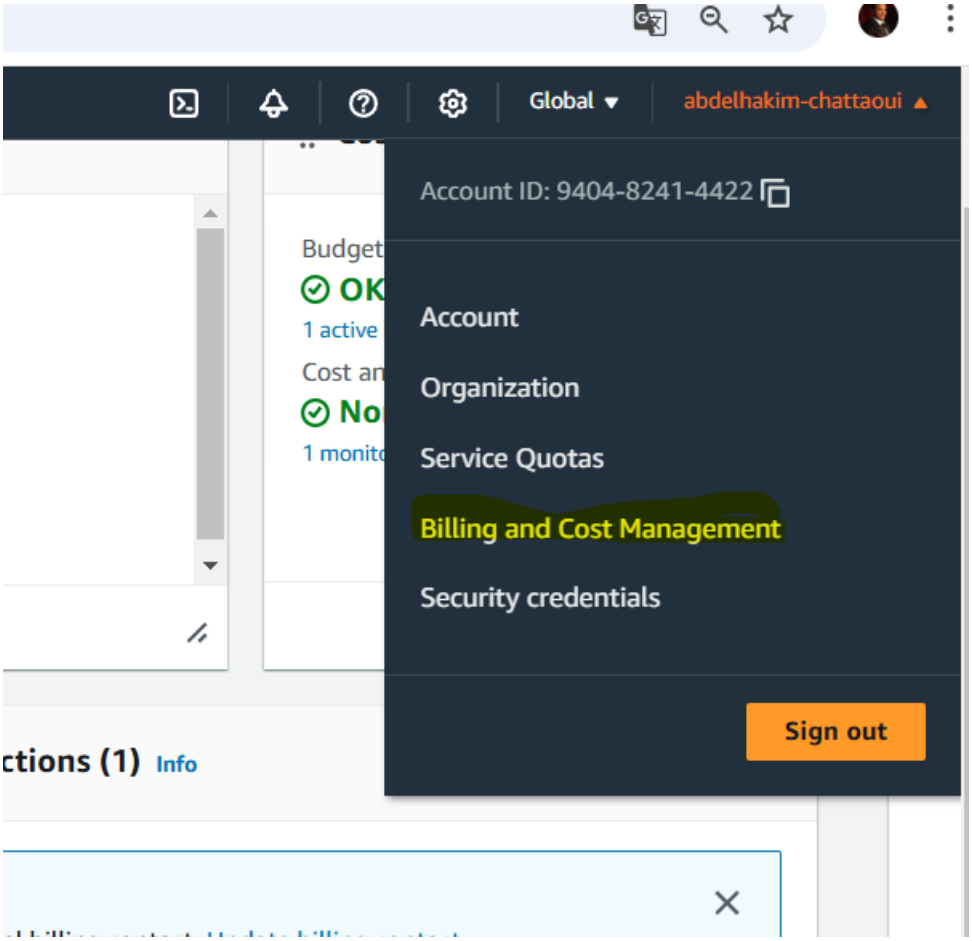
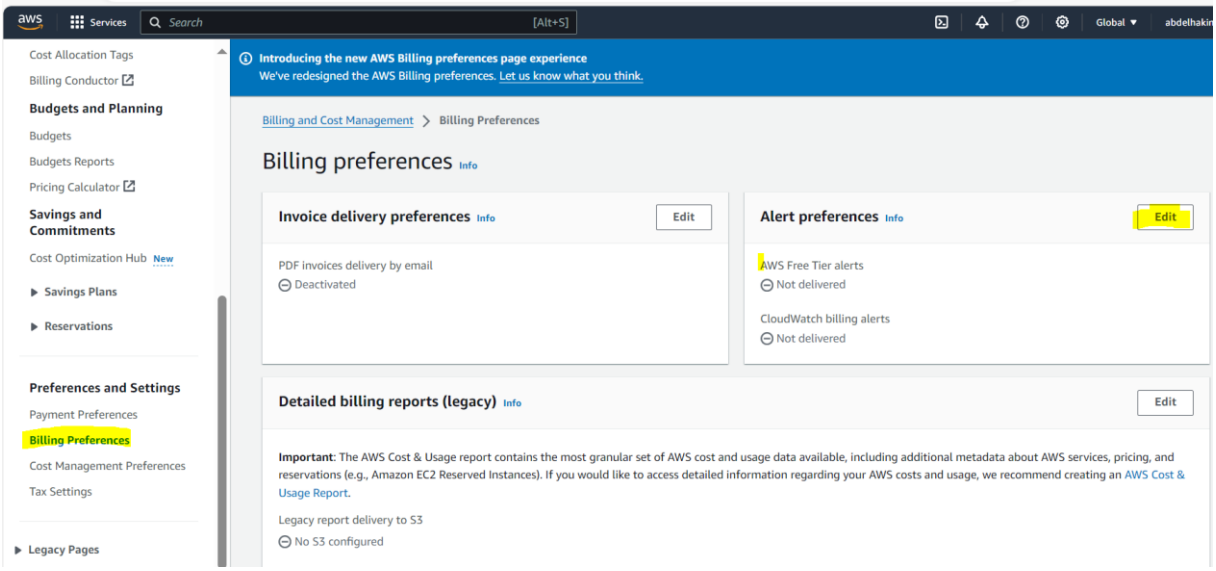
