

Rendu - TP09

Compte rendu du TP09 effectué par Thomas PEUGNET.

Nous créons un Rôle EC2RoleforSSM.

The screenshot shows the AWS IAM Roles page. At the top, a green banner indicates that 'Role EC2RoleforSSM created.' Below this, the 'Roles (6)' section is displayed, listing six roles with their respective trusted entities and last activity. A table lists the roles:

Role name	Trusted entities	Last activity
AWSServiceRoleForAutoScaling	AWS Service: autoscaling (Service-Li	10 minutes ago
AWSServiceRoleForElasticLoadBalancing	AWS Service: elasticloadbalancing (S	12 minutes ago
AWSServiceRoleForOrganizations	AWS Service: organizations (Service-	-
AWSServiceRoleForSupport	AWS Service: support (Service-Linker	-
AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service	-
EC2RoleforSSM	AWS Service: ec2	-

Below the table, there are three sections: 'Roles Anywhere' (info), 'Access AWS from your non AWS workloads' (info), 'X.509 Standard' (info), and 'Temporary credentials' (info). The 'Temporary credentials' section includes a note about using AWS Certificate Manager Private Certificate Authority to authenticate identities. At the bottom of the page, there are links for CloudShell, Feedback, and a copyright notice.

Nous créons notre instance EC2 Linux Thomas Inspector.

The screenshot shows the AWS EC2 Instances page. On the left, there's a navigation sidebar with sections like Dashboard, EC2 Global View, Events, Instances (with sub-options like Instances, Instance Types, Launch Templates, etc.), Images, Elastic Block Store, Network & Security, Load Balancing, Auto Scaling, and CloudShell/Feedback.

The main area displays a table of instances. One instance, "EC2 Linux Tho...", is selected and shown in a detailed view below the table. The detailed view includes tabs for Details, Status and alarms, Monitoring, Security, Networking, Storage, and Tags. Under the Details tab, the "Instance summary" section provides information such as Instance ID (i-0b5809a8fa9a535fb), Public IPv4 address (13.39.48.222), Instance state (Running), Hostname type (IP name: ip-172-31-42-192.eu-west-3.compute.internal), Answer private resource DNS name (IPv4 (A)), Auto-assigned IP address (13.39.48.222 [Public IP]), and VPC ID (vpc-024ad8fd0fd5c3446).

Nous vérifions notre règle.

The screenshot shows the "Compare security group rules" page. At the top, it says "Compare security group rules info" and explains that Amazon EC2 evaluates all the rules of the selected security groups to control inbound and outbound traffic. It allows selecting more security groups to view their inbound rules.

The "Common security groups" section shows a dropdown menu with "Select security groups" and a list item "default sg-0945111edc8da4214 X". Below this, a note says "Security groups that you add or remove here will be added to or removed from all your network interfaces."

The "Inbound rules (1)" section shows a table with one rule:

Security group name	Security group ID	Type	Protocol	Port range	Source	Description
default	sg-0945111edc8da4214	All traffic	All	All	sg-0945111edc8da4214	-

At the bottom right, there are "Cancel" and "Select security groups" buttons.

Nous activons Inspector.

The screenshot shows the AWS Inspector dashboard. On the left, a sidebar lists navigation options like Dashboard, Findings, General settings, and Video tutorials. The main area displays several informational cards:

- Welcome to Inspector**: To get started, activate Amazon EC2, Amazon ECR, AWS Lambda scanning for your member accounts. Includes a "Manage all accounts" button.
- Welcome to Inspector. Your first scan is underway.**
- Inspector now supports deep inspection of EC2 Instances.** Amazon Inspector now supports deep inspection of EC2 instances. Includes a "Activate deep inspection" button.
- 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. Includes a "Learn more" link.
- 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. Includes a "Learn more" link.

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

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.

CloudShell **Feedback** © 2024, Amazon Web Services, Inc. or its affiliates. **Privacy** **Terms** **Cookie preferences**

Nous activons l'inspector sur notre account management.

The screenshot shows the AWS Inspector dashboard after account activation. The main area displays the following information:

You have successfully activated 1 account.

Summary (Info): Viewing data from all accounts.

Environment coverage: Your accounts, instances, and repositories that are activated with Inspector. Shows 100% coverage with 1 / 1 instance and 0 / 0 repositories.

