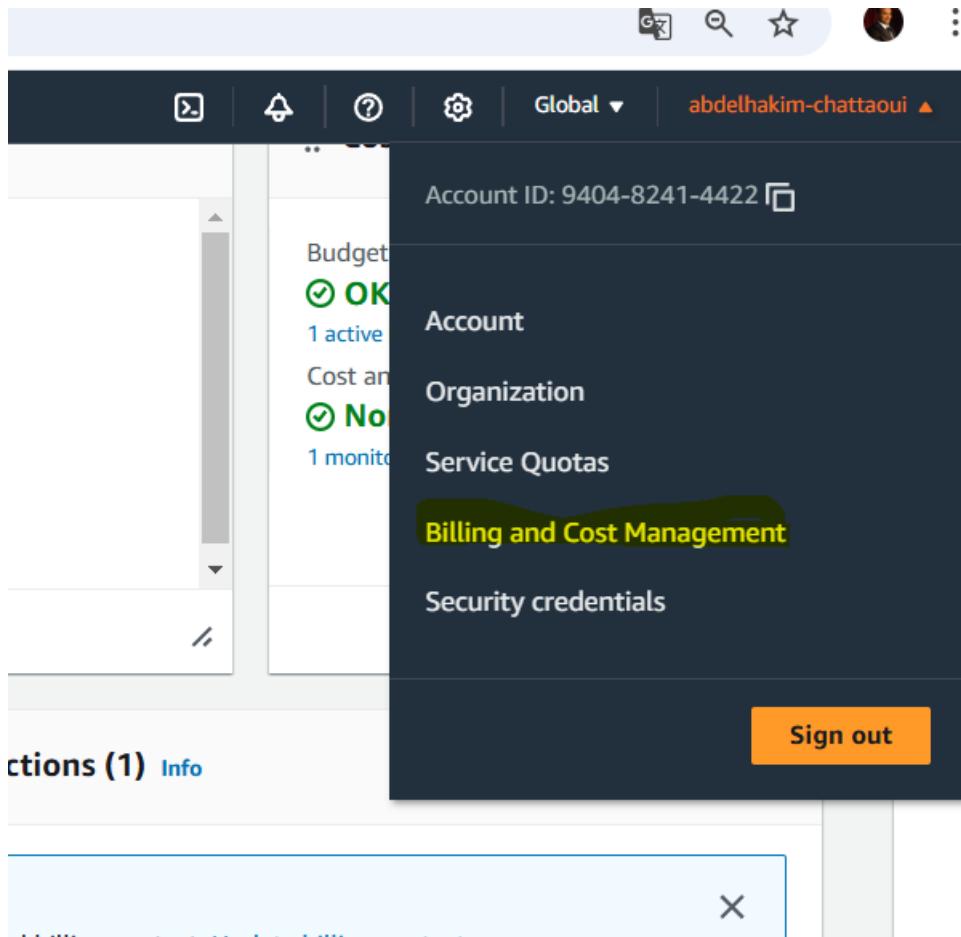


## Sécurisation de notre compte AWS

- 1- Configuration pour recevoir une alerte en cas de dépassement du **AWS Free Tier**.



The screenshot shows the AWS Billing Preferences page. On the left, a sidebar lists various preferences and settings, with 'Billing Preferences' highlighted. The main content area shows 'Billing preferences' with sections for 'Invoice delivery preferences' and 'Alert preferences'. Under 'Invoice delivery preferences', it says 'PDF invoices delivery by email' and 'Deactivated'. Under 'Alert preferences', it lists 'AWS Free Tier alerts' (Not delivered) and 'CloudWatch billing alerts' (Not delivered). At the bottom, there's a note about detailed billing reports and legacy pages.

Introducing the new AWS Billing preferences page experience  
We've redesigned the AWS Billing preferences. Let us know what you think.

Billing preferences

Invoice delivery preferences

PDF invoices delivery by email  
Deactivated

Alert preferences

AWS Free Tier alerts  
Not delivered

CloudWatch billing alerts  
Not delivered

Detailed billing reports (legacy)

Important: The AWS Cost & Usage report contains the most granular set of AWS cost and usage data available, including additional metadata about AWS services, pricing, and reservations (e.g., Amazon EC2 Reserved Instances). If you would like to access detailed information regarding your AWS costs and usage, we recommend creating an AWS Cost & Usage Report.

Legacy report delivery to S3  
No S3 configured

## Billing preferences Info

### Invoice delivery preferences Info

Edit

PDF invoices delivery by email

Deactivated

### Alert preferences Info

Receive AWS Free Tier alerts

If this option is selected, your AWS Free Tier usage alerts will be sent to the email address that you used to create your account. To send these alerts to a different email address, specify it below.

Email address to receive Free Tier usage alerts - *optional*

[REDACTED]@gmail.com

Receive CloudWatch billing alerts

Once enabled, this preference cannot be disabled.

Update

Cancel

 Your alert preferences were updated successfully.

### Invoice delivery preferences Info

Edit

PDF invoices delivery by email

Deactivated

### Alert preferences Info

Edit

AWS Free Tier alerts

Delivered to  
abdelhakim.chattaoui2@gmail.com

CloudWatch billing alerts

Not delivered

### Detailed billing reports (legacy) Info

Edit

### Invoice delivery preferences Info

Edit

PDF invoices delivery by email

Deactivated

### Alert preferences Info

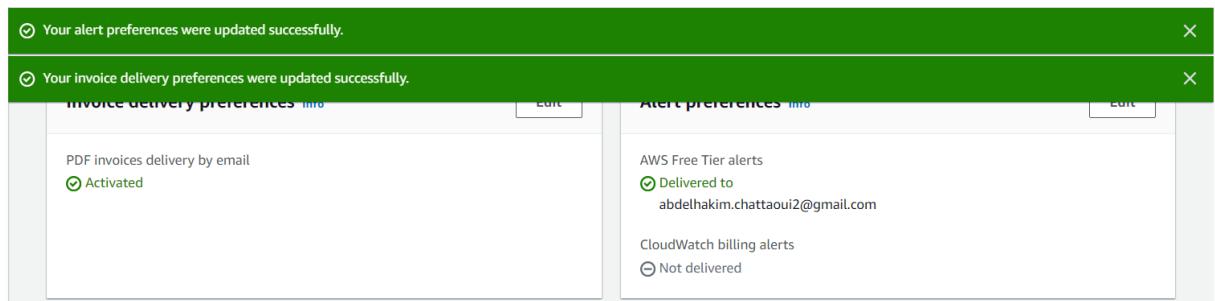
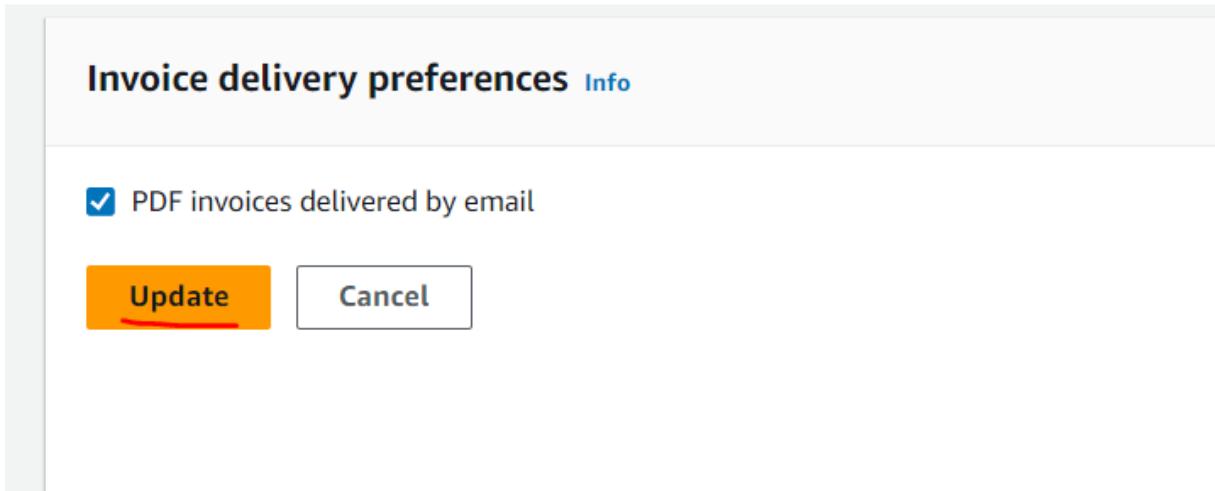
Edit

AWS Free Tier alerts

Delivered to  
abdelhakim.chattaoui2@gmail.com

CloudWatch billing alerts

Not delivered



## 2- Changement de la politique par défaut des mots de passe d'AWS

## Edit password policy Info

### Password policy

#### IAM default

Apply default password requirements.

#### Custom

Apply customized password requirements.

Password minimum length

8 characters

Password strength

Include a minimum of three of the following mix of character types:

- Uppercase
- Lowercase
- Numbers
- Non-alphanumeric characters

Other requirements

- Never expire password
- Must not be identical to your AWS account name or email address

[Cancel](#)

[Save changes](#)

## Edit password policy Info

### Password policy

IAM default

Apply default password requirements.

Custom

Apply customized password requirements.

#### Password minimum length.

Enforce a minimum length of characters.

**14** characters

Needs to be between 6 and 128.

#### Password strength

- Require at least one uppercase letter from the Latin alphabet (A-Z)
- Require at least one lowercase letter from the Latin alphabet (a-z)
- Require at least one number
- Require at least one non-alphanumeric character (! @ # \$ % ^ & \* ( ) \_ + - = [ ] { } | ')

#### Other requirements

- Turn on password expiration
- Password expiration requires administrator reset
- Allow users to change their own password
- Prevent password reuse

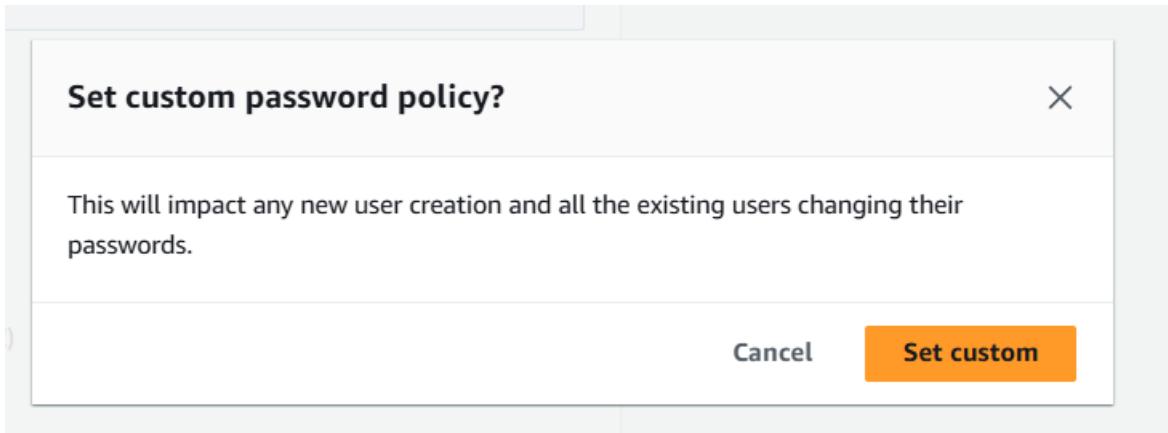
## COMBIEN DE TEMPS FAUT-IL À UN PIRATE POUR TROUVER VOTRE MOT DE PASSE 2024

[www.hivesystems.com/password](http://www.hivesystems.com/password)

Nombre de caractères	Nombres seulement	Lettres minuscules	Lettres majuscules et minuscules	Nombres, lettres majuscules et minuscules	Nombres, lettres majuscules et minuscules, symboles
4	Immédiat	Immédiat	3 secs	6 secs	9 secs
5	Immédiat	4 secs	2 mins	6 mins	10 mins
6	Immédiat	2 mins	2 heures	6 heures	12 heures
7	4 secs	50 mins	4 jours	2 semaines	1 mois
8	37 secs	22 heures	8 mois	3 ans	7 ans
9	6 mins	3 semaines	33 ans	161 ans	479 ans
10	1 heure	2 ans	1k ans	9k ans	33k ans
11	10 heures	44 ans	89k ans	618k ans	2M ans
12	4 jours	1k ans	4M ans	38M ans	164M ans
13	1 mois	29k ans	241M ans	2Md ans	11Md ans
14	1 an	766k ans	12Md ans	147Md ans	805Md ans
15	12 ans	19M ans	652Md ans	9Bn ans	56Bn ans
16	119 ans	517M ans	33Bn ans	566Bn ans	3qd ans
17	1k ans	13Md ans	1qd ans	35qd ans	276qd ans
18	11k ans	350Md ans	91qd ans	2qn ans	19qn ans



> 12 x RTX 4090 | bcrypt



⌚ Password requirements for IAM users are updated.