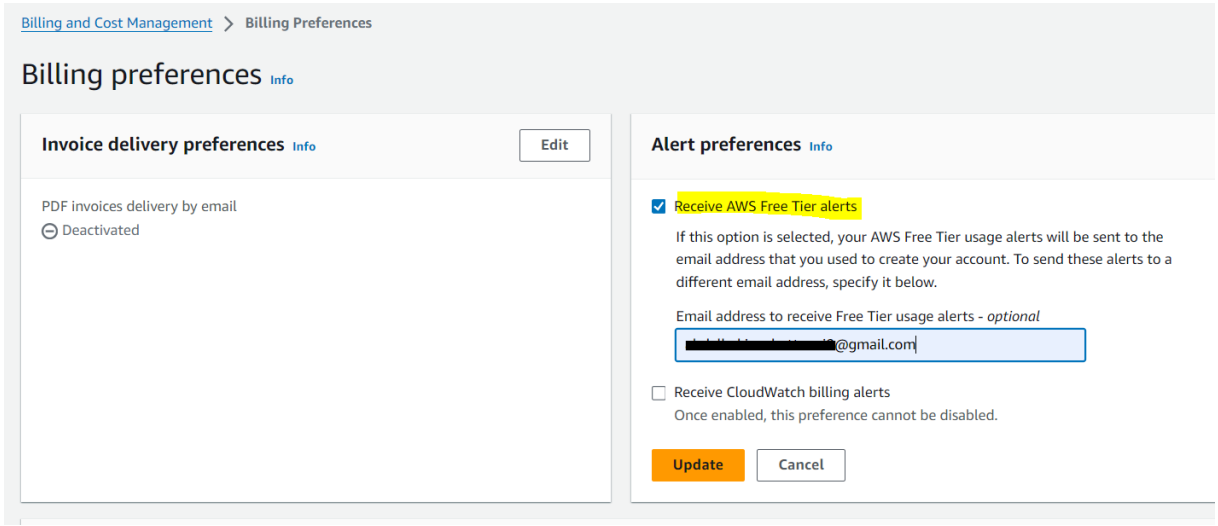
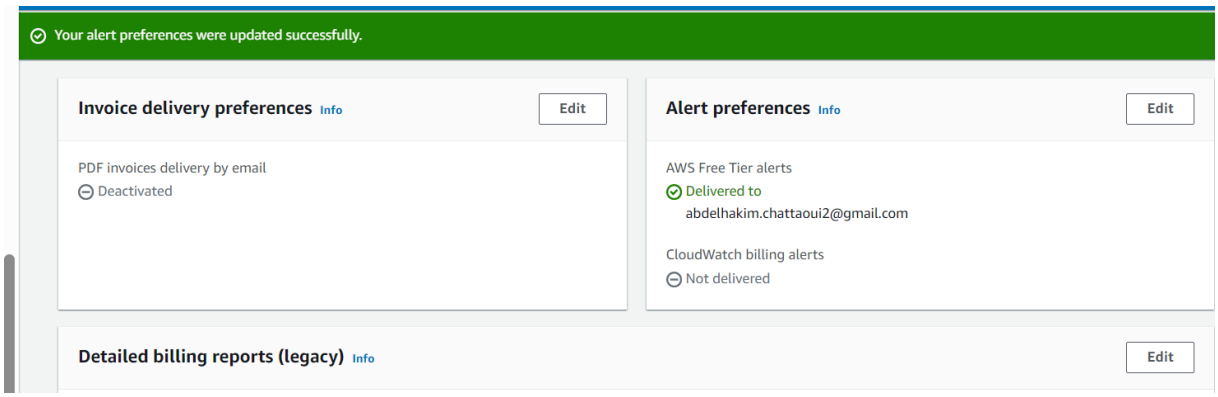
Sécurisation de notre compte AWS

