chattaoui (940482414422)	ami-03216a20ecc5d72ee	LINUX	December 4, 2024 10:20 AM (UTC...	Agentless

## TP 9 : AWS SSM & Inspector

Inspector > Settings > Account management > Instances

### Account management [Info](#)

Manage your accounts, and review the coverage of your instances, repositories, images and Lambda functions.

Accounts | **Instances** | Container repositories | Container images | Lambda functions

All 2	<b>Scanning</b> 1	Not scanning 1
----------	----------------------	-------------------

**Instances (1) [Info](#)**

Q Add filter

Resource type **EQUALS** Amazon EC2 Instance Scan status code **EQUALS** Active Clear filters

EC2 Instance	EC2 instance tags	Account	AMI	Operating system	Last scanned	Monitored using
i-069439dc2b5e65048...	Name: EC2 linux Hakim inspec...	abdelhakim-chattaoui (940482414422)	ami-03216a20ecc5d72ee	<b>LINUX</b>	December 4, 2024 10:20 AM (UTC...	Agentless

Vérifiez que vous n'avez aucune faille détectée ni de mise à jour à prévoir.

Inspector > Findings > By instance > i-069439dc2b5e65048

### i-069439dc2b5e65048 [Info](#)

EC2 instance

#### Details

EC2 instance i-069439dc2b5e65048 <a href="#">🔗</a>	Launched at December 3, 2024 10:19 AM (UTC+01:00)	Created by 940482414422
Role -	AWS account 940482414422	Security group default
Amazon machine image ami-03216a20ecc5d72ee		

Finding summary  
■ 0 Critical ■ 0 High ■ 0 Medium

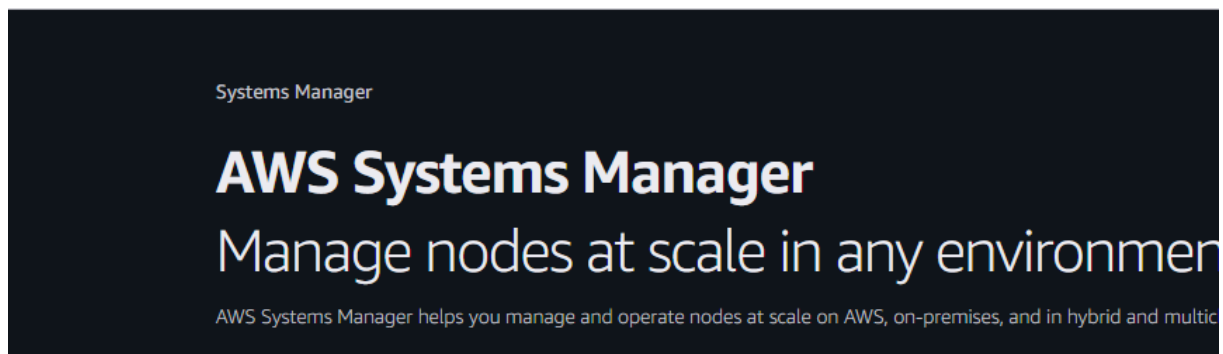
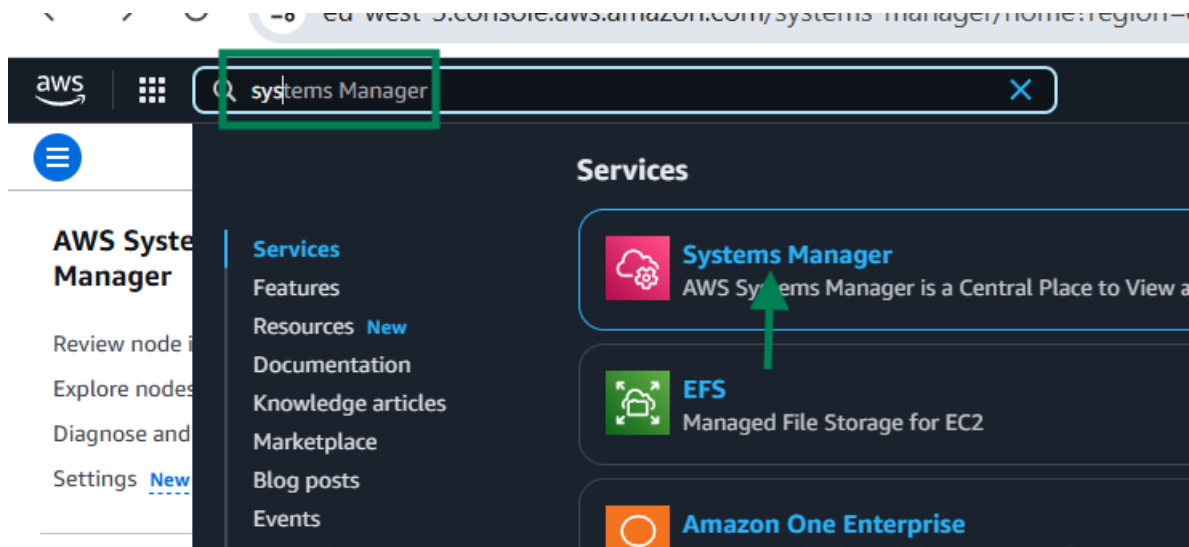
#### Findings (0)

Choose a row to view the finding details. All findings are related to this instance.

Finding status: Active Filter criteria: Q Add filter

Resource ID **EQUALS** i-069439dc2b5e65048 X Clear filters

Severity	Title	Type
No findings No findings to display.		