[IAM](#) > [Account Settings](#)

## Account settings Info

**Password policy** Info

Configure the password requirements for the IAM users.

This AWS account uses the following custom password policy:

Password minimum length <b>14 characters</b>	Other requirements • <b>Never expire password</b>
Password strength <ul style="list-style-type: none"><li>Require at least one uppercase letter from the Latin alphabet (A-Z)</li><li>Require at least one lowercase letter from the Latin alphabet (a-z)</li><li>Require at least one number</li><li>Require at least one non-alphanumeric character</li></ul>	

- 3- Créeation d'un budget mensuel de 5 dollars et réception d'une notification lorsque 85 % de ce budget est atteint.

Billing and Payments

- Bills
- Payments
- Credits
- Purchase Orders

**Cost Analysis**

- Cost Explorer
- Cost Explorer Saved Reports
- Cost Anomaly Detection
- Free Tier
- Data Exports

**Cost Organization**

- Cost Categories
- Cost Allocation Tags
- Billing Conductor

**Budgets and Planning**

- Budgets** (highlighted)
- Budgets Reports
- Pricing Calculator

**Savings and Commitments**

**Choose budget type**

**Budget setup**

- Use a template (simplified)  
Use the recommended configurations. You can change some configuration options after the budget is created.
- Customize (advanced)  
Customize a budget to set parameters specific to your use case. You can customize the time period, the start month, and specific accounts.

**Templates - new**

Choose a template that best matches your use case.

- Zero spend budget  
Create a budget that notifies you once your spending exceeds \$0.01 which is above the AWS Free Tier limits.
- Monthly cost budget  
Create a monthly budget that notifies you if you exceed, or are forecasted to exceed, the budget amount.
- Daily Savings Plans coverage budget  
Create a coverage budget for your Savings Plans that notifies you when you fall below the defined target.
- Daily reservation utilization budget  
Create a utilization budget for your reservations that notifies you when you fall below the defined target.

**Monthly cost budget - Template**

Billing and Payments

- Bills
- Payments
- Credits
- Purchase Orders

**Cost Analysis**

- Cost Explorer
- Cost Explorer Saved Reports
- Cost Anomaly Detection
- Free Tier
- Data Exports

**Cost Organization**

- Cost Categories
- Cost Allocation Tags
- Billing Conductor

**Budgets and Planning**

- Budgets**
- Budgets Reports
- Pricing Calculator

**Savings and Commitments**

Provide a descriptive name for this budget.

My Monthly Cost Budget

Names must be between 1-100 characters.

Enter your budgeted amount (\$)

Last month's cost:

Email recipients

Specify the email recipients you want to notify when the threshold has exceeded.

Scope

All AWS services are in scope in this budget.

You will be notified when 1) your **actual spend** reaches 85% 2) your **actual spend** reaches 100% 3) if your **forecasted spend** is expected to reach 100%.

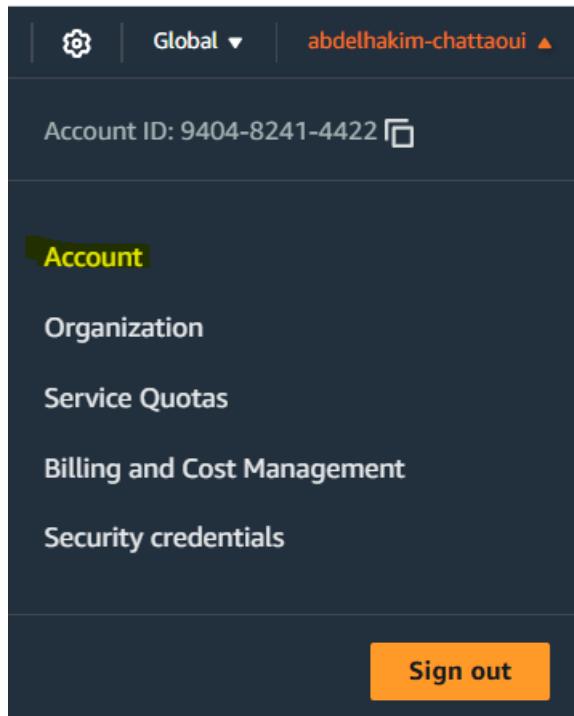
**Template settings**

This template has default configurations that can be changed later. To change any of these settings, see **Custom**. You can also download this template in **JSON**.

Create budget

Budgets (1) <small>Info</small>						
		<input type="button" value="Download CSV"/>		Actions ▾		<b>Create budget</b>
		<input type="text" value="Find a budget"/>		Type - Show all budgets ▾	< 1 > ⌂	
	Name	▲   Thresholds	▼   Budget	Amount used	Forecasted a...	Current vs. budgeted ▾   For...
<input type="checkbox"/>	<a href="#">My Monthly Cost Budget</a>	<input type="button" value="OK"/>	\$5.00	\$0.00	-	0.00%

4- Activation de l'accès des utilisateurs IAM aux informations de facturation.



**IAM user and role access to Billing information** Info

IAM user/role access to billing information

Deactivated

[Edit](#)

**IAM user and role access to Billing information** Info

Activate IAM Access

Cancel [Update](#)

**IAM user and role access to Billing information** Info

IAM user/role access to billing information

Activated

[Edit](#)

**5- RBAC :** Nous allons ajouter un groupe *facturation*, lui attribuer les droits de facturation et y ajouter l'utilisateur *mathias*.

### Ajoutez un groupe

The screenshot shows the AWS IAM User groups page. The left sidebar is titled "Identity and Access Management (IAM)" and includes "User groups" under "Access management". The main content area is titled "User groups (0) Info" and contains a message: "A user group is a collection of IAM users. Use groups to specify permissions for a collection of users." Below this is a search bar and a table header with columns: "Group name", "Users", "Permissions", and "Creation time". A message at the bottom states "No resources to display".

The screenshot shows the "Create user group" page. The left sidebar is identical to the previous one. The main content area has a "Name the group" section with a "User group name" field containing "facturation". Below it is an "Add users to the group - Optional (0) Info" section with a search bar and a table header for "User name". A message at the bottom says "No resources to display".

### Attacher la policy *Billing* au groupe facturation

The screenshot shows the "Attach permissions policies - Optional (1/949) Info" page. The left sidebar is identical. The main content area has a search bar and a table header for "Policy name". A filter bar at the top right shows "Filter by Type" and "All types" with "4 matches". The table lists four policies, with the last one, "Billing", being checked. The table columns are: "Policy name", "Type", "Used as", and "Description". The "Billing" row has a tooltip: "Grants permissions for billing and cost...".

The screenshot shows the AWS Identity and Access Management (IAM) console. On the left, the navigation pane is visible with sections like 'Access management' (User groups, Roles, Policies, Identity providers, Account settings), 'Access reports' (Access Analyzer), and 'Dashboard'. The main content area is titled 'User groups' and shows a single entry: 'facturation' (Info). A green checkmark icon next to 'Defined' indicates the group was created successfully. The status bar at the top right says 'facturation user group created.'

Vérifiez que la permission a bien été accordée au groupe.

This screenshot shows the detailed view of the 'facturation' user group. The 'Permissions' tab is selected. It lists one attached policy: 'Billing' (AWS managed - job function). The ARN of the group is also displayed.

Ajoutez un utilisateur nommé **Mathias** et associez-le au groupe **facturation**.

The screenshot shows the AWS IAM 'Users' page. The 'Users' tab is selected in the navigation pane. The main content area displays a table with columns: 'User name', 'Path', 'Group', 'Last activity', 'MFA', 'Password age', and 'Console last sign-in'. A message at the bottom states 'No resources to display'.

IAM > Users > Create user

Step 1  
Specify user details

Step 2  
Set permissions

Step 3  
Review and create

## Specify user details

**User details**

User name

The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = . @ \_ - (hyphen)

Provide user access to the AWS Management Console - optional  
If you're providing console access to a person, it's a best practice [to manage their access in IAM Identity Center.](#)

**Info** If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. [Learn more](#)

**Cancel** **Next**

IAM > Users > Create user

Step 1  
Specify user details

Step 2  
Set permissions

Step 3  
Review and create

## Set permissions

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. [Learn more](#)

**Permissions options**

- Add user to group  
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.
- Copy permissions  
Copy all group memberships, attached managed policies, and inline policies from an existing user.
- Attach policies directly  
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

**User groups (1/1)**

Group name	Users	Attached policies	Created
<input checked="" type="checkbox"/> facturation	0	Billing	2024-09-25 (8 minutes ago)

**Set permissions boundary - optional**

**Cancel** **Previous** **Next**

Step 1  
Specify user details

Step 2  
Set permissions

Step 3  
Review and create

## Review and create

Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.

**User details**

User name <input type="text" value="Mathias"/>	Console password type None	Require password reset No
---	-------------------------------	------------------------------

**Permissions summary**

Name	Type	Used as
<input type="checkbox"/> facturation	Group	Permissions group

**Tags - optional**

Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

No tags associated with the resource.

**Add new tag**  
You can add up to 50 more tags.

**Cancel** **Previous** **Create user**

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

**Users**

Roles

IAM > Users

Users (1) Info

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

Search

User name / Group: Last activity MFA Password age Console last sign-in

User name	Path	Group	Last activity	MFA	Password age	Console last sign-in
Mathias	/	1	-	-	-	-

Pour réaliser les tests avec l'utilisateur, nous allons lui ajouter l'accès à la console.

Identity and Access Management (IAM)

Search IAM

Dashboard

Access management

User groups

**Users**

Roles

Policies

Identity providers

Account settings

Access reports

Access Analyzer

External access

Unused access

IAM > Users > Mathias

Mathias Info

Delete

Summary

ARN arn:aws:iam: <b>[REDACTED]</b> :user/Mathias	Console access Disabled	Access key 1 <a href="#">Create access key</a>
Created September 25, 2024, 09:23 (UTC+02:00)	Last console sign-in -	

Permissions Groups (1) Tags Security credentials Last Accessed

Console sign-in

Enable console access

Console sign-in link <a href="https://[REDACTED].signin.aws.amazon.com/console">https://[REDACTED].signin.aws.amazon.com/console</a>	Console password Not enabled
---	---------------------------------

## Enable console access

X

Enable console access for Mathias.

Console password

- Autogenerated password  
 Custom password

.....