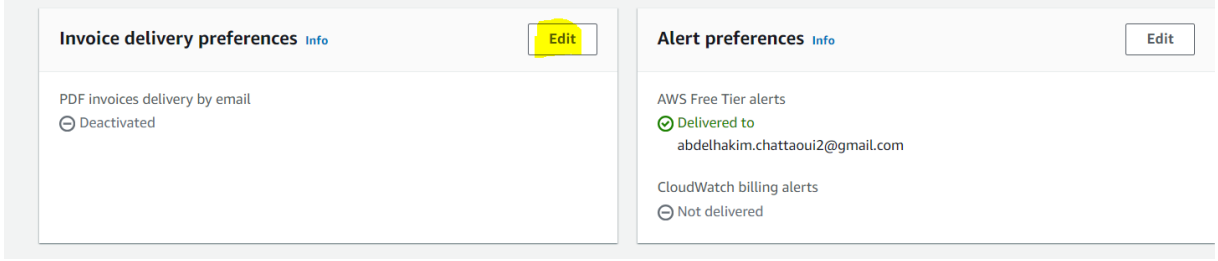
1- Configuration pour recevoir une alerte en cas de dépassement du **AWS Free Tier**.

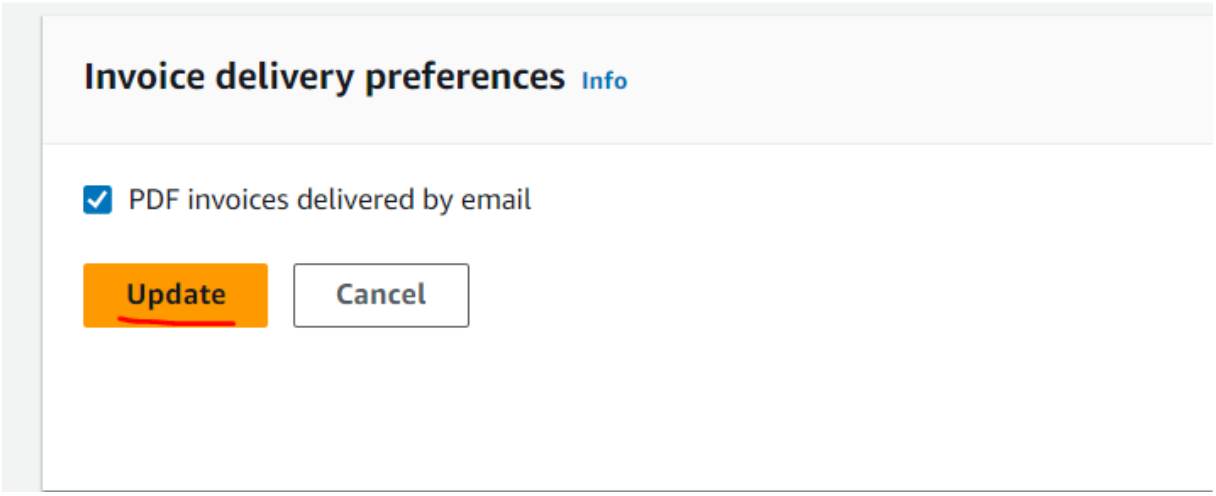


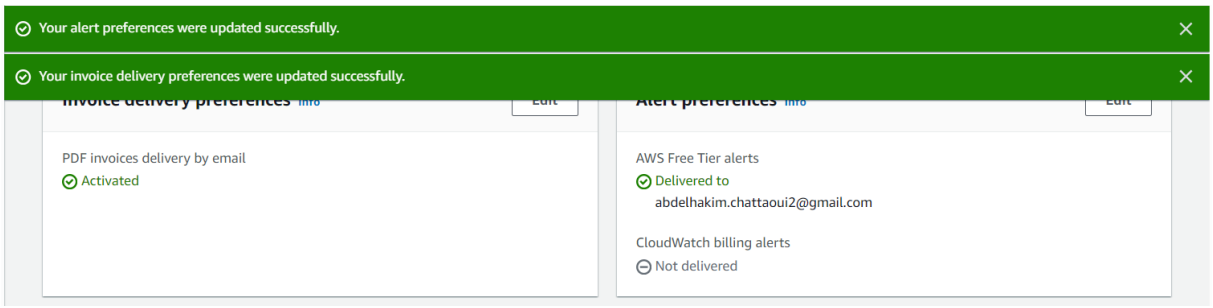



Billing and Cost Management
Billing Preferences
Billing preferences Info
Invoice delivery preferences Info
Edit
PDF invoices delivery by email
Deactivated
Alert preferences Info
Receive AWS Free Tier alerts
If this option is selected, your AWS Free Tier usage alerts will be sent to the email address 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