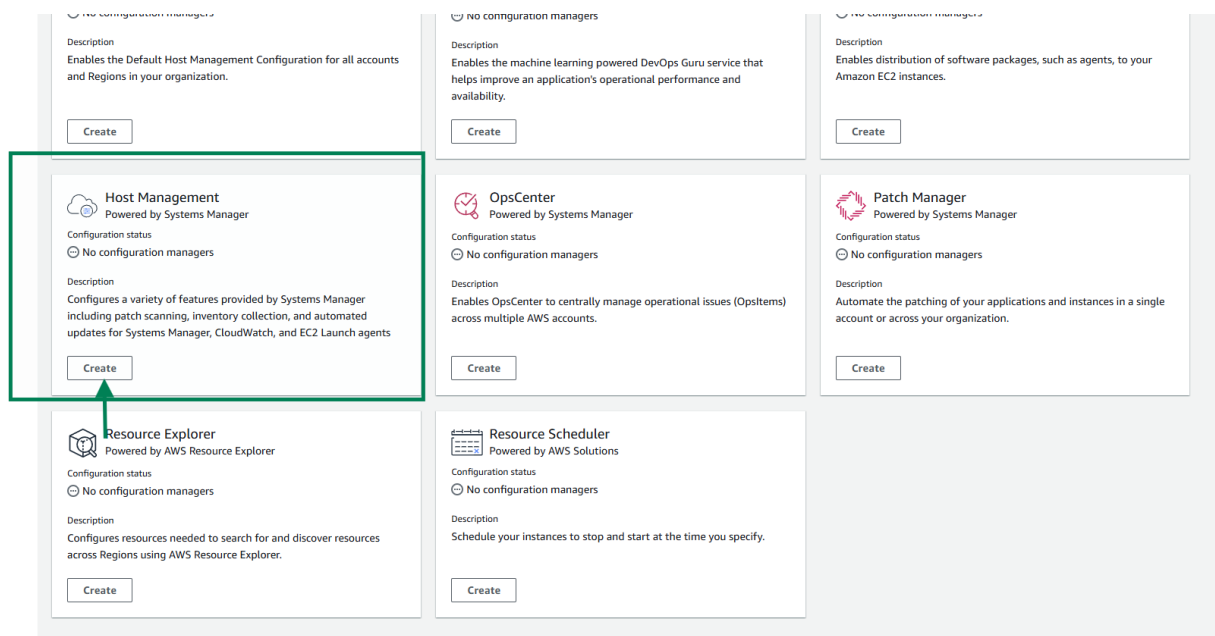
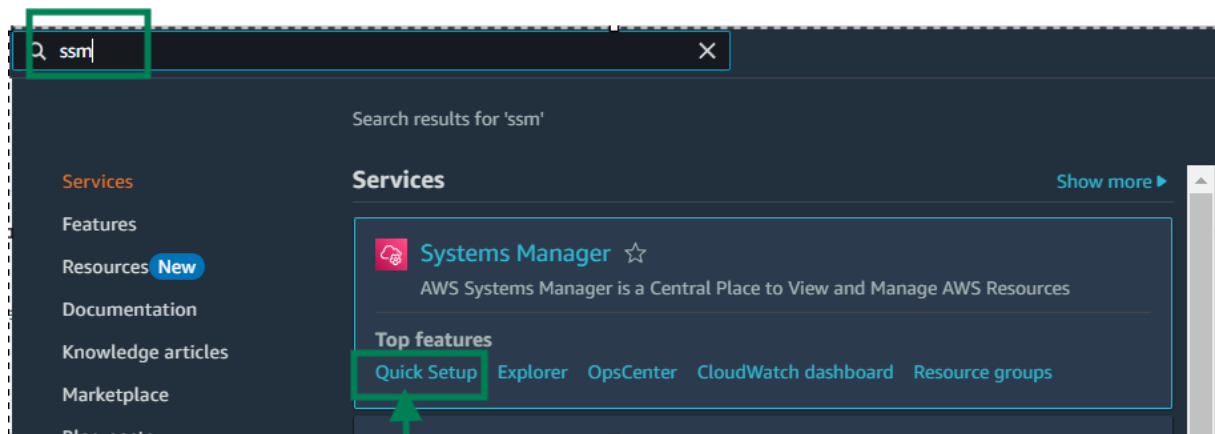
### Introducing the new integrated experience

The new Systems Manager experience is an intuitive, easy to use interface to simplify node management and efficiency. You can now manage nodes across AWS accounts and Regions from a central location. Get started with the new Systems Manager experience by logging in as an administrator account to manage nodes across your organization.

[Get started](#)

### Benefits

## TP 9 : AWS SSM & Inspector



[Systems Manager](#) > [Quick Setup](#) > Create configuration

## Customize Host Management configuration options

### Configure Systems Manager features to help manage your instances

This Quick Setup type helps you configure Systems Manager features including patch scanning and inventory collection, and more. It can also create instance profiles with the permissions required for using Systems Manager. To help you improve your security posture, you can also choose to set up automated updates for the Systems Manager, CloudWatch, and EC2 Launch agents.

### Configuration Options

Quick Setup configures the following Systems Manager components based on best practices. Select the check boxes for actions you want to schedule. [Learn more](#)

#### Systems Manager

- ☒ Update Systems Manager (SSM) Agent every two weeks.
- ☒ Collect inventory from your instances every 30 minutes.
- ☒ Scan instances for missing patches daily.

#### Amazon CloudWatch

- ☐ Install and configure the CloudWatch agent.
- ☐ Update the CloudWatch agent once every 30 days.

#### Amazon EC2 Launch Agent

- ☐ Update the EC2 launch agent once every 30 days.  
Select the check box to receive updates to the installed EC2 Windows, Linux, and Mac launch agent on [supported operating system versions](#).

If you run this configuration, [Systems Manager Explorer](#) is enabled.

Learn more about the metrics included in [the CloudWatch agent's basic configuration](#) and [Amazon CloudWatch pricing](#).