- Must be at least 8 characters long
- Must include at least three of the following mix of character types: uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), and symbols ! @ # \$ % ^ & \* ( ) \_ + - (hyphen) = [ ] { } | '

Show password

User must create new password at next sign-in

Users automatically get the [IAMUserChangePassword](#) policy to allow them to change their own password.

Cancel

Enable console access

## Console password



You have successfully enabled the user's new password.

This is the only time you can view this password. After you close this window, if the password is lost, you must create a new one.

Console sign-in URL

[https://\[REDACTED\].signin.aws.amazon.com/console](https://[REDACTED].signin.aws.amazon.com/console)

User name

Mathias

Console password

\*\*\*\*\* [Show](#)

[Download .csv file](#)

[Close](#)

## Add Entry



### Add Entry

Create a new entry.

General Advanced Properties Auto-Type History

Title:	PWD user Mathis	Icon:	
User name:	Mathias		
Password:	*****		
Repeat:	*****		
Quality:	78 bits	13 ch.	
URL:	<a href="https://[REDACTED].signin.aws.amazon.com/console">https://[REDACTED].signin.aws.amazon.com/console</a>		
Notes:			
<input type="checkbox"/> Expires:	25/09/2024 00:00:00		



OK

Cancel



Global ▾

Mathias @ [REDACTED]



Account ID: [REDACTED] ?

IAM user: Mathias

Account

Organization

Service Quotas

**Billing and Cost Management**

Security credentials

[Switch role](#)[Sign out](#)

The screenshot shows the AWS Billing and Cost Management home page. On the left, there's a navigation sidebar with sections like Home, Getting Started, Billing and Payments (with Bills, Payments, Credits, Purchase Orders), Cost Analysis (with Cost Explorer), and a link to Cost Explorer Saved Reports. The main content area is titled "Billing and Cost Management home" and contains a "Cost summary" section. It displays month-to-date cost (\$0.00), last month's cost for the same period (\$0.00 from Aug 1–26), total forecasted cost for the current month (Access denied), and last month's total cost (\$0.00). A "View bill" button is at the bottom right.

## Identity-Based Policy

Ajoute un utilisateur nommé « votre nom » et lui attribue le rôle d'administrateur.

The screenshot shows the AWS IAM Users page and the "Create user" wizard.

**IAM > Users**

**Users (1) Info**

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

User name	Path	Group	Last activity	MFA	Pass
Mathias	/	1	9 minutes ago	-	1

**IAM > Users > Create user**

**Specify user details**

**User details**

User name: hakim

The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = . @ \_ - (hyphen)

Provide user access to the AWS Management Console - optional  
If you're providing console access to a person, it's a best practice to manage their access in IAM Identity Center.

If you are creating programmatic access through access keys or service-specific credentials for AWS CodeCommit or Amazon Keyspaces, you can generate them after you create this IAM user. [Learn more](#)

Cancel **Next**

IAM > Users > Create user

Step 1  
[Specify user details](#)

---

Step 2  
**Set permissions**

---

Step 3  
Review and create

**Permissions options**

- Add user to group  
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.
- Copy permissions  
Copy all group memberships, attached managed policies, and inline policies from an existing user.
- Attach policies directly  
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

**Permissions policies (1229)**

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

**Create policy**

**Permissions policies (1229)**

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

Filter by Type

Policy name	Type	Attached entities
<input type="checkbox"/> <a href="#">AdministratorAccess</a>	AWS managed - job function	0

**AdministratorAccess**

Provides full access to AWS services and resources.

[Copy JSON](#)

```

1  {
2      "Version": "2012-10-17",
3      "Statement": [
4          {
5              "Effect": "Allow",
6              "Action": "*",
7              "Resource": "*"
8          }
9      ]
10 }

```

Policy name	Type	Attached entities
<input checked="" type="checkbox"/> <a href="#">AdministratorAccess</a>	AWS managed - job function	0

IAM > Users > Create user

Step 1 Specify user details

Step 2 Set permissions

Step 3 Review and create

### Review and create

Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.

User details		
User name	Console password type	Require password reset
hakim	None	No

### Permissions summary

Name	Type	Used as
AdministratorAccess	AWS managed - job function	Permissions policy

### Tags - optional

Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

No tags associated with the resource.

Add new tag

You can add up to 50 more tags.

Cancel Previous Create user

IAM > Users

**Users (2) Info**

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

User name	Path	Group	Last activity	MFA	Password age	Console last sign-in	Access key ID	Active key age
hakim	/	0	-	-	-	-	-	-
Mathias	/	1	16 minutes ago	-	17 hours	September 26, 2024, 0...	-	-

**hakim Info**

**Summary**

ARN arn:aws:iam:█████████████████████:user/hakim	Console access Disabled	Access key 1 Create access key
Created September 26, 2024, 03:22 (UTC+02:00)	Last console sign-in -	

Permissions Groups Tags Security credentials Last Accessed

**Console sign-in**

Console sign-in link https://██████████████████████.signin.aws.amazon.com/console	Console password Not enabled
--	---------------------------------

Enable console access

## Enable console access

X

Enable console access for hakim.

### Console password

- Autogenerated password  
 Custom password

\*\*\*\*\*

- Must be at least 8 characters long
- Must include at least three of the following mix of character types: uppercase letters (A-Z), lowercase letters (a-z), numbers (0-9), and symbols ! @ # \$ % ^ & \* ( ) \_ + - (hyphen) = [ ] { } | '

Show password

User must create new password at next sign-in

Users automatically get the [IAMUserChangePassword](#) policy to allow them to change their own password.

Cancel

[Enable console access](#)

## Console password



You have successfully enabled the user's new password.

This is the only time you can view this password. After you close this window, if the password is lost, you must create a new one.

Console sign-in URL



[https://\[REDACTED\].signin.aws.amazon.com/console](https://[REDACTED].signin.aws.amazon.com/console)

User name



hakim

Console password



\*\*\*\*\* [Show](#)

[Download .csv file](#)

[Close](#)

**Add Entry**  
Create a new entry.

General Advanced Properties Auto-Type History

Title:	<input type="text" value="hakim admin aws"/>	Icon:	
User name:	<input type="text" value="hakim"/>		
Password:	<input type="password" value="*****"/>	•••	
Repeat:	<input type="password" value="*****"/>		
Quality:	66 bits	12 ch.	
URL:	<input type="text" value="https://[REDACTED]signin.aws.amazon.com/console"/>		
Notes:	<input type="text" value=""/>		
Expires:	<input type="text" value="26/09/2024 00:00:00"/>	<input type="button" value="Calendar"/>	<input type="button" value="Clock"/>
Tools		<input type="button" value="OK"/>	<input type="button" value="Cancel"/>

Activez le MFA pour l'utilisateur récemment ajouté.

Multi-factor authentication (MFA) (0)			
Use MFA to increase the security of your AWS environment. Signing in with MFA requires an authentication code from an MFA device. Each user can have a maximum of 8 MFA devices assigned. <a href="#">Learn more</a>			
Type	Identifier	Certifications	Created on
No MFA devices. Assign an MFA device to improve the security of your AWS environment			
<input type="button" value="Assign MFA device"/>			

# Select MFA device Info

## MFA device name

### Device name

This name will be used within the identifying ARN for this device.

**hakim-admin-aws**

Maximum 64 characters. Use alphanumeric and '+ = , . @ - \_' characters.

## MFA device

### Device options

In addition to username and password, you will use this device to authenticate into your account.



#### Passkey or security key

Authenticate using your fingerprint, face, or screen lock. Create a passkey on this device or use another device, like a FIDO2 security key.



#### Authenticator app

Authenticate using a code generated by an app installed on your mobile device or computer.



#### Hardware TOTP token

Authenticate using a code generated by Hardware TOTP token or other hardware devices.

Cancel

**Next**

## Authenticator app

A virtual MFA device is an application running on your device that you can configure by scanning a QR code.

1

Install a compatible application such as Google Authenticator, Duo Mobile, or Authy app on your mobile device or computer.

[See a list of compatible applications](#)

2

Show QR code

Open your authenticator app, choose **Show QR code** on this page, then use the app to scan the code. Alternatively, you can type a secret key.  
[Show secret key](#)

3

Type two consecutive MFA codes below

Enter a code from your virtual app below

MFA Code 1

Wait 30 seconds, and enter a second code entry.

MFA Code 2

Cancel

Previous

Add MFA

## Authenticator app

A virtual MFA device is an application running on your device that you can configure by scanning a QR code.

1

Install a compatible application such as Google Authenticator, Duo Mobile, or Authy app on your mobile device or computer.

[See a list of compatible applications](#)

2



Open your authenticator app, choose **Show QR code** on this page, then use the app to scan the code.

Alternatively, you can type a secret key. [Show secret key](#)

3

Type two consecutive MFA codes below

Enter a code from your virtual app below

977818

Wait 30 seconds, and enter a second code entry.

939347

Cancel

Previous

Add MFA

## Users (2) [Info](#)

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

[C](#)

[Delete](#)

[Create user](#)

<input type="checkbox"/>	User name	Path	Groups	Last activity	MFA	Password age	Console last sign-in	Access key ID
<input type="checkbox"/>	<a href="#">hakim</a>	/	0	-	Virtual	12 minutes	-	-
<input type="checkbox"/>	<a href="#">Mathias</a>	/	1	33 minutes ago	-	18 hours	September 26, 2024, 0...	-

Connectez-vous en tant qu'utilisateur administrateur récemment ajouté et vérifiez que vous avez bien les droits d'administrateur.



## Connexion en tant qu'utilisateur IAM

ID de compte (12 chiffres) ou alias de compte

[REDACTED]

Nom d'utilisateur :

hakim

Mot de passe :

.....

Se souvenir de ce compte

**Connexion**



# Multi-Factor Authentication

Saisissez un code MFA pour terminer la connexion.

Code MFA :

566501

Envoyer

[Annuler](#)

The screenshot shows the AWS Management Console interface. At the top, there's a navigation bar with the AWS logo, a 'Services' button, and a search bar containing the text 'ec2'. Below the search bar, the results for 'ec2' are displayed under the heading 'Search results for "ec2"'.

The left sidebar contains a navigation menu with the following items:

- EC2 Dashboard**
- EC2 Global View
- Events
- Instances** (selected, indicated by a dropdown arrow)
- Instances
- Instance Types
- Launch Templates
- Spot Requests
- Savings Plans
- Reserved Instances
- Dedicated Hosts
- Capacity
- Reservations **New**

Below the Instances section, there are two more collapsed sections:

- Images**
- ...

The main content area on the right is titled 'Services' and lists several services:

- EC2** ☆ Virtual Servers in the Cloud
- EC2 Image Builder** ☆ A managed service to automate build, customize and deploy OS images
- Recycle Bin** Protect resources from accidental deletion
- Amazon Inspector** ☆ Continual vulnerability management at scale

At the top right of the main content area, there are several small icons for filtering and navigating the results.