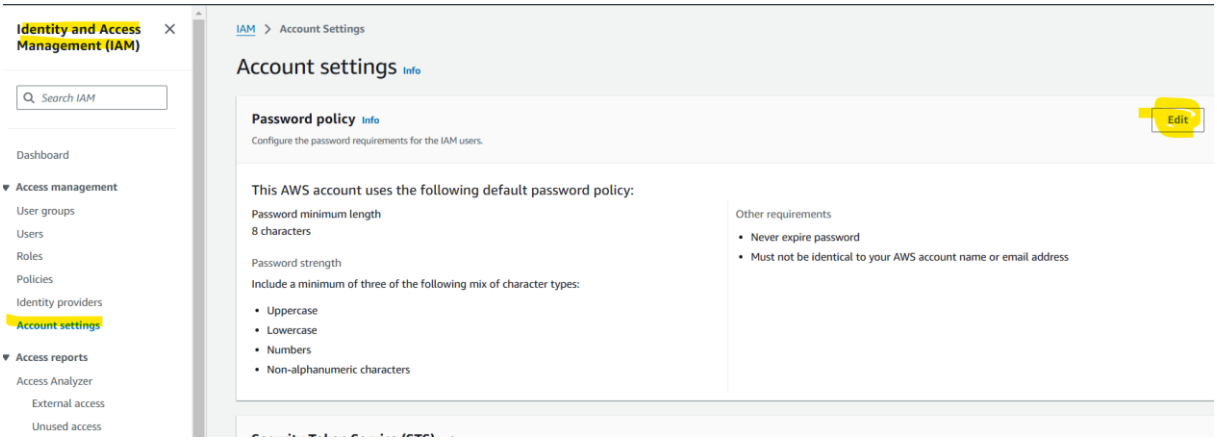

Your alert preferences were updated successfully.
Invoice delivery preferences Info
Edit
PDF invoices delivery by email
Deactivated
Alert preferences Info
Edit
AWS Free Tier alerts
Delivered to
abdelhakim.chattaoui2@gmail.com
CloudWatch billing alerts
Not delivered
Detailed billing reports (legacy) Info
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