Critical findings: All active critical findings in your environment. Shows 0 Critical findings across ECR container, EC2 instance, and Lambda functions.

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

Findings with public exploit available	Findings with fix available
0 / 0 total findings	0 / 0 total findings

Risk based remediations: Vulnerabilities impacting the most instances and images. Shows "No top at-risk packages" and "No top at-risk packages to display".

Container image scans within CI/CD pipeline (New): Assess your container images for vulnerabilities in CI/CD pipelines before deployment or pushing to container registries. Includes "How to use" and "How it works" sections.

CloudShell **Feedback** © 2024, Amazon Web Services, Inc. or its affiliates. **Privacy** **Terms** **Cookie preferences**

Nous constatons qu'AWS inspector a terminé de scanner notre instance.

The screenshot shows the AWS Inspector service interface. On the left, a sidebar contains navigation links for Inspector, Findings, Resources coverage, General settings, and Usage. The main content area displays a success message: "You have successfully activated 1 account." Below this, the "Account management" section shows a summary of instances: 1 Scanning, 1 Not scanning, and 0 Not configured. The "Instances" section lists one instance: "i-0b5809a8fa9a535fb" (Name: EC2 Linux Thomas Inspector). The instance details include Account (thomaspeugnet), AMI (ami-03216a20ecc5d...), Operating system (LINUX), Last scanned (December 11, 2024 ...), and Monitored using (Agent-based).

Nous avons visiblement quelques failles, probablement dues à des mises à jour non effectuées pour le moment.

The screenshot shows the AWS Inspector service interface, focusing on the findings for the EC2 instance "i-0b5809a8fa9a535fb". The "Details" section provides instance metadata: Launched at December 11, 2024 9:51 AM (UTC+01:00), Created by 794038237731, Role arn:aws:iam::794038237731:instance-profile/EC2RoleforSSM, and Security group default. The "Finding summary" indicates 0 Critical, 1 High, and 3 Medium vulnerabilities. The "Findings (5)" section lists five specific vulnerabilities:

Severity	Title	Type	Age	Status
High	CVE-2024-49996 - kernel, kernel-tools and 1 more	Package Vulnerability	3 minutes	Active
Medium	CVE-2024-6252 - python3, python3-libs	Package Vulnerability	3 minutes	Active
Medium	CVE-2024-35195 - python3-requests, python3-pip-wheel	Package Vulnerability	3 minutes	Active
Medium	CVE-2024-41080 - kernel, kernel-tools and 1 more	Package Vulnerability	3 minutes	Active
Untriaged	CVE-2024-34459 - libxml2	Package Vulnerability	3 minutes	Active

Nous configurons en Quick Setup notre Systems Manager.

AWS Systems Manager

Your Host Management Quick Setup was successfully created.

Name	Manager ARN	Resource code
<i>None specified</i>	arn:aws:ssm-quicksetup:eu-west-3:794038237731:configuration-manager/39f393fb-eddf-4c9b-9df9-556cd1b651f7	51hmg
Configuration type and version	Description	
Host Management 4.0	<i>None specified</i>	

Status **Settings** **Tags**

You are missing prerequisites for QuickSetup to work correctly in your account to resolve, choose "Finish onboarding". As part of this process, you enable Systems Manager Explorer.

Finish onboarding

Filter by

- Regions
- Deployment status
- Association status

Configuration deployment status

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

Total	Success	Failed	Pending
1	1	0	0

Configuration association status

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

Total	Success	Failed	Pending
5	1	0	4

Configuration details

Last updated: just now Configuration progress updated every 30 seconds.

Account	Region	Configuration deployment status	Configuration status
794038237731	eu-west-3	Success	1 Success 4 Pending

Search account ID

CloudWatch Dashboard CloudShell Feedback

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Nous démarrons une session sur notre instance.

Session ID: thomaspeu-2jk23z6d5qy2aczjeaejjdrsyu Instance ID: i-0b5809a8fa9a535fb **Terminate**

```
sh-5.2$ ifconfig
enX0: flags=4163<UP,BROADCAST,MULTICAST> mtu 9001
    inet 172.31.42.192 brd 172.31.42.255 netmask 255.255.240.0 broadcast 172.31.47.255
        ether 0e:31:a0:b1:7a:b5 txqueuelen 1000 (Ethernet)
        RX packets 106542 bytes 189528824 (180.7 MiB)
        RX errors 0 dropped 0 overruns 0 frame 0
        TX packets 20793 bytes 1754614 (1.6 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 brd 127.0.0.1 netmask 255.0.0.0
        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$
```

Nous constatons que l'adresse est bien celle de notre instance.