### Targets

Targets determine where this configuration will be deployed.

Choose the accounts and Regions you want to deploy this configuration to.

☐ Entire Organization  
Deploys your configuration to all OUs and Regions in your organization.

☐ Custom  
Choose the OUs and Regions you want to deploy this configuration to.

☒ Current account  
Choose the Regions to deploy this configuration to within the currently signed in account.

Choose between deploying to the current Region or a custom set of Regions.

☒ Current Region  
Deploy configuration to the current Region.

☐ Choose Regions  
Choose the Regions you want to deploy this configuration to.

Choose how you want to target instances - optional

☒ All instances  
Deploy your configuration to all instances in the target account and Regions.

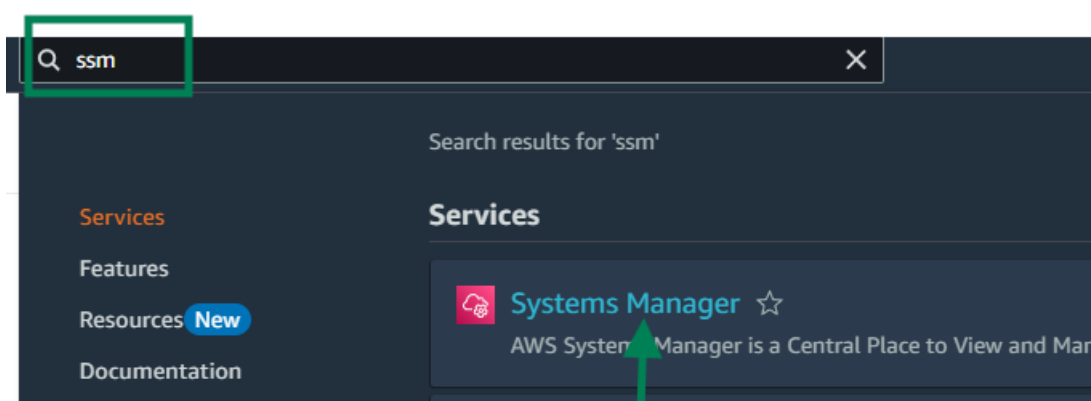
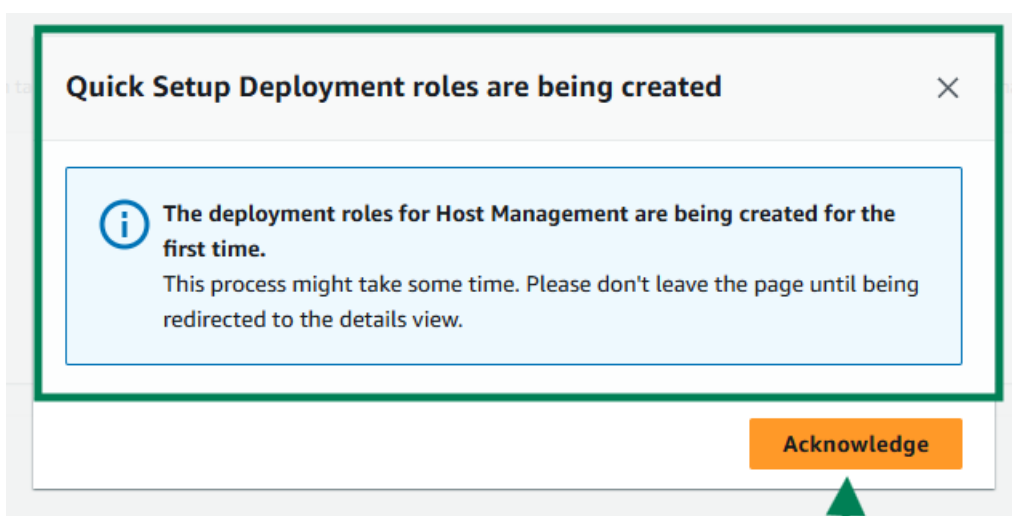
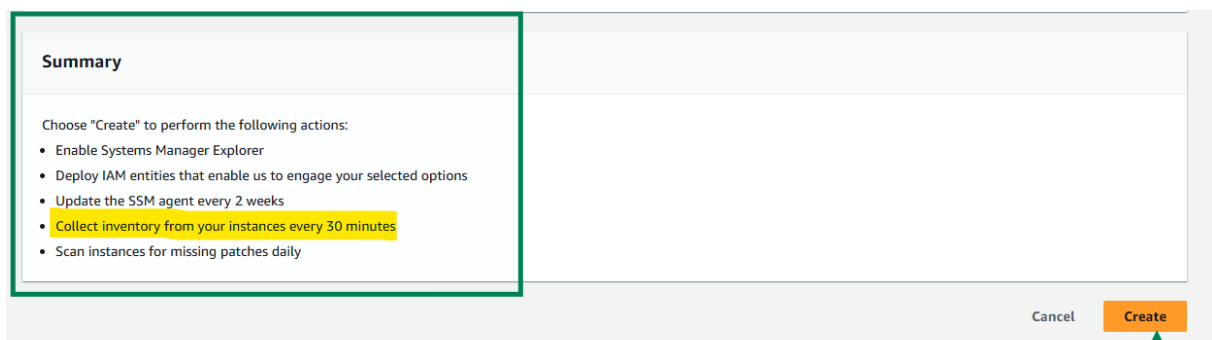
☐ Tag  
The key-value pair for the tag you want to target. Specifying a tag selects all instances with that tag.


☐ Resource Group  
Specify a resource group. Only instances in that group will be configured.

☐ Manual  
Manually specify the instances you want to configure.