IAM > Account Settings > Edit password policy

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

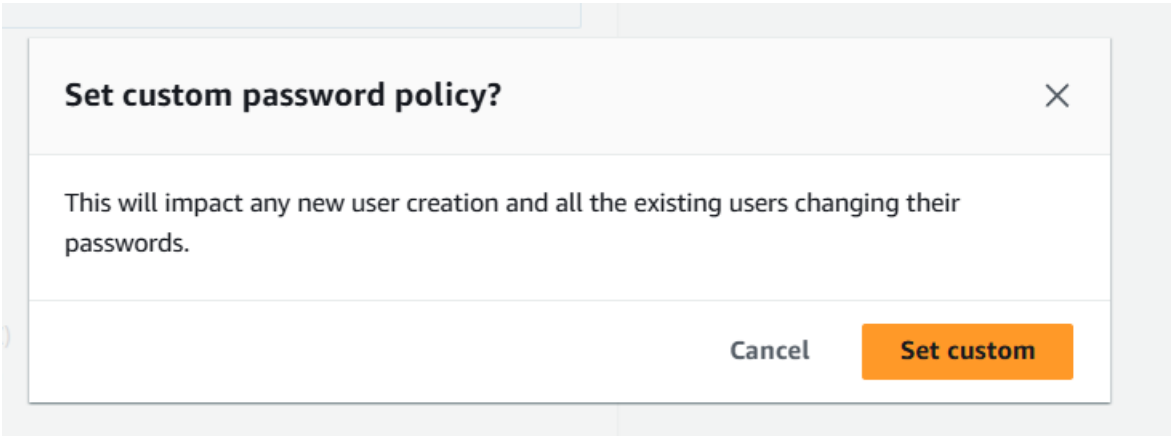
COMBIEN DE TEMPS FAUT-IL À UN PIRATE POUR TROUVER VOTRE MOT DE PASSE 2024

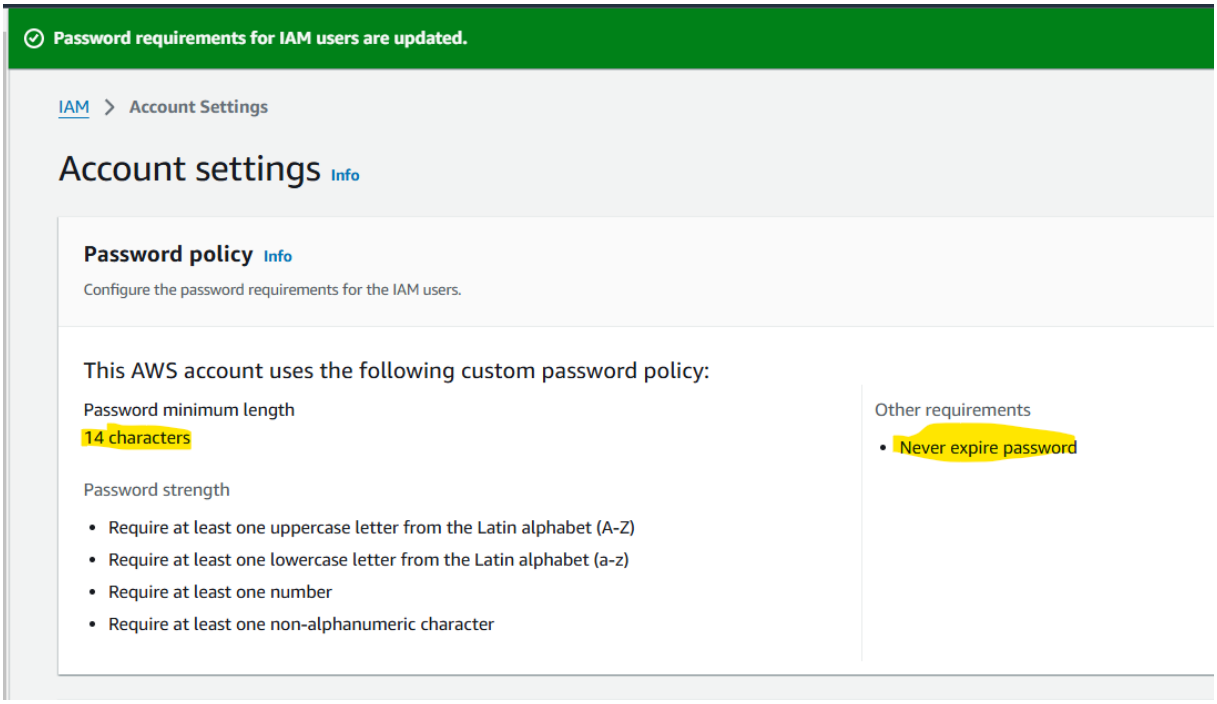
www.hivesystems.com/password

Nombre de caractères	Nombres seulement	Lettres minuscules	Lettres majuscules et minesecules	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