Screenshot of the AWS EC2 Instances details page for instance i-0b5809a8fa9a535fb.

Instance summary for i-0b5809a8fa9a535fb (EC2 Linux Thomas Inspector)

- Public IPv4 address:** 13.39.48.222
- Instance state:** Running
- VPC ID:** vpc-024ad8fd0fd5c3446
- Subnet ID:** subnet-05ba9dbb9df51e1c5
- Instance ARN:** arn:aws:ec2:eu-west-3:794038237731:instance/i-0b5809a8fa9a535fb

Details tab selected. Other tabs include Status and alarms, Monitoring, Security, Networking, Storage, and Tags.

Monitoring section shows:

- AMI ID: ami-03216a20ecc5d72ee
- AMI name: al2023-ami-2023.6.20241121.0-kernel-6.1-x86_64
- Stop protection: Disabled
- Launch time: Wed Dec 11 2024 09:51:59 GMT+0100 (heure normale d'Europe centrale) (12 minutes)

Platform details: Linux/UNIX

Termination protection: Disabled

AMI location: amazon/al2023-ami-2023.6.20241121.0-kernel-6.1-x86_64

Nous exécutons Patch Manager sur notre instance.

Screenshot of the AWS Systems Manager Patch Manager Association execution summary.

Operation was Successful

AWS-PatchNowAssociation

Association ID: 0f5768e3-abaf-43e8-a18f-7f27b7924ee9	Execution ID: 1f9e6351-f623-418d-b0bf-60dce8d68662
Status: Success	Operation: Scan
Reboot option: NoReboot	Targets: Instances: *
Summary: Success=1	

Scan/Install operation summary



Succeeded

Pending Skipped Succeeded Failed

Nous créons notre Security Group allow-http-ftp.

The screenshot shows the AWS VPC dashboard. A green banner at the top indicates that a security group was created successfully. The main page displays a security group named "sg-055dd9814ccf8452a - allow-http-ftp". The "Details" tab is selected, showing information such as the security group name, ID, owner, and inbound/outbound rules count. Below this, the "Inbound rules" tab is active, displaying two entries:

Name	Security group rule...	IP version	Type	Protocol	Port range	Source
-	sgr-08e75a7cd2c4e5051	IPv4	HTTP	TCP	80	0.0.0.0/0
-	sgr-0e0de9e87c7f91ef9	IPv4	Custom TCP	TCP	21	0.0.0.0/0

Nous ajoutons ce security group à notre instance.

The screenshot shows the EC2 Instances page with the instance "i-0b5809a8fa9a535fb" selected. A modal dialog titled "Change security groups" is open. It shows "Instance details" for the selected instance and lists "Associated security groups". The "Associated security groups" section shows the instance is currently associated with two security groups: "allow-http-ftp" and "default". The "Save" button at the bottom right of the dialog is highlighted.

Nous constatons en effet, lors du scan de notre instance, que nous avons une vulnérabilité sur le port 80.

Nous supprimons notre configuration SSM.

Nous désactivons AWS Inspector.

The screenshot shows the AWS Inspector Settings page. On the left, there's a sidebar with various navigation options like Dashboard, Findings, and General settings. The main area displays two notifications at the top: one about a 15-day free trial for EC2 scanning, ECR container scanning, and Lambda scanning, and another about Amazon Inspector adding re-scan configuration for ECR container image scanning. Below these notifications, the 'General' section of the Settings page is visible, featuring a 'Permissions' section and a 'Deactivated administrator' section. A modal dialog box titled 'Deactivate Inspector' is open in the center. It contains a warning message: 'When you deactivate Inspector, all of your data will be deleted and cannot be restored.' Below this is a text input field with the placeholder 'To confirm that you want to deactivate Inspector, type: Deactivate' containing the text 'deactivate'. At the bottom of the dialog are 'Cancel' and 'Deactivate Inspector' buttons, with the latter being orange. To the right of the dialog, there's a note: 'Choose a delegated administrator, Inspector is activated for that account.' At the bottom of the page, there are links for Video tutorials and What's New, along with standard footer links for CloudShell, Feedback, Privacy, Terms, and Cookie preferences.