## TP 9 : AWS SSM & Inspector





**AWS Systems Manager**

Review node insights [New](#)

Explore nodes [New](#)

Diagnose and remediate [New](#)

Settings [New](#)

▼ **Node Tools**

Compliance

Distributor

Fleet Manager

Hybrid Activations

Inventory

Patch Manager

Run Command

Session Manager

State Manager

▼ **Change Management Tools**

Automation

Change Calendar

Systems Manager

# AWS Systems Manager

## Manage nodes at scale in

AWS Systems Manager helps you manage and operate nodes at scale on

### Benefits

**Enhance visibility across your entire infrastructure**

Systems Manager provides a centralized view of your managed nodes. Review insights across your fleets and filter by node information such as ID, name, and operating system.

**Boost operational efficiency with automation**

Systems Manager provides a centralized view of your managed nodes. Review insights across your fleets and filter by node information such as ID, name, and operating system.

### Use cases


✔ Your Host Management Quick Setup was successfully created.

Systems Manager > Quick Setup > Configuration details

### Host Management

[Upgrade](#) [Edit](#) [Delete](#)

**Configuration manager Details**

Name <i>None specified</i>	Manager ARN arn:aws:ssm-quicksetup:eu-west-3:940482414422:configuration-manager/e86f5605-5dc6-4b2b-a716-8aa58a1c6158	Resource code 2vxym
Configuration type and version Host Management 4.0 	Description <i>None specified</i>	

**Filter by**

- ▶ Regions
- ▶ Deployment status
- ▶ Association status

**Configuration deployment status**  
The status of your configuration's deployment to its targets.

1  
Total


**Configuration association status**  
The status of the State Manager associations created by your configuration.

5  
Total


## TP 9 : AWS SSM & Inspector

Configuration details			
The status of each configuration deployment.			
Last updated: just now Configuration progress updated every 30 seconds.			
<input type="text" value="Search account ID"/>			
Account	Region	Configuration deployment status	Configuration status
940482414422	eu-west-3	Success	4 Success 1 Pending

Testez que vous pouvez prendre le contrôle de l'instance sans être obligé d'ajouter des groupes de sécurité.

**Session Manager**  
Quickly and securely access your Windows and Linux instances

Session Manager is a managed service that provides you with one-click secure access to your instances without the need to open inbound ports and manage bastion hosts. You have centralized access control over who can access your instances and full auditing capabilities to ensure compliance with corporate policies.

**How it works**

- 1 Configure your instances to use Session Manager
- 2 Assign user IAM policies to control instance access
- 3 Specify account options for session logs
- 4 Start a session on your instances by launching bash or shell terminal

**Why use Session Manager?**

- Improved security posture
- Centralized access control

**Getting started**

- What is Session Manager?
- Set up Session Manager
- Set up session logging
- Set up session notifications
- Create and manage sessions
- Monitor session activity

**More resources**

- Documentation

## TP 9 : AWS SSM & Inspector

AWS Systems Manager > Session Manager > Start a session

Step 1  
**Specify target**

Step 2 - optional  
Specify session document

Step 3  
Review and launch

### Specify target

Select an instance to connect to using Session Manager.

**Reason**

*Reason for session - optional*  
The reason for connecting to the instance. This value is included in the details of the event created by AWS CloudTrail when you start the session.

This value can have up to 256 characters.

**Target instances**

Instance name	Instance ID	Agent version	Instance state	Availability zone	Platform
<input checked="" type="radio"/> EC2 linux Hakim inspe...	i-Oa0043a1eb17a5fe7	3.3.1345.0	running	eu-west-3c	Amazon Linux