**EC2 Dashboard**

EC2 Global View

Events

▼ Instances

- Instances
- Instance Types
- Launch Templates
- Spot Requests
- Savings Plans
- Reserved Instances
- Dedicated Hosts
- Capacity
- Reservations [New](#)

**Resources**

You are using the following Amazon EC2 resources in the Europe (Stockholm) Region:

Instances (running)	0	Auto Scaling Groups	0
Capacity Reservations	0	Dedicated Hosts	0
Elastic IPs	0	Instances	0
Key pairs	0	Load balancers	0
Placement groups	0	Security groups	1
Snapshots	0	Volumes	0

[aws](#) | [Services](#) |  X ✖ ▲ ? ⚙️

**EC2 Dashboard**

EC2 Global View

Events

▼ Instances

- Instances
- Instance Types
- Launch Templates
- Spot Requests
- Savings Plans
- Reserved Instances
- Dedicated Hosts
- Capacity
- Reservations [New](#)

Search results for 'iam'

**Services**

- Features
- Resources [New](#)
- Documentation
- Knowledge articles
- Marketplace
- Blog posts
- Events
- Tutorials

**Services**

-  **IAM** ☆ Manage access to AWS resources
-  **IAM Identity Center** ☆ Manage workforce user access to multiple AWS accounts and cloud applications
-  **Resource Access Manager** ☆ Share AWS resources with other accounts or AWS Organizations
-  **AWS App Mesh** ☆

**Identity and Access Management (IAM)**

**Dashboard**

**Access management**

- User groups
- Users
- Roles
- Policies
- Identity providers
- Account settings

**Access reports**

- Access Analyzer
- External access
- Unused access
- Analyzer settings
- Credential report

**IAM Dashboard**

**Security recommendations** 0

- Root user has MFA
- You have MFA
- Your user, hakim, does not have any active access keys that have been unused for more than a year.

**IAM resources**

Resources in this AWS Account

User groups	Users	Roles	Policies
1	2	2	0

\*\*\*\*\*

**Identity and Access Management (IAM)**

**Dashboard**

**Access management**

**User groups**

**User groups (1) Info**

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

Group name	Users	Permissions	Creation time
facturation	1	Defined	18 hours ago

6- Ajoutez un alias au compte AWS (au lieu de se connecter avec un ID de compte, nous allons nous connecter avec un alias qui est unique dans le monde).

Chacun de vous utilise son prénom-nom comme alias du compte AWS.

**Identity and Access Management (IAM)**

**Dashboard**

**Access management**

**User groups**

**IAM Dashboard**

**Security recommendations** 0

- Root user has MFA
- You have MFA
- Your user, hakim, does not have any active access keys that have been unused for more than a year.

**AWS Account**

Account ID: [REDACTED]  
**Create** Account Alias  
Sign-in URL for IAM users in this account: [https://\[REDACTED\].signin.aws.amazon.com/console](https://[REDACTED].signin.aws.amazon.com/console)

**IAM resources**

Resources in this AWS Account

User groups	Users	Roles	Policies	Identity providers
1	2	2	0	0

**Quick Links**

**My security credentials**

Manage your access keys, multi-factor authentication (MFA) and other credentials.

## Create alias for AWS account [REDACTED] X

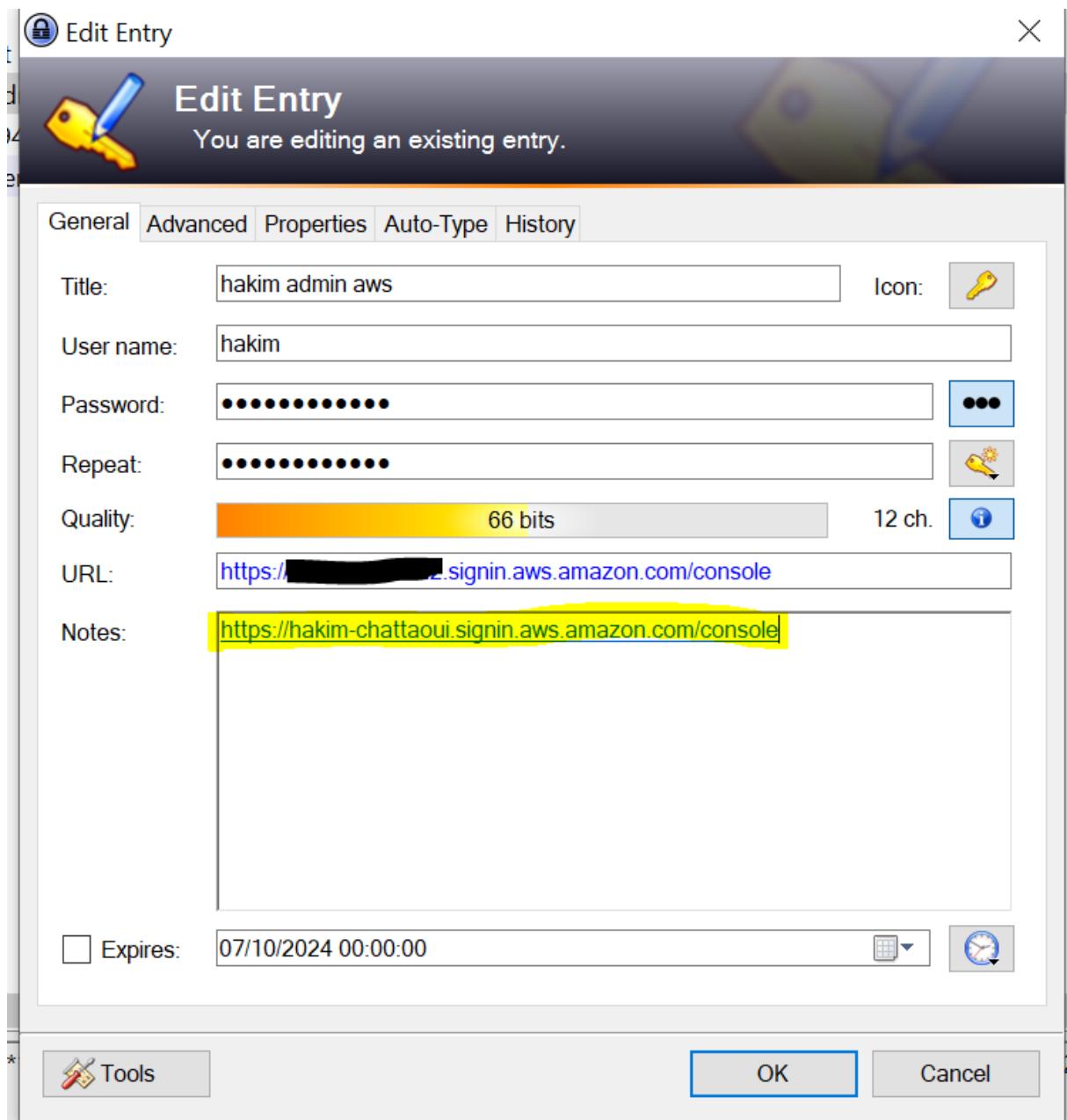
A  
au  
au  
au  
do  
tin  
ou

Preferred alias  
 Must be not more than 63 characters. Valid characters are a-z, 0-9, and - (hyphen).

New sign-in URL  
<https://hakim-chattaoui.signin.aws.amazon.com/console>

i IAM users will still be able to use the default URL containing the AWS account ID.

Cancel Create alias



Pour tester l'alias, il faut se déconnecter et essayer de se reconnecter en utilisant l'URL ci-après, qui contient le nom et non l'ID.

<https://hakim-chattaoui.signin.aws.amazon.com/console>



[https://eu-north-1.siginin.aws.amazon.com/oauth?client\\_id=arn%3Aaw](https://eu-north-1.siginin.aws.amazon.com/oauth?client_id=arn%3Aaw)



## Connexion en tant qu'utilisateur IAM

ID de compte (12 chiffres) ou alias de compte

hakim-chattaoui

Nom d'utilisateur :

Mot de passe :

Se souvenir de ce compte

**Connexion**

[Connexion à l'aide de l'adresse e-mail de l'utilisateur racine](#)

[Vous avez oublié votre mot de passe?](#)



## Connexion en tant qu'utilisateur IAM

ID de compte (12 chiffres) ou alias de compte

hakim-chattaoui

Nom d'utilisateur :

hakim

Mot de passe :

.....

Se souvenir de ce compte

Connexion

# Multi-Factor Authentication

Saisissez un code MFA pour terminer la connexion.

Code MFA :

737324

**Envoyer**

[Annuler](#)



Vérifiez que vous avez actuellement accès par l'alias récemment ajouté.

The screenshot shows the AWS Management Console Home page. At the top, there's a navigation bar with the AWS logo, a 'Services' dropdown, a search bar, and account information ('Paris' and 'hakim @ hakim-chattaoui'). Below the navigation, there's a sidebar with a 'Console Home' link and a 'Recently visited' section listing IAM, EC2, and Billing and Cost Management. To the right of the sidebar, there's a large 'Applications' section. It shows '0' applications in the region 'Europe (Paris)'. There's a 'Create application' button and a note saying 'No applications. Get started by creating an application.' A 'Create application' button is also located at the bottom of this section.

## RBAC

Parmi les bonnes pratiques recommandées par AWS, il est conseillé d'utiliser des groupes et d'attribuer les droits aux groupes plutôt qu'aux utilisateurs individuels. Pour cela, nous allons créer un groupe *admin* dans lequel nous allons ajouter l'utilisateur portant votre nom.

**Identity and Access Management (IAM)**

**User groups**

**User groups (1) Info**

A user group is a collection of IAM users. Use groups to specify permissions for a collection of users.

Group name	Users	Permissions	Creation time
facturation	1	Defined	1 month ago

**Create group**

**Identity and Access Management (IAM)**

**User groups**

**Create user group**

**Name the group**

User group name  
Enter a meaningful name to identify this group.  
**Admin**

Maximum 128 characters. Use alphanumeric and '+-=\_,@-' characters.

**Add users to the group - Optional (1/2) Info**

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

User name
<b>hakim</b>
Mathias

**Attach permissions policies - Optional (1/965) Info**

You can attach up to 10 policies to this user group. All the users in this group will have permissions that are defined in the selected policies.

Filter by Type

Policy name	Type	Used as
<b>AdministratorAccess</b>	AWS managed - job function	Permissions policy (1)

**AdministratorAccess**

Allows API Gateway to push logs to us...  
Provides full access to Amazon AppFlow...  
Provides read only access to Amazon A...  
Provides full access to Amazon AppStr...  
Amazon AppStream 2.0 access to AWS...  
Provides read only access to Amazon A...  
Default policy for Amazon AppStream ...

**Create user group**

The screenshot shows the AWS IAM User groups page. At the top, a green banner says "Admin user group created." On the right, there are "View group", "Delete", and "Create group" buttons. Below the banner, the page title is "User groups (2) Info". A subtitle says "A user group is a collection of IAM users. Use groups to specify permissions for a collection of users." There is a search bar and a table with the following data:

Group name	Users	Permissions	Creation time
Admin	1	Defined	Now
facturation	1	Defined	1 month ago

Pour sécuriser notre environnement et rester dans le **Free Tier**, nous allons ajouter les deux conditions suivantes :

- Interdire le lancement de machines virtuelles (VM) si elles ne sont pas de type *t2.micro*.
- Interdire le lancement de machines virtuelles (VM) en dehors de la région de Paris (eu-west-3).

Creation de la policy « allow-only-paris-region ».