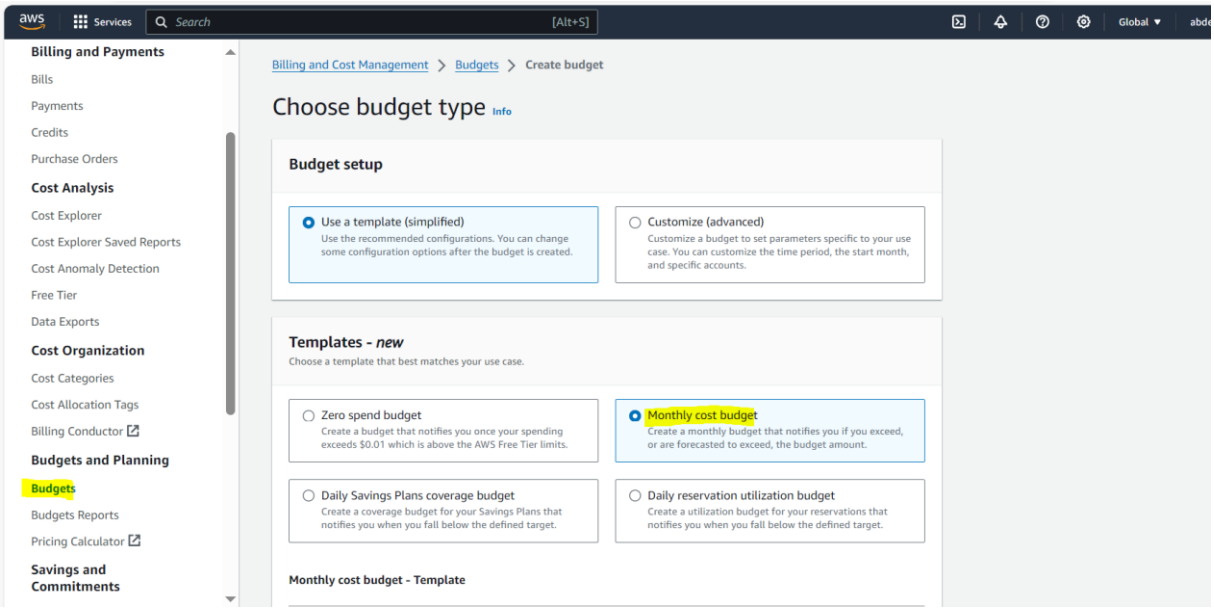
HIVE SYSTEMS

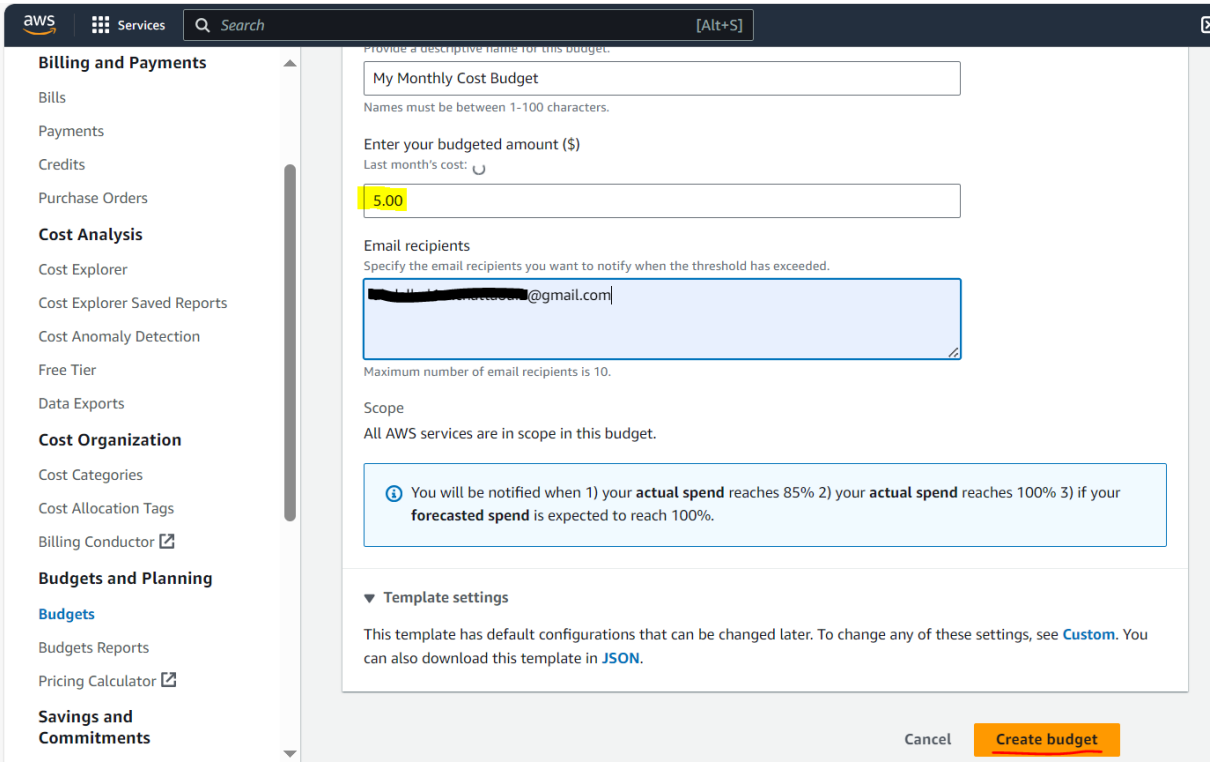
> 12 x RTX 4090 | bcrypt

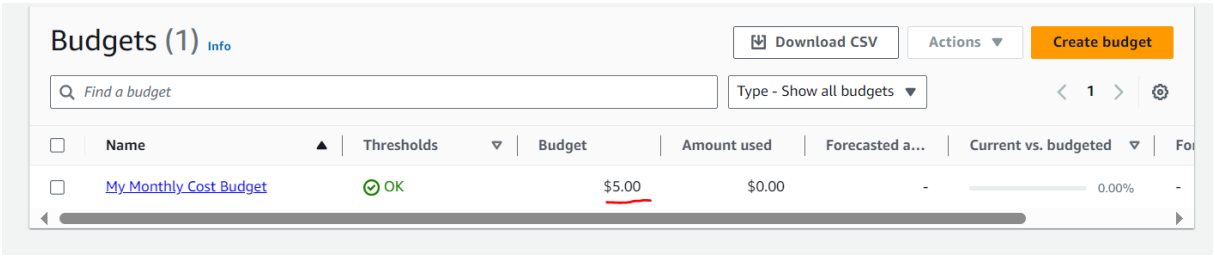

Set custom password policy?
This will impact any new user creation and all the existing users changing their passwords.
Cancel
Set custom


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
14 characters
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
Never expire password

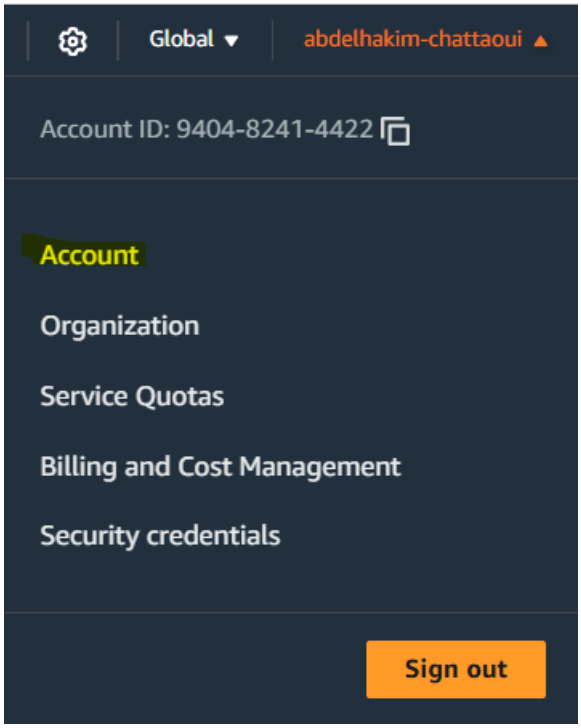
3- Création d'un budget mensuel de 5 dollars et réception d'une notification lorsque 85 % de ce budget est atteint.