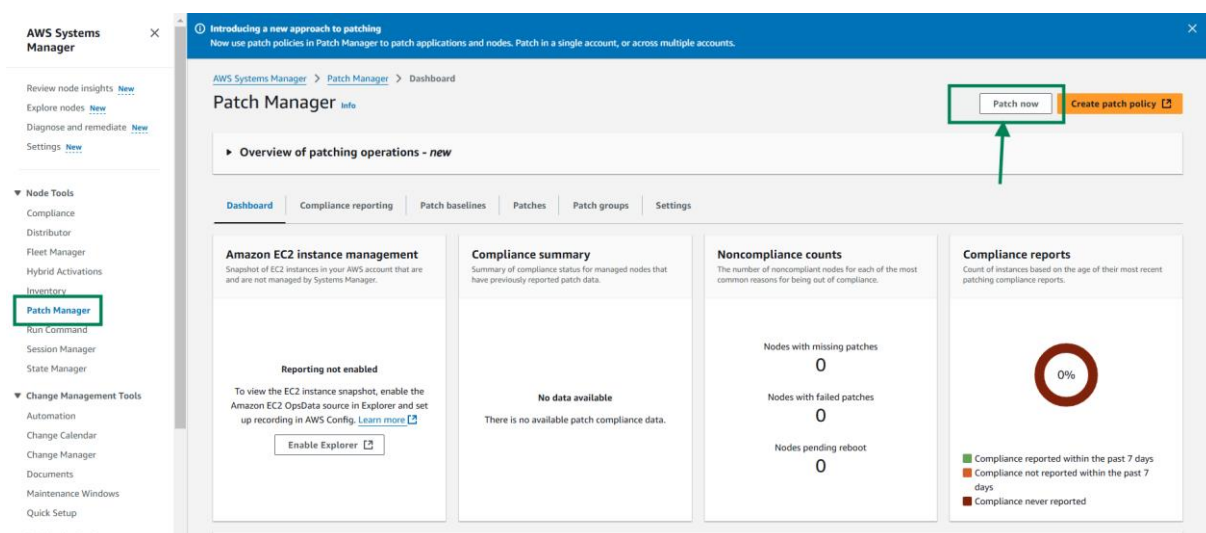
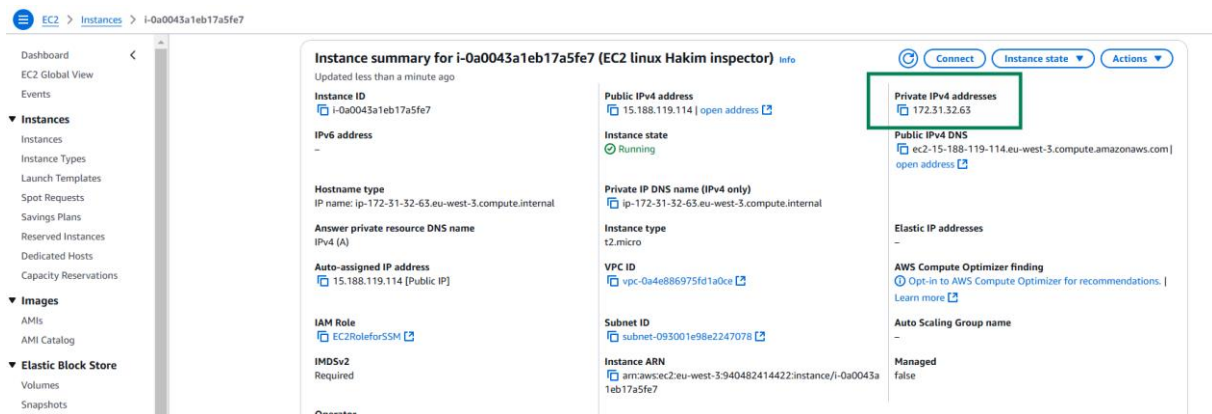
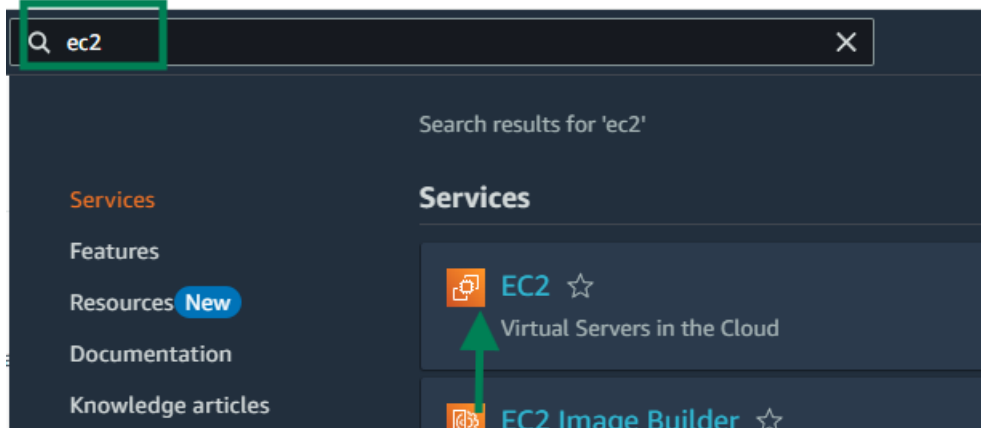
```
sh-5.2$ ifconfig
enX0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 9001
    inet 172.31.32.63 netmask 255.255.240.0 broadcast 172.31.47.255
    inet6 fe80::cec:151f:feed:2b19 prefixlen 64 scopeid 0x20<link>
    ether 0e:ec:f5:ed:2b:19 txqueuelen 1000 (Ethernet)
    RX packets 77640 bytes 156643633 (149.3 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 13945 bytes 1538638 (1.4 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 12 bytes 1020 (1020.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 12 bytes 1020 (1020.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

sh-5.2$
```

## TP 9 : AWS SSM & Inspector

Vérifiez qu'il s'agit bien de votre instance EC2 Linux.



## TP 9 : AWS SSM & Inspector

AWS Systems Manager > Patch Manager > Patch now

**New Features**

We listened to your concerns and now we provide a way to orchestrate complex patch operations in a way that does not compromise your fleet's availability. The Patch Lifecycle Hooks feature is available under advanced options below.

### Patch instances now [Info](#)

#### Basic configuration

Scan for missing patches or install patches, with or without rebooting. For more patching options, use the [Configure patching](#) page.

**Patching operation**

☒ Scan

☐ Scan and install

**Instances to patch**


Choose whether to patch all instances or only the instances you specify

☒ Patch all instances


☐ Patch only the target instances I specify

**Patching log storage**

Select or create an S3 bucket for storing patching operation logs. Select **Do not store logs** if you don't require log information.