The screenshot shows the AWS IAM Policies page. On the left, a sidebar menu includes "Identity providers", "Account settings", "Access management" (with "Policies" selected), "Access reports", "Access Analyzer", "External access", "Unused access", "Analyzer settings", "Credential report", and "Organization activity". The main area shows a table of policies:

Policy name	Type	Used as	Description
AccessAnalyzerServiceRolePolicy	AWS managed	None	Allow Access Analyzer to analyze resou...
AdministratorAccess	AWS managed - job function	Permissions policy (1)	Provides full access to AWS services an...
AdministratorAccess-Amplify	AWS managed	None	Grants account administrative permissi...
AdministratorAccess-AWSElasti...	AWS managed	None	Grants account administrative permissi...
AlexaForBusinessDeviceSetup	AWS managed	None	Provide device setup access to AlexaFo...
AlexaForBusinessFullAccess	AWS managed	None	Grants full access to AlexaForBusiness ...
AlexaForBusinessGatewayExec...	AWS managed	None	Provide gateway execution access to A...
AlexaForBusinessLifesizeDeleg...	AWS managed	None	Provide access to Lifesize AVS devices
AlexaForBusinessNetworkProfil...	AWS managed	None	This policy enables Alexa for Business ...
AlexaForBusinessPolyDelegate...	AWS managed	None	Provide access to Poly AVS devices

The screenshot shows the AWS IAM Policy Editor interface. On the left, there is a 'Policy editor' pane containing a JSON code editor with syntax highlighting. A red arrow points from the top-left towards the code area. On the right, there is a 'Statement' pane with tabs for 'Edit statement', 'Select a statement', and 'Add new statement'. A red arrow points from the top-right towards the 'Next' button at the bottom right of the pane. The bottom of the screen shows status information: 'JSON Ln 16, Col 0', '5977 of 6144 characters remaining', and security metrics: 'Security: 0', 'Errors: 0', 'Warnings: 0', and 'Suggestions: 0'. The 'Next' button is highlighted with a red arrow.

```

1 "Version": "2012-10-17",
2 "Statement": [
3     {
4         "Effect": "Deny",
5         "Action": "ec2:RunInstances",
6         "Resource": "*",
7         "Condition": {
8             "StringNotEquals": {
9                 "aws:RequestedRegion": "eu-west-3"
10            }
11        }
12    }
13 ]
14 }
15 }
16

```

Utilise le code JSON ci-après

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "ec2:RunInstances",
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "aws:RequestedRegion": "eu-west-3"
        }
      }
    }
  ]
}
```

## Review and create Info

Review the permissions, specify details, and tags.

### Policy details

#### Policy name

Enter a meaningful name to identify this policy.

allow-only-paris-region

Maximum 128 characters. Use alphanumeric and '+,-,@-\_-' characters.

#### Description - optional

Add a short explanation for this policy.

Maximum 1,000 characters. Use alphanumeric and '+,-,@-\_-' characters.

### Permissions defined in this policy Info

Edit

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it

Search

#### Explicit deny (1 of 427 services)

Service	▲   Access level	▼   Resource	Request condition
EC2	Limited: Write	All resources	aws:RequestedRegion != eu-west-3
Allow (0 of 427 services)			<input checked="" type="checkbox"/> Show remaining 426 services

### Add tags - optional Info

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 policy



⌚ Policy allow-only-paris-region created.

IAM > Policies

### Policies (1250) Info

A policy is an object in AWS that defines permissions.

Filter by Type			
<input type="text" value="Search"/>	All types	<   >	
Policy name	Type	Used as	
<input type="radio"/> <a href="#">AccessAnalyzerServiceRolePolicy</a>	AWS managed	None	
<input type="radio"/> <a href="#">AdministratorAccess</a>	AWS managed - job function	Permissions policy (1)	
<input type="radio"/> <a href="#">AdministratorAccess-Amplify</a>	AWS managed	None	
<input type="radio"/> <a href="#">AdministratorAccess-AWSElasticBeanstalk</a>	AWS managed	None	
<input type="radio"/> <a href="#">AlexaForBusinessDeviceSetup</a>	AWS managed	None	
<input type="radio"/> <a href="#">AlexaForBusinessFullAccess</a>	AWS managed	None	
<input type="radio"/> <a href="#">AlexaForBusinessGatewayExecution</a>	AWS managed	None	
<input type="radio"/> <a href="#">AlexaForBusinessLifesizeDelegatedAccess...</a>	AWS managed	None	
<input type="radio"/> <a href="#">AlexaForBusinessNetworkProfileServicePo...</a>	AWS managed	None	
<input type="radio"/> <a href="#">AlexaForBusinessPolyDelegatedAccessPolicy</a>	AWS managed	None	
<input type="radio"/> <a href="#">AlexaForBusinessReadOnlyAccess</a>	AWS managed	None	
<input type="radio"/> <a href="#">allow-only-paris-region</a>	Customer managed	None	

Appliquez cette policy au groupe **admin** qui contient l'utilisateur portant votre nom.

Identity and Access Management (IAM)

IAM > User groups > Admin

### Admin Info

Summary

User group name: Admin, Creation time: November 10, 2024, 10:21 (UTC+01:00), ARN: arn:aws:iam:940482414422:group/admin

Users (1) Permissions Last Accessed

Permissions policies (1) Info

You can attach up to 10 managed policies.

Filter by Type			
<input type="text" value="Search"/>	All types	<   >   ⌂	
Policy name	Type	Attached entities	
<input type="checkbox"/> <a href="#">AdministratorAccess</a>	AWS managed - job function	2	

Add permissions ▲ Attach policies ▼ Create inline policy

Attach permission policies to Admin

Current permission policies (1)

Other permission policies (1/963)

You can attach up to 10 managed policies to this user group. All of the users in this group inherit the attached permissions.

Filter by Type			
<input type="text" value="paris"/>	All types	<   >   ⌂	
Policy name	Type	Used as	Description
<input checked="" type="checkbox"/> <a href="#">allow-only-paris-region</a>	Customer managed	None	

Cancel **Attach policies** ⌂

**Policies attached to this user group.**

IAM > User groups > Admin

## Admin Info

**Summary**

User group name Admin	Creation time November 10, 2024, 10:21 (UTC+01:00)	ARN arn:aws:iam::940482-
--------------------------	---	-----------------------------

Users (1) **Permissions** Last Accessed

**Permissions policies (2) Info**

You can attach up to 10 managed policies.

Policy name	Type	Attached entities
<input type="checkbox"/> <a href="#">AdministratorAccess</a>	AWS managed - job function	2
<input type="checkbox"/> <a href="#">allow-only-paris-region</a>	Customer managed	1

Test de lancement d'une VM t2.micro en dehors de la région de Paris (eu-west-3).

aws Services  X

Identity and Access Management (IAM)

Search IAM

Dashboard

▼ Access management

- User groups**
- Users
- Roles
- Policies
- Identity providers
- Account settings

▼ Access reports

- Access Analyzer
- External access
- Unused access
- Analyzer settings
- Credential report
- Organization activity
- Service control policies

Search results for 'ec2'

**Services** Show more ▶

-  EC2 ☆  
Virtual Servers in the Cloud
-  EC2 Image Builder ☆  
A managed service to automate build, customize and deploy OS images
-  Recycle Bin  
Protect resources from accidental deletion

**Features** Show more ▶

- Dashboard  

- EC2 Instances  

- AMIs  


**Resources** / for a focused search

[Alt+S]

### Resources

You are using the following Amazon EC2 resources in the US East (N. Virginia) Region:

Instances (running)	0	Auto Scaling Groups	0	Capacity Reservations	0
Dedicated Hosts	0	Elastic IPs	0	Instances	0
Key pairs	0	Load balancers	0	Placement groups	0
Security groups	1	Snapshots	0	Volumes	0

### Launch instance

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

[Launch instance](#) | [Migrate a server](#)

Note: Your instances will launch in the US East (N. Virginia) Region

### Service health

AWS Health Dashboard

Region	Status
US East (N. Virginia)	This service is operating normally.

### Zones

Zone name	Zone ID
us-east-1a	use1-az6
us-east-1b	use1-az1