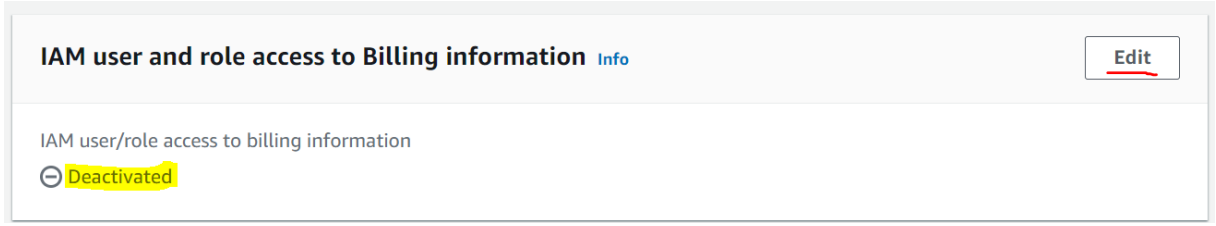


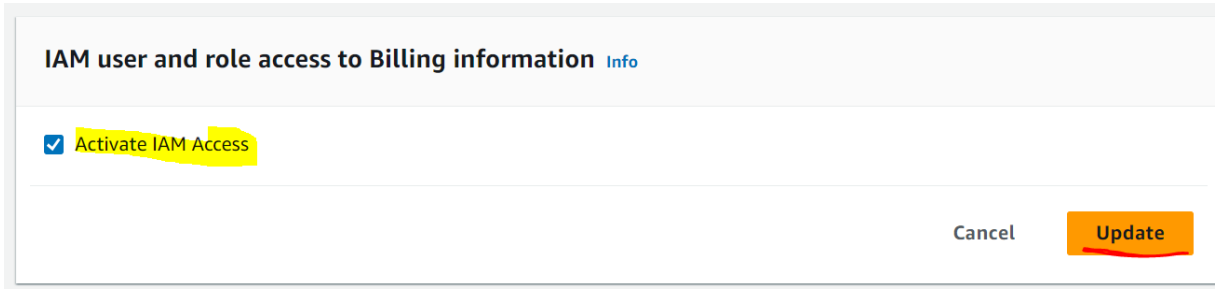


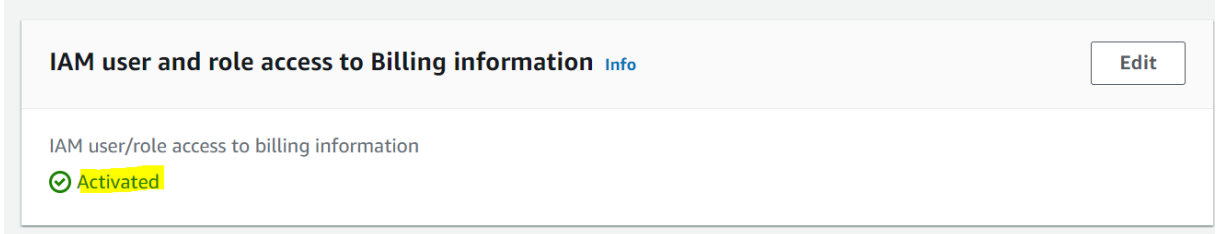


4- Activation de l'accès des utilisateurs IAM aux informations de facturation.