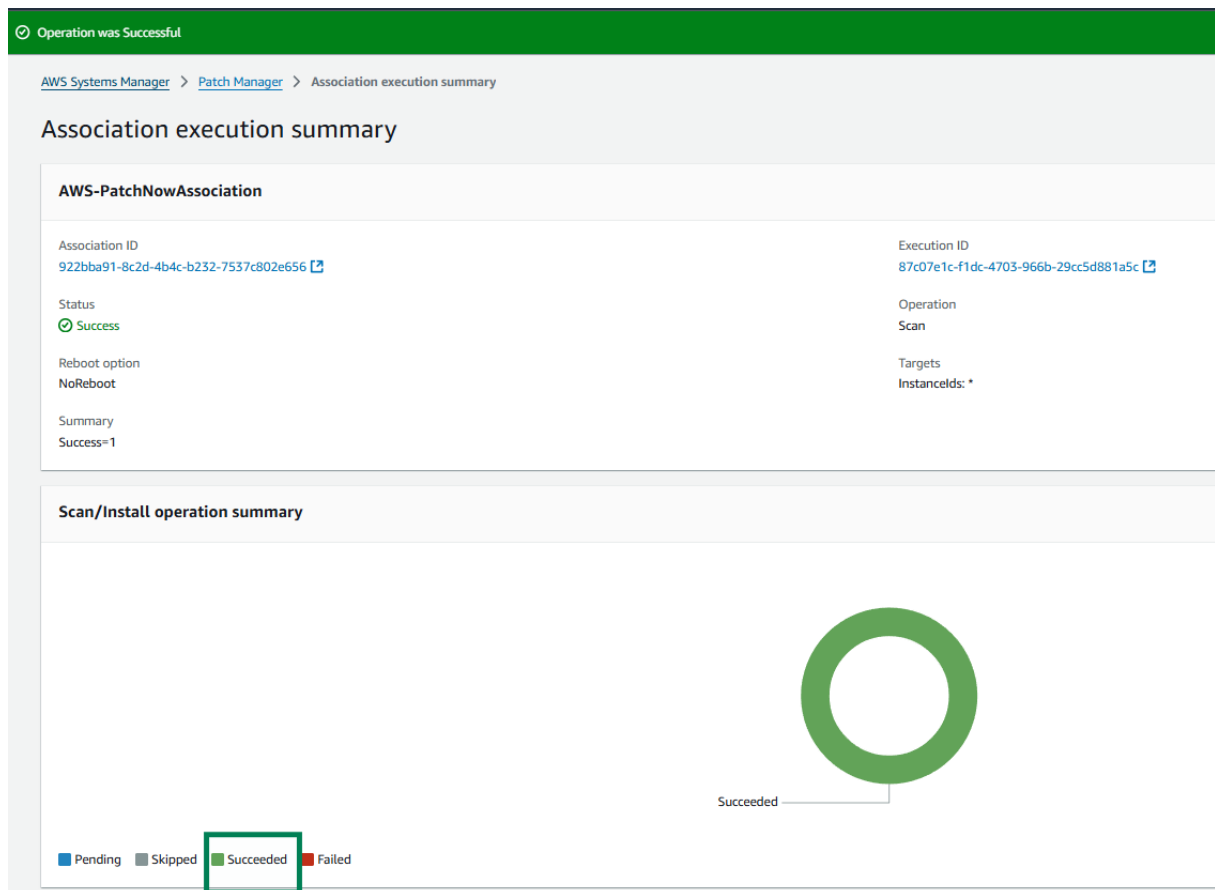
bucket-hakim14-11-2024 

**Patch now**

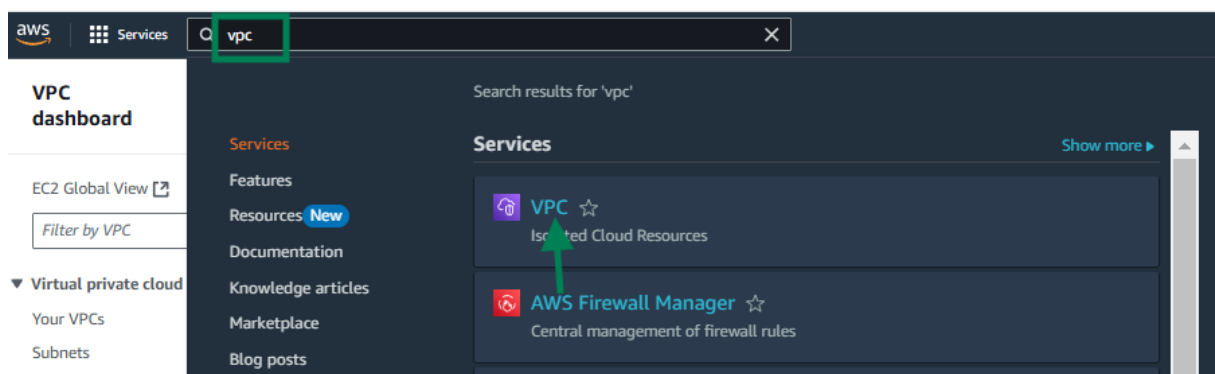


Après quelques instants, vous aurez les résultats suivants :

## TP 9 : AWS SSM & Inspector



Ajoutez un groupe de sécurité nommé « allow-http-ftp » qui autorise les flux HTTP et FTP.



## TP 9 : AWS SSM & Inspector

The screenshot shows the AWS VPC console's 'Security Groups' page. On the left sidebar, 'Security groups' is highlighted under the 'Security' section. The main area displays a table of existing security groups. In the top right corner, the 'Create security group' button is highlighted with a green box and an arrow.

Name	Security group ID	Security group name	VPC ID	Description	Owner	Inbound rules count
-	sg-0b0f5ca8b1b91e85	Bastion to private	vpc-0d0a9a938f2a8c1f	Bastion to private	940482414422	2 Permission entries
-	sg-090635c2f9b13339c	SG-allow-SSH-ICMP	vpc-0d0a9a938f2a8c1f	SG-allow-SSH-ICMP	940482414422	2 Permission entries
-	sg-07a72c4ab5455eb20	default	vpc-0d0a9a938f2a8c1f	default VPC security group	940482414422	1 Permission entry
-	sg-0b29d74e548e5a8375	allow only ssh	vpc-0d0a9a938f2a8c1f	launch-wizard-1 created 2024-11-30T...	940482414422	1 Permission entry
-	sg-0d472b79b0f234a1	default	vpc-0a4e886975d1a0ce	default VPC security group	940482414422	1 Permission entry

The screenshot shows the 'Create security group' form in the AWS VPC console. The form is divided into three main sections: 'Basic details', 'Inbound rules', and 'Tags - optional'. The 'Basic details' section includes fields for 'Security group name', 'Description', and 'VPC'. The 'Inbound rules' section allows adding rules with fields for 'Type', 'Protocol', 'Port range', 'Source', and 'Description'. The 'Tags - optional' section allows adding tags. The 'Create security group' button is highlighted with a green box and an arrow.