us-east-1c	use1-az2
us-east-1d	use1-az4
us-east-1e	use1-az3

EC2 Free Tier Offers for all AWS Regions.

2 EC2 free tier offers in use

End of month forecast

Exceeds free tier

View Global EC2 resources

Offer usage (monthly)

Linux EC2 Instances

749.465556 hours remaining

Storage space on EBS

29.99 GB remaining

US East (N. Virginia) us-east-1

US East (Ohio) us-east-2

US West (N. California) us-west-1

US West (Oregon) us-west-2

Asia Pacific (Mumbai) ap-south-1

Asia Pacific (Osaka) ap-northeast-3

Asia Pacific (Seoul) ap-northeast-2

Asia Pacific (Singapore) ap-southeast-1

Asia Pacific (Sydney) ap-southeast-2

Asia Pacific (Tokyo) ap-northeast-1

Canada (Central) ca-central-1

Europe (Frankfurt) eu-central-1

Europe (Ireland) eu-west-1

Europe (London) eu-west-2

Europe (Paris) eu-west-3

Europe (Stockholm) eu-north-1

South America (São Paulo) sa-east-1

There are 13 Regions that are not enabled for this account

[Alt+S]

### Resources

You are using the following Amazon EC2 resources in the Europe (Frankfurt) Region:

Instances (running)	0	Auto Scaling Groups	0	Capacity Reservations	0
Dedicated Hosts	0	Elastic IPs	0	Instances	0
Key pairs	1	Load balancers	0	Placement groups	0
Security groups	3	Snapshots	0	Volumes	0

### Launch instance

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

[Launch instance](#) | [Migrate a server](#)

Note: Your instances will launch in the Europe

### Service health

AWS Health Dashboard

Region	Status
Europe (Frankfurt)	This service is operating normally.

EC2 Free Tier Offers for all AWS Regions.

2 EC2 free tier offers in use

End of month forecast

Exceeds free tier

View Global EC2 resources

Offer usage (monthly)

Linux EC2 Instances

749.465556 hours remaining

Storage space on EBS

29.99 GB remaining

EC2 Free Tier Info

Offers for all AWS Regions.

2 EC2 free tier offers in use

End of month forecast

Exceeds free tier

View Global EC2 resources

Offer usage (monthly)

Linux EC2 Instances

749.465556 hours remaining

Storage space on EBS

29.99 GB remaining

EC2 > ... > Launch an instance

## 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  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

**Quick Start**

### Summary

Number of instances Info

Software Image (AMI)  
Amazon Linux 2023 AMI 2023.6.2... read more  
ami-0eddb4a4e7d846d6f

Virtual server type (instance type)  
t2.micro

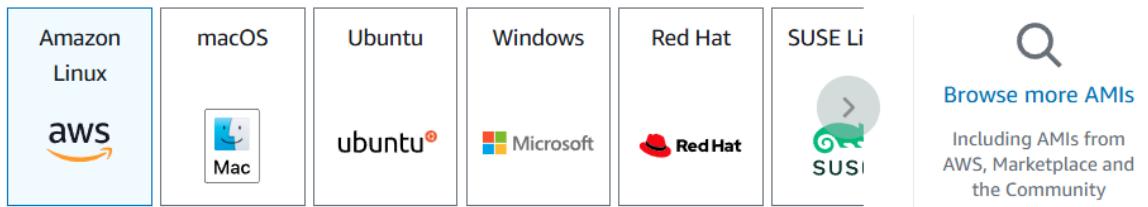
Firewall (security group)  
New security group

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

**Launch instance** Cancel Preview code

## Quick Start



### Amazon Machine Image (AMI)

Amazon Linux 2023 AMI ami-0eddb4a4e7d846d6f (64-bit (x86), uefi-preferred) / ami-012f2cc696716174e (64-bit (Arm), uefi) Virtualization: hvm ENA enabled: true Root device type: ebs	<b>Free tier eligible</b>
---	---------------------------

### 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 2023.6.20241031.0 x86\_64 HVM kernel-6.1

Architecture	Boot mode	AMI ID	Username	<small>i</small>
64-bit (x86) <small>▼</small>	uefi-preferred	ami-0eddb4a4e7d846d6f	ec2-user	<b>Verified provider</b>

**Quick Start**

Amazon Linux

macOS

Ubuntu

Windows

Red Hat

SUSE Li

Browse more AMIs
Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

**Amazon Linux 2023 AMI**  
 ami-0eddb4a4e7d846df (64-bit (x86), uefi-preferred) / ami-012f2cc696716174e (64-bit (Arm), uefi)  
 Virtualization: hvm ENA enabled: true Root device type: ebs

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 2023.6.20241031.0 x86\_64 HVM kernel-6.1

Architecture	Boot mode	AMI ID	Username	①
64-bit (x86)	uefi-preferred	ami-0eddb4a4e7d846df	ec2-user	Verified provider

**▼ Summary**

Number of instances | [Info](#)

**Software Image (AMI)**  
 Amazon Linux 2023 AMI 2023.6.2...read more  
 ami-0eddb4a4e7d846df

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

**Firewall (security group)**  
 New security group

**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

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



**Select an existing key pair or create a key pair**

We noticed that you didn't select a key pair. If you want to be able to connect to your instance it is recommended that you create one or select an existing one.

Existing key pair     Create new key pair

Proceed without key pair

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



## Vous devez avoir ce message d'erreur.

[EC2](#) > ... > Launch an instance

Instance launch failed  
 You are not authorized to perform this operation. User: arn:aws:iam::940482414422:user/hakim is not authorized to perform: ec2:RunInstances on resource: arn:aws:ec2:eu-central-1:940482414422:instance/ with an explicit deny in an identity-based policy. Encoded authorization failure message: TmY0KmL\_x518pye3RCWAz\_TD0HkXiocWk8E-IN3wfrdbQZ4vwVjImtKhdfGX09DgbDMUWrnPAPjFuXB\_K9sShjANDZ2-h80Jeg7B5bSKG9fmuWQqCL58FQRb\_Ek1kroygBV-oEkjXwjebjoFfpoPSuQq3dHsGQcbh49R9vN98kuSRBet5i1TLT9WsmyQeyysMd7VtNOvtZkEo79SC\_8e5jHVAxJgYccMrbkAOZSqp5\_BytSakUzd-hVR60ZozP4887iUS18burODCghRaUAK7EsPAdjogvpOz6jAq4dsjh1jRLkbQf6GirrajiOVduAHEDWl8gM-g2w2FesruARCom\_Adhwvn1Rb0t1HxqXwizCgzc-ZpcXfdCxum3LNxTx18auyJB3uDKf02AyNW1CON\_xeszR50916Z-na14VMGFje6LFx4kT9GWhf80fL\_GJURh916\_02cb55OwkrrwKwRy4\_7dE-WyyxCwSSpbIMV3Yvh-Ej35RqnAl8uAGoelpMOT0651crOs2mzRuLHckirLksfv4JWWVSNuCs\_tJSoyMC752Y0yUVHSrALOW-1NLPyndhm8ZMg7QyT9HKXNTzofZnevvK4m-Flu-Y8\_5Ch4tPlyCrujL1scJRU3\_NMBybTxbOsIHF08rvWnckThYezS6u41TYToitZbOH2zRdLY4brjaXNrtywVg8TC6vXvjdhNlmip6iudiZ7RdktdkjVhw2-eUk3fUCRSpPolzI4lvNeiHi2daJAMG51CBUYmN0ZVYE62z10BWFfskb24A0MDlwA41nHBEJJ-sg\_in\_rJGSRSU7T5sy2\_nHME6wFiNadathRjkdb3hJZsjWzUD\_0AblhTojNsUQEnv8

▼ Launch log

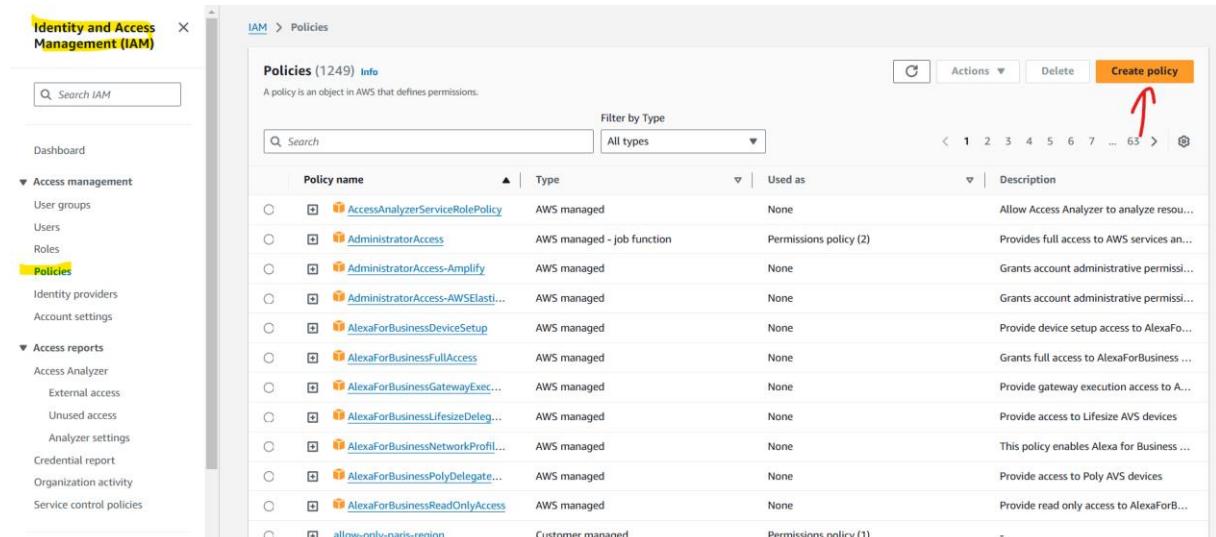
Initializing requests	<span style="color: green;">Succeeded</span>
Creating security groups	<span style="color: green;">Succeeded</span>
Creating security group rules	<span style="color: green;">Succeeded</span>
Launch initiation	<span style="color: red;">Failed</span>

[Cancel](#) [Edit instance config](#) [Retry failed tasks](#)

Si ce n'est pas le cas et que l'instance parvient à se lancer, merci de m'informer afin que je puisse vous aider à arrêter cette instance.

Passez à la mise en place de la deuxième policy qui interdit le lancement de machines virtuelles (VM) si elles ne sont pas de type *t2.micro* (Free).

Creation de la policy « allow-only-t2.micro ».



The screenshot shows the AWS IAM Policies page. On the left, there's a navigation sidebar with 'Identity and Access Management (IAM)' selected. The main area displays a table of policies:

Policy name	Type	Used as	Description
<a href="#">AccessAnalyzerServiceRolePolicy</a>	AWS managed	None	Allow Access Analyzer to analyze resou...
<a href="#">AdministratorAccess</a>	AWS managed - job function	Permissions policy (2)	Provides full access to AWS services an...
<a href="#">AdministratorAccess-Amplify</a>	AWS managed	None	Grants account administrative permis...
<a href="#">AdministratorAccess-AWSElasti...</a>	AWS managed	None	Grants account administrative permis...
<a href="#">AlexaForBusinessDeviceSetup</a>	AWS managed	None	Provide device setup access to AlexaFo...
<a href="#">AlexaForBusinessFullAccess</a>	AWS managed	None	Grants full access to AlexaForBusiness ...
<a href="#">AlexaForBusinessGatewayExec...</a>	AWS managed	None	Provide gateway execution access to A...
<a href="#">AlexaForBusinessLifesizeDeleg...</a>	AWS managed	None	Provide access to Lifesize AVS devices
<a href="#">AlexaForBusinessNetworkProfil...</a>	AWS managed	None	This policy enables Alexa for Business ...
<a href="#">AlexaForBusinessPolyDelegate...</a>	AWS managed	None	Provide access to Poly AVS devices
<a href="#">AlexaForBusinessReadOnlyAccess</a>	AWS managed	None	Provide read only access to AlexaForB...
<a href="#">allow-only-paris-region</a>	Customer managed	Permissions policy (1)	-

Utilise le code JSON ci-après

{

"Version": "2012-10-17",

"Statement": [