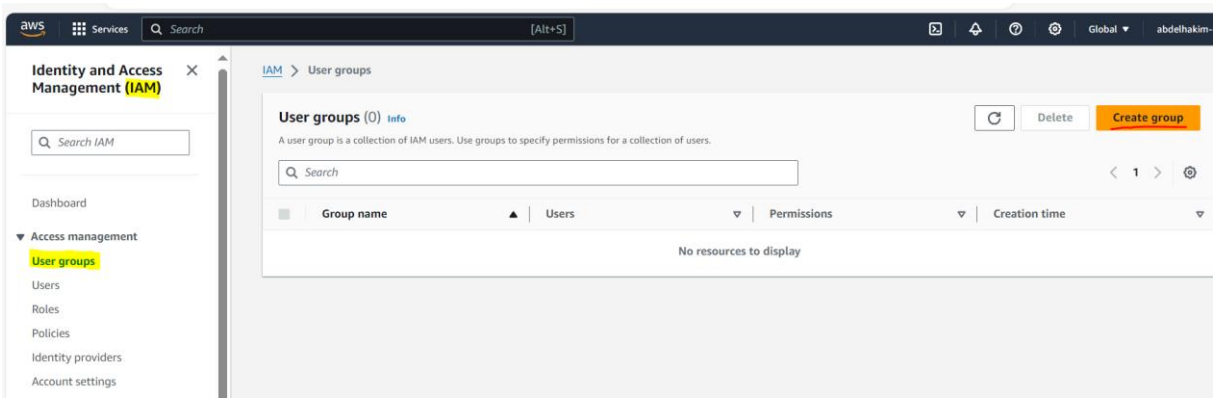


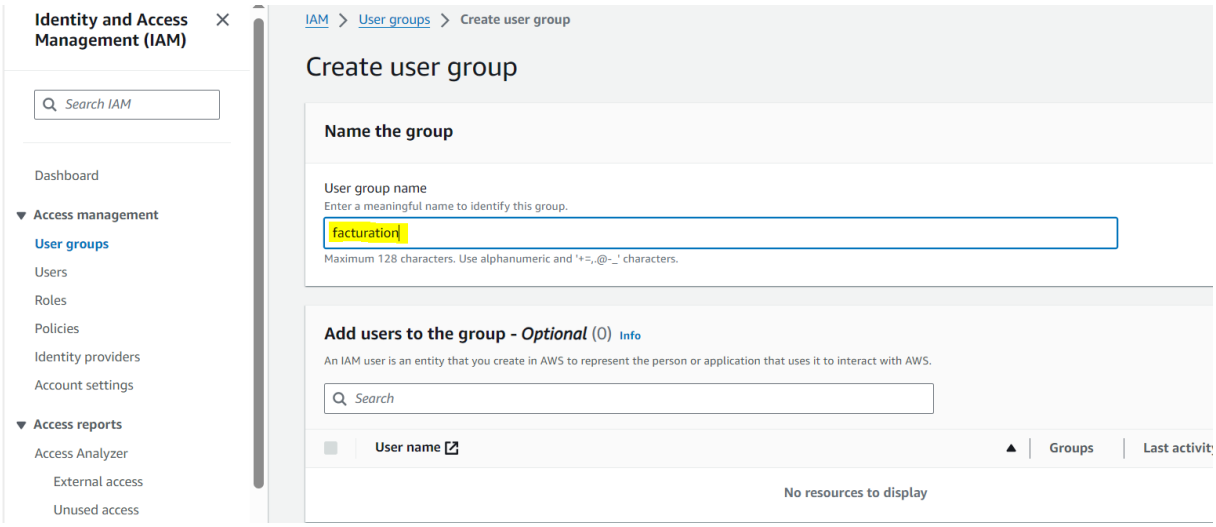


5- **RBAC :** Nous allons ajouter un groupe *facturation*, lui attribuer les droits de facturation et y ajouter l'utilisateur *mathias*.

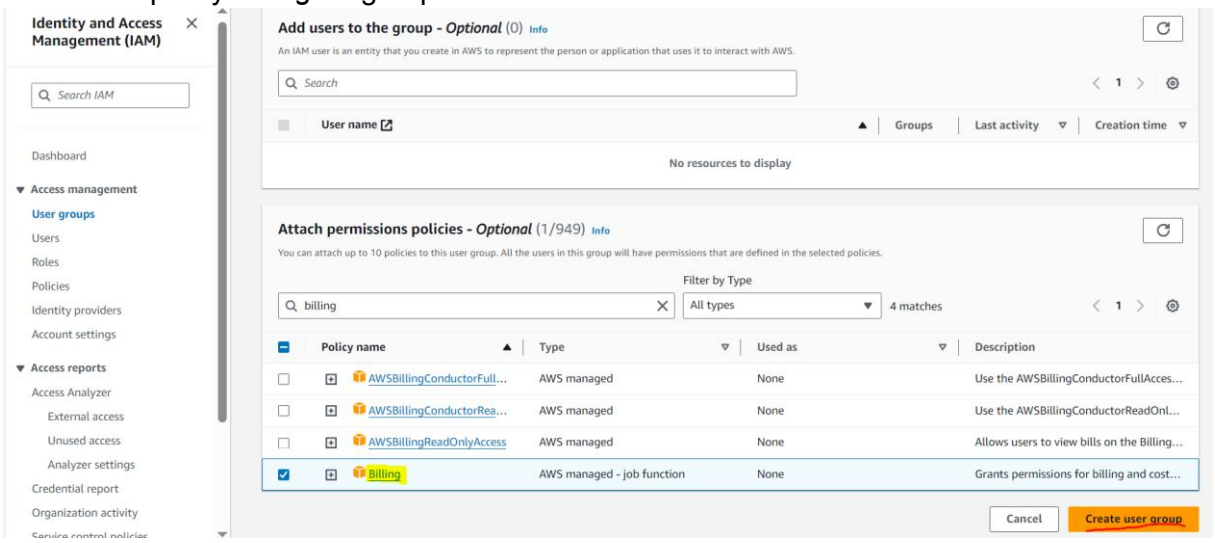