**Basic details**

Security group name: allow-http-ftp  
Description: allow-http-ftp  
VPC: vpc-0a4e886975d1a0ce

**Inbound rules**

Type	Protocol	Port range	Source	Description - optional
HTTP	TCP	80	Anywhere-IPv4	allow http
Custom TCP	TCP	21	Anywhere-IPv4	allow ftp

**Tags - optional**

No tags associated with the resource.

Buttons: Add rule, Add new tag, Cancel, Create security group



## TP 9 : AWS SSM & Inspector

Security group (sg-00f97944cc9dafc24 | allow-http-ftp) was created successfully

Details

VPC > Security Groups > sg-00f97944cc9dafc24 - allow-http-ftp

sg-00f97944cc9dafc24 - allow-http-ftp

Actions

Details

Security group name	allow-http-ftp	Security group ID	sg-00f97944cc9dafc24	Description	allow-http-ftp	VPC ID	vpc-Qa4e886975fd1a0ce
Owner	940482414422	Inbound rules count	2 Permission entries	Outbound rules count	1 Permission entry		

Inbound rules (2)

Name	Security group rule...	IP version	Type	Protocol	Port range	Source	Description
-	sg-0ed1a7e8be7c49c72	IPv4	Custom TCP	TCP	21	0.0.0.0/0	allow ftp
-	sg-0303b6457b03d8...	IPv4	HTTP	TCP	80	0.0.0.0/0	allow http

Search results for 'ec2'

Services

EC2

EC2 Image Builder

EC2 Global View

Instances (1/1) info

Find instance by attribute or tag (case-sensitive)

Instance state: running

Clear filters

Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...	Elastic IP
EC2 Linux Hakim Inspector	Running	t2.micro	2/2 checks passed	View alarms	eu-west-3c	ec2-15-188-119-114.eu...	15.188.119.114	-

Change security groups

Modify IAM role

## TP 9 : AWS SSM & Inspector

### Change security groups Info

Amazon EC2 evaluates all the rules of the selected security groups to control inbound and outbound traffic to and from your instance. You can use this window to add and remove security groups.

**Instance details**

Instance ID  
i-0a0043a1eb17a5fe7

Network interface ID  
eni-050f45a8199f29d45

**Associated security groups**

Add one or more security groups to the network interface. You can also remove security groups.

allow-http-ftp ( sg-00f97944cc9dafc24 )

default ( sg-0d472b7f0b0f234a1 )

allow-http-ftp ( sg-00f97944cc9dafc24 )

Security group ID	Security group name	Description	
sg-0d472b7f0b0f234a1	default	default VPC security group	940482414422 <input type="button" value="Remove"/>

### Change security groups Info

Amazon EC2 evaluates all the rules of the selected security groups to control inbound and outbound traffic to and from your instance. You can use this window to add and remove security groups.

**Instance details**

Instance ID  
i-0a0043a1eb17a5fe7

Network interface ID  
eni-050f45a8199f29d45

**Associated security groups**

Add one or more security groups to the network interface. You can also remove security groups.

**Security groups associated with the network interface (eni-050f45a8199f29d45)**

Security group ID	Security group name	Description	Owner ID	
sg-00f97944cc9dafc24	allow-http-ftp	allow-http-ftp	940482414422	<input type="button" value="Remove"/>
sg-0d472b7f0b0f234a1	default	default VPC security group	940482414422	<input type="button" value="Remove"/>

**Services**

Services

Features

Resources New

Documentation

Knowledge articles

Blog posts

Events

Tutorials

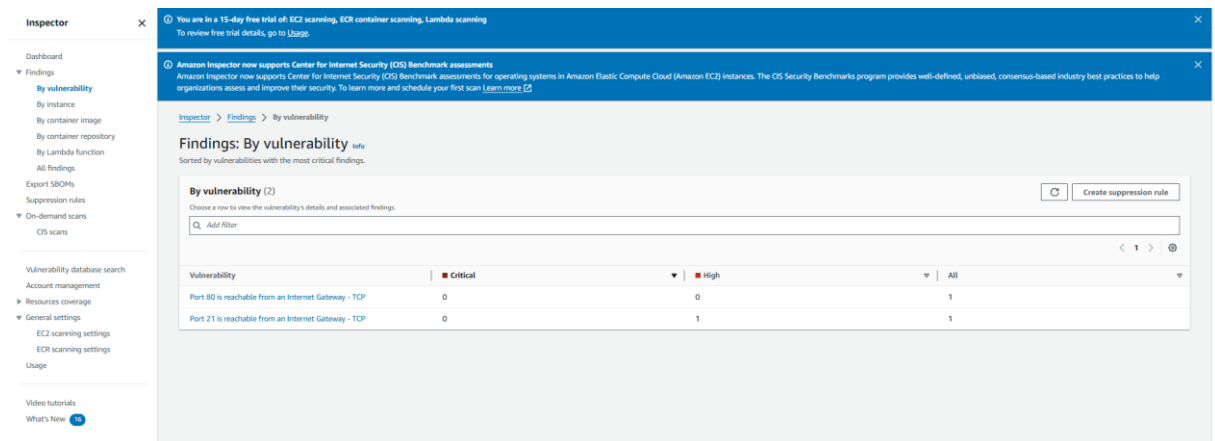
**Amazon FinSpace**  
Data processing and analytics for Capital Markets with Managed kdb Insights

**Amazon Inspector**  
Continuous vulnerability management at scale

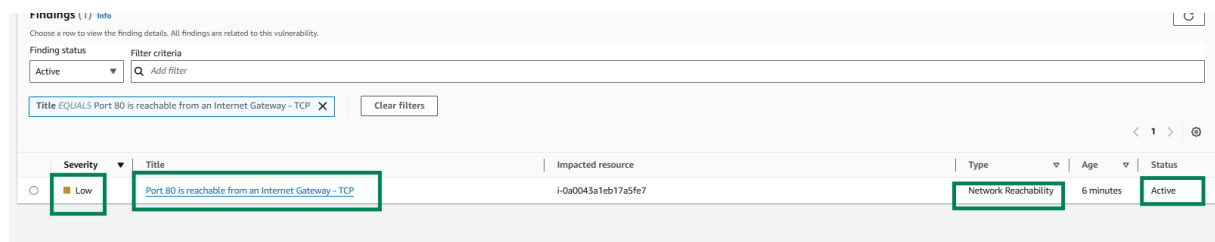
**Amazon Lookout for Vision**  
Identify defects using computer vision to automate quality inspection.