```
        "Effect": "Deny",
        "Action": "ec2:RunInstances",
        "Resource": "*",
        "Condition": {
            "StringNotEquals": {
                "ec2:InstanceType": "t2.micro"
            }
        }
    }
]
```

Step 1  
**Specify permissions** [Info](#)

Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.

Step 2  
Review and create

**Policy editor**

```
1▼ {  
2    "version": "2012-10-17",  
3    "statement": [  
4        {  
5            "effect": "Deny",  
6            "action": "ec2:RunInstances",  
7            "resource": "",  
8            "condition": {  
9                "StringNotIn": {  
10                    "ec2:InstanceType": "t1.micro"  
11                }  
12            }  
13        }  
14    ]  
15}  
16
```

**Visual** **JSON** **Actions**

**Edit statement**

**Select a statement**

Select an existing statement in the policy or add a new statement.

**+ Add new statement**

**+ Add new statement**

JSON: Line 16, Col 0

5981 of 6144 characters remaining

Security: 0 Errors: 0 Warnings: 0 Suggestions: 0

**Cancel** **Next**

IAM > Policies > Create policy

Step 1  
Specify permissions

Step 2  
Review and create

### Review and create Info

Review the permissions, specify details, and tags.

#### Policy details

**Policy name**  
Enter a meaningful name to identify this policy.  
**allow-only-t2.micro**  
Maximum 128 characters. Use alphanumeric and '+-=,@-\_.' characters.

**Description - optional**  
Add a short explanation for this policy.

Maximum 1,000 characters. Use alphanumeric and '+-=,@-\_.' characters.

#### Permissions defined in this policy Info

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it.

Search

##### Explicit deny (1 of 427 services)

Service	Access level	Resource	Request condition
<a href="#">EC2</a>	Limited: Write	All resources	ec2:InstanceType != t2.micro

**Permissions defined in this policy Info**

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it.

Search

**Edit**

##### Explicit deny (1 of 427 services)

Service	Access level	Resource	Request condition
<a href="#">EC2</a>	Limited: Write	All resources	ec2:InstanceType != t2.micro

**Show remaining 426 services**

##### Allow (0 of 427 services)

Service	Access level	Resource	Request condition
No resources to display			

**Add tags - optional Info**

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.

**Create policy**

Appliquez cette policy au groupe **admin** qui contient l'utilisateur portant votre nom.

Identity and Access Management (IAM)

IAM > User groups > Admin

**Admin Info**

**Edit**

#### Summary

User group name: **Admin** Creation time: November 10, 2024, 10:21 (UTC+01:00) ARN: arn:aws:iam:540482414422:group/Admin

#### Users in this group (1)

An IAM user is an entity that you create in AWS to represent the person or application that uses it to interact with AWS.

Search

User name	Last Accessed	Groups	Last activity	Creation time
<input checked="" type="checkbox"/> <b>valerie</b>	5 minutes ago	1	5 minutes ago	1 month ago

Screenshot of the AWS IAM 'Permissions' tab for a user named 'Admin'. The 'AdministratorAccess' policy is attached.

Policy name	Type	Attached entities
<a href="#">AdministratorAccess</a>	AWS managed - job function	2
<a href="#">allow-only-paris-region</a>	Customer managed	1

Screenshot of the 'Attach permission policies to Admin' dialog. The 'allow-only-t2.micro' policy is selected for attachment.

Policy name	Type	Used as	Description
<a href="#">allow-only-t2.micro</a>	Customer managed	None	-
<a href="#">AmazonOneEnterpriseInstallerAccess</a>	AWS managed	None	This policy grants limited read and write p...
<a href="#">AmazonRedshiftAllCommandsFullAccess</a>	AWS managed	None	This policy includes permissions to run SQ...
<a href="#">AWSApplicationMigrationAgentInstallationPolicy</a>	AWS managed	None	This policy allows installing the AWS Repli...
<a href="#">AWSDenyAll</a>	AWS managed	None	Deny all access
<a href="#">AWSElasticDisasterRecoveryAgentInstallationPolicy</a>	AWS managed	None	This policy allows installing the AWS Repli...
<a href="#">AWSElasticDisasterRecoveryFallbackInstallationPolicy</a>	AWS managed	None	You can attach the AWSElasticDisasterRec...
<a href="#">AWSIAMIdentityCenterAllowListForIdentityContext</a>	AWS managed	None	Provides the list of actions that are allowe...
<a href="#">ROSInstallerPolicy</a>	AWS managed	None	Allows the Red Hat OpenShift Service on A...

Screenshot of the 'Admin' user group summary page. The 'allow-only-t2.micro' policy is attached.

Policy name	Type	Attached
<a href="#">AdministratorAccess</a>	AWS managed - job function	2
<a href="#">allow-only-paris-region</a>	Customer managed	1
<a href="#">allow-only-t2.micro</a>	Customer managed	1

Test de lancement d'une VM t2.nano dans la région de Paris (eu-west-3).

Screenshot of the AWS CloudFormation console showing the "Launch instance" step.

**Resources**

You are using the following Amazon EC2 resources in the Europe (Paris) Region:

Instances (running)	0	Auto Scaling Groups	0	Capacity Reservations	0
Dedicated Hosts	0	Elastic IPs	0	Instances	0
Key pairs	1	Load balancers	0	Placement groups	0
Security groups	3	Snapshots	0	Volumes	0

**Launch instance**

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

**Service health**

AWS Health Dashboard

Region: Europe (Paris)

Status: This service is operating normally.

**Offer usage (monthly)**

Linux EC2 Instances: 749.465556 hours remaining

Storage space on EBS: 29.99 GB remaining

**Application and OS Images (Amazon Machine Image)**

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

**Quick Start**

- Amazon Linux
- Ubuntu
- Windows
- Red Hat
- SUSE Linux
- Debian

**Amazon Machine Image (AMI)**

**Amazon Linux 2023 AMI**

ami-0db5e28c1b3823bb7 (64-bit (x86), uefi-preferred) / ami-0849a4d04c8822ce6 (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 2023.6.20241031.0 x86\_64 HVM kernel-6.1

Architecture	Boot mode	AMI ID	Username	i
64-bit (x86) ▾	uefi-preferred	ami-0db5e28c1b3823bb7	ec2-user	Verified provider

## ▼ Instance type [Info](#) | [Get advice](#)

### Instance type

t2.nano

Family: t2 1 vCPU 0.5 GiB Memory Current generation: true  
On-Demand Ubuntu Pro base pricing: **0.0084 USD per Hour**  
On-Demand SUSE base pricing: 0.0066 USD per Hour  
On-Demand Linux base pricing: 0.0066 USD per Hour  
On-Demand Windows base pricing: 0.0089 USD per Hour

All generations

[Compare instance types](#)

Additional costs apply for AMIs with pre-installed software

▼ 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 X

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](#)

Software Image (AMI)  
Amazon Linux 2023 AMI 2023.6.2... [read more](#)  
ami-0db5e28c1b3823bb7

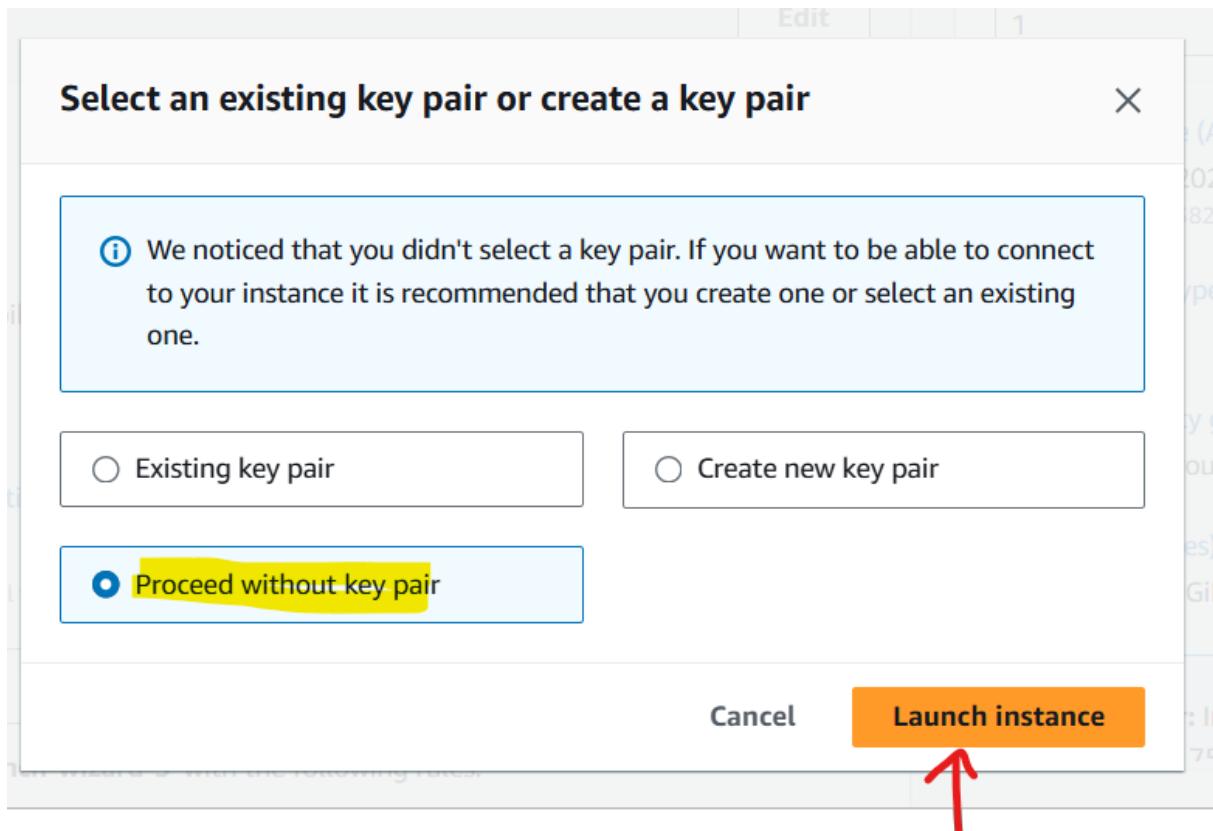
Virtual server type (instance type)  
t2.nano

Firewall (security group)  
New security group

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

ⓘ Free tier: In your first year includes 750 hours of t2.micro for X

Cancel **Launch instance** Preview code



Vous devez avoir ce message d'erreur.

**Instance launch failed**

You are not authorized to perform this operation. User: arn:aws:iam::940482414422:user/hakim is not authorized to perform: ec2:RunInstances on resource: arn:aws:ec2:eu-west-3:940482414422:instance/\* with an explicit deny in an identity-based policy. Encoded authorization failure message: -tKAYLLzIzVfp6DGsJy3T0Bi-L2eJRUKixQFR6\_SfMSUlwjsJ\_1jy29ydZk\_PBX3\_5YyPdhfxzvSt7hzYKQcVZeyn6zeCY\_2QLevb5h7wtxR13xcq7NVot2N4u4WPUeVg2Wr6qKpsqnvHloGJWuxbhE3-Gbax4tF9JTIWYLycf4qTjjTrx3cD7cjMq2bDRtu6CkNIjmVFtHujdTpUHNfGgJcGdLg7dSWELBypkZ7RXFMjWS1RHjd1t5KBlg\_LDfaz7y-AlgAvnMdrL2Z\_UwovUO8rJ8pkXDmijSEXXYcb6LspfBQadpMPX21QOP\_i\_ep2wUnGrsdpsysYP9HOYG2EPXWPD31IK\_PxqROqgksJe9imnYML4QjALJ546c6iuG2r8bIN\_zMtrHgiMKmfuXH5h5v7flaf0EbgKtepgyFxslqyjqkFP6NAgHg9S074hQHUPrVgKGwnUH-PuCa9cfkZxuYz\_JDRRWodBMK1IHeweRL9zJ9fiH4ZSNP-H3n28etk3j7CyzCdh140VnBglNT5g0JHRc4p6ZDxsSwisaGDD2U8skJrV--cp15bmefey6YY-IPdcusn4lm-Coko7\_gmdrhncfhmTxN8o9XurjLidLKSqxF9U1XaOODbvflb8ohKGnLgf45aHp7i0tNtzN16KDU6GfsDbgUYFxq624gjUJqnUFxWWJOTw80eAXLGsL\_IIEDQjRYV4Tiu-8AVjdn-H5bVe7WmESY\_zY7vpwKMbfxn74i30XbkD\_R40EzGqCZFlpZ5zg08Paj0N5Nrc2gYJgNzsxTv5MqGWk0VWNF-p1Gx37Wj4z5x28xgRNakpwvb5arXygL6kJgMDCg-QAFIvGzuSMqnlM'

**Launch log**

Initializing requests	<span style="color: green;">Succeeded</span>
Creating security groups	<span style="color: green;">Succeeded</span>
Creating security group rules	<span style="color: green;">Succeeded</span>
Launch initiation	<span style="color: red;">Failed</span>

**Action Buttons:** Cancel, Edit instance config, Retry failed tasks

Si ce n'est pas le cas et que l'instance parvient à se lancer, merci de m'informer afin que je puisse vous aider à arrêter cette instance.

## 7 ABAC : Nous allons gérer les autorisations AWS en nous basant sur les attributs

Ajoutez une policy nommée **EC2limitedAccess** avec le code JSON ci-après.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeImages",
                "ec2:DescribeTags"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:RebootInstances",
                "ec2:StartInstances",
                "ec2:StopInstances"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalTag/Department": "EC2Admins",
                    "ec2:ResourceTag/Environment": "Production"
                }
            }
        }
    ]
}
```

IAM > Policies > Create policy

Step 1  
Specify permissions

Step 2  
Review and create

### Specify permissions Info

Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.

**Policy editor**

Visual JSON Actions ▾

```

3 "Statement": [
4   {
5     "Effect": "Allow",
6     "Action": [
7       "ec2:DescribeInstances",
8       "ec2:DescribeImages",
9       "ec2:DescribeTags"
10    ],
11    "Resource": "*"
12  },
13  {
14    "Effect": "Allow",
15    "Action": [
16      "ec2:RebootInstances",
17      "ec2:StartInstances",
18      "ec2:StopInstances"
19    ],
20    "Resource": "*",
21    "Condition": {
22      "StringEquals": {
23        "aws:PrincipalTag/Department": "EC2Admins",
24        "aws:PrincipalTag/Environment": "Production"
25      }
26    }
27  }
28 ]

```

Edit statement

Select a statement

Select an existing statement in the policy or add a new statement.

+ Add new statement

IAM > Policies > Create policy

Step 1  
Specify permissions

Step 2  
Review and create

### Review and create Info

Review the permissions, specify details, and tags.

**Policy details**

**Policy name**  
Enter a meaningful name to identify this policy.  
  
Maximum 128 characters. Use alphanumeric and '+-=\_,@-' characters.

**Description - optional**  
Add a short explanation for this policy.  
  
Maximum 1,000 characters. Use alphanumeric and '+-=\_,@-' characters.

**Permissions defined in this policy Info**  
Edit

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it.

Search

Show remaining 426 services

**Allow (1 of 427 services)**

Service	▲   Access level	▼   Resource	Request condition
EC2	Limited: List, Write	All resources	Multiple

**Add tags - optional Info**  
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 policy

Identity and Access Management (IAM)

Policies (1251) Info

A policy is an object in AWS that defines permissions.

Policy name	Type	Used as	Description
AccessAnalyzerServiceRolePolicy	AWS managed	None	Allow Access Analyzer to analyze resou...
AdministratorAccess	AWS managed - job function	Permissions policy (2)	Provides full access to AWS services an...
AdministratorAccess-Amplify	AWS managed	None	Grants account administrative permisi...

Ajoutez un utilisateur nommé **testABAC** et affectez-lui la policy **EC2limitedAccess**.

Identity and Access Management (IAM)

Users (2) Info

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

User name	Path	Group	Last activity	MFA	Password age	Console last sign-in	Access key ID
hakim	/	1	4 hours ago	Virtual	45 days	November 10, 2024, 1...	-
Mathias	/	1	45 days ago	-	46 days	September 26, 2024, 0...	-

Create user

Specify user details

User details

User name: testABAC

Provide user access to the AWS Management Console - optional

If you're providing console access to a person, it's a best practice to manage their access in IAM Identity Center.

Cancel Next

IAM > Users > Create user

Step 1  
Specify user details

Step 2  
Set permissions

Step 3  
Review and create

## Set permissions

Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. [Learn more](#)

### Permissions options

- Add user to group  
Add user to an existing group, or create a new group. We recommend using groups to manage user permissions by job function.
- Copy permissions  
Copy all group memberships, attached managed policies, and inline policies from an existing user.
- Attach policies directly  
Attach a managed policy directly to a user. As a best practice, we recommend attaching policies to a group instead. Then, add the user to the appropriate group.

### Permissions policies (1/1252)

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

Filter by Type		1 match
<input type="text" value="Q_ limitedA"/>	All types	< 1 >
<input checked="" type="checkbox"/> Policy name	Type	Attached entities
<input checked="" type="checkbox"/> EC2limitedAccess	Customer managed	0

▶ Set permissions boundary - optional

Cancel Previous Next

Ajoutez des tags à l'utilisateur testABAC avec key= Department et value= EC2Admins

IAM > Users > Create user

Step 1  
Specify user details

Step 2  
Set permissions

Step 3  
Review and create

## Review and create

Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.

### User details

User name	Console password type	Require password reset
testABAC	None	No

### Permissions summary

Name	Type	Used as
EC2limitedAccess	Customer managed	Permissions policy

### Tags - optional

Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

No tags associated with the resource.

Add new tag

You can add up to 50 more tags.

Cancel Previous Create user

IAM > Users > Create user

Step 1  
Specify user details

Step 2  
Set permissions

Step 3  
**Review and create**

### Review and create

Review your choices. After you create the user, you can view and download the autogenerated password, if enabled.

User details		
User name testABAC	Console password type None	Require password reset No

### Permissions summary

Name	Type	Used as
<a href="#">EC2limitedAccess</a>	Customer managed	Permissions policy

### Tags - optional

Tags are key-value pairs you can add to AWS resources to help identify, organize, or search for resources. Choose any tags you want to associate with this user.

Key	Value - optional
Department	EC2Admins

Add new tag

You can add up to 49 more tags.

Lancez une instance EC2 de type *t2.micro* avec le tag suivant : key = Environment et value = Production.

aws | Services Search for ec2

**Dashboard**

- EC2 Global View
- Events
- Instances**
  - Instances
  - Instance Types
  - Launch Templates
  - Spot Requests
  - Savings Plans
  - Reserved Instances
  - Dedicated Hosts
  - Capacity
  - Reservations [New](#)
- Images**
  - AMIs
  - Custom AMIs

**Services**

Search results for 'ec2'

- EC2** ☆ Virtual Servers in the Cloud
- EC2 Image Builder ☆ A managed service to automate build, customize and deploy OS images
- Recycle Bin Protect resources from accidental deletion

**Features**

- Dashboard
- EC2 feature

**Dashboard**

EC2 Global View

Events

**Instances**

- Instances
- Instance Types
- Launch Templates
- Spot Requests
- Savings Plans
- Reserved Instances
- Dedicated Hosts
- Capacity
- Reservations [New](#)

**Images**

- AMIs
- AMI Catalog

**Elastic Block Store**

- Volumes
- Snapshots
- Lifecycle Manager

**Resources**

You are using the following Amazon EC2 resources in the Europe (Paris) Region

Instances (running)	0	Auto Scaling Groups	0
Dedicated Hosts	0	Elastic IPs	0
Key pairs	1	Load balancers	0
Security groups	4	Snapshots	0

**Launch instance**

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

[Launch instance](#) ▾

[Migrate a server](#) ↗

Note: Your instances will launch in the Europe (Paris) Region

**Service health**

AWS Health

Region  
Europe (Paris)

Status  
 This service is healthy

**Zones**

Name  
EC2 test ABAC

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

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

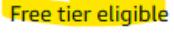
Recents    Quick Start

Amazon Linux    Ubuntu    Windows    Red Hat    SUSE Linux    Debian

aws    ubuntu®    Microsoft    Red Hat    SUSE    debian

Browse more AMIs   
Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Amazon Linux 2023 AMI   
Free tier eligible

ami-0db5e28c1b3823bb7 (64-bit (x86), uefi-preferred) / ami-0849a4d04c8822ce6 (64-bit (Arm), uefi)  
Virtualization: hvm    ENA enabled: true    Root device type: ebs

▼ 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 X

Add new volume

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

0 x File systems Edit

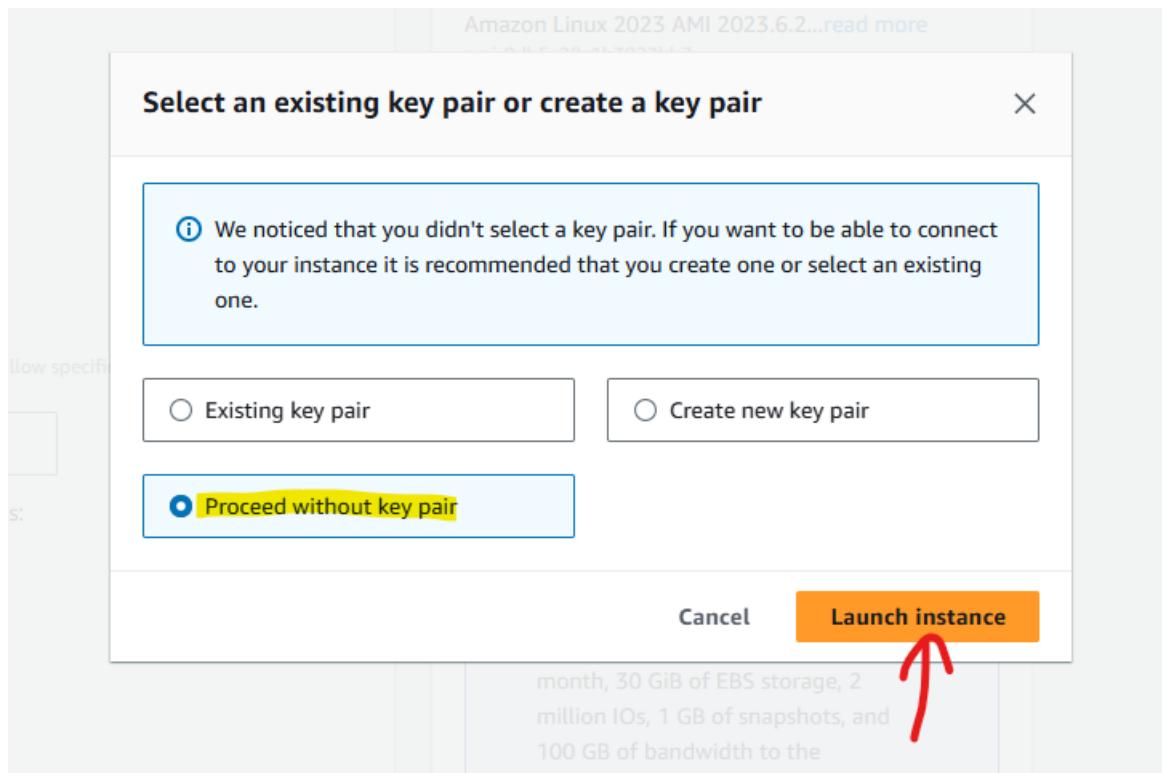
► Advanced details [Info](#)

New security group

Storage (volumes)  
1 volume(s) ~ 8 GiB

ⓘ Free tier: In your first year includes X  
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 I/Os, 1 GB of snapshots, and 100 GB of bandwidth to the internet.

Cancel    Launch instance   
Preview code



Instance state = running  Clear filters

Name	Value	Environment	Value
ENVIRONMENT	Production	ENVIRONMENT	Production

i-0b10d8b95d375f6c4

Details    Status and alarms    Monitoring    Security    Networking    Storage    **Tags**

Tags

Key	Value
Environment	Production

Manage tags

**i-09d8eab642e06cea6**

Details | Status and alarms | Monitoring | Security | Networking | Storage | **Tags**

Tags	
<input type="text"/>	
Key	Value
Environment	Production

Lance une desiemme Instence EC2 avec la tag key= Environment value = Dev

EC2 > Instances > i-093bfda43d2e8b85b > Manage tags

**Manage tags** Info

A tag is a custom label that you assign to an AWS resource. You can use tags to help organize and identify your instances.

Key	Value - optional
<input type="text"/> Environment	<input type="text"/> Dev

**Add new tag**

You can add up to 49 more tags.

Cancel **Save**

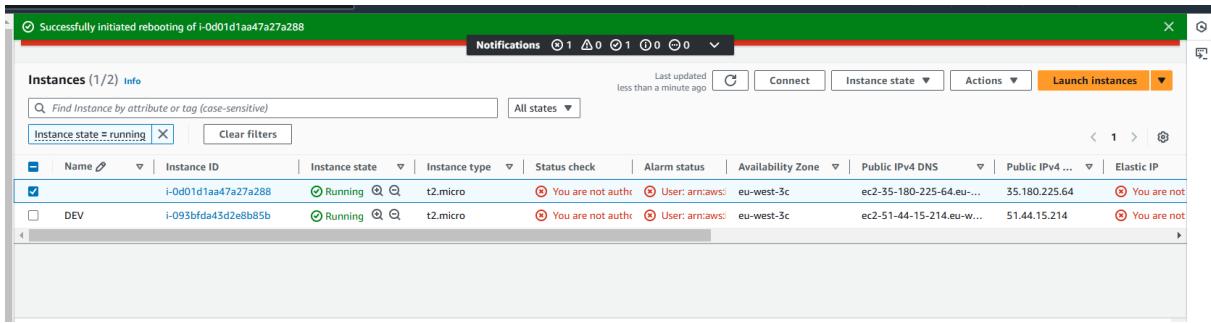
Connectez-vous en tant qu'utilisateur **testABAC**.

Vérifiez que les deux instances sont à l'état *Running*.

Instances (2/2) Info

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...
Production	i-0d01d1aa47a27a288	<span>Running</span>	t2.micro	<span>2/2 checks passed</span>	<span>View alarms</span>	eu-west-3c	ec2-35-180-225-64.eu...	35.180.225.64
DEV	i-093bfda43d2e8b85b	<span>Running</span>	t2.micro	<span>2/2 checks passed</span>	<span>View alarms</span>	eu-west-3c	ec2-51-44-15-214.eu-w...	51.44.15.214

Testez le redémarrage de l'instance *Production* (l'action doit réussir).



Testez le redémarrage de l'instance Dev (l'action doit échouer).