**Features**

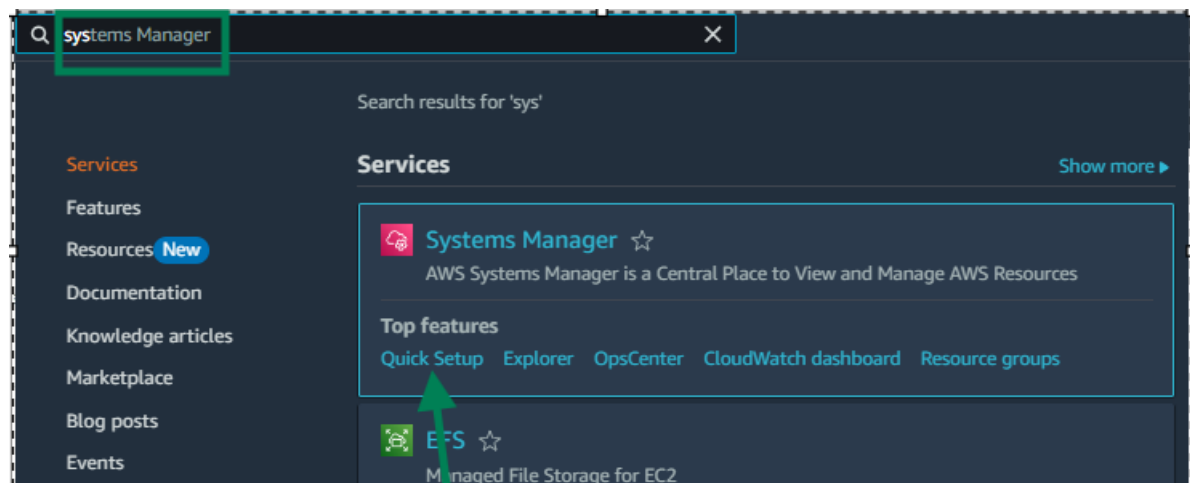
## TP 9 : AWS SSM & Inspector



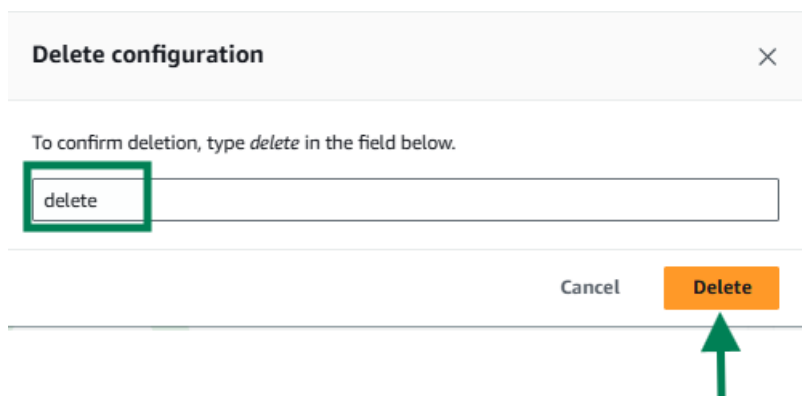
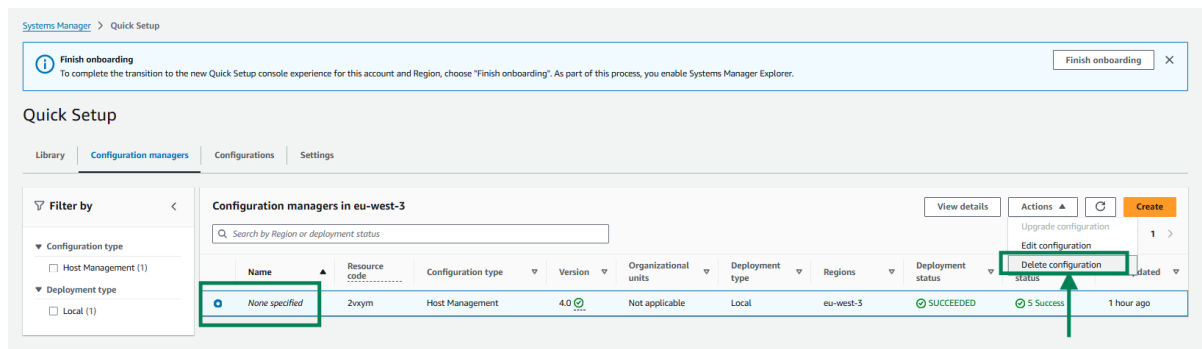
Vous devez avoir une vulnérabilité de haute criticité détectée par AWS Inspector, qui consiste à ce que le service FTP soit ouvert à toutes les destinations, ainsi qu'une autre de faible criticité, liée au service HTTP.



À la fin du TP, nous allons nettoyer tout. Commencez par désactiver **Systems Manager**.



## TP 9 : AWS SSM & Inspector



Désactivez **AWS Inspector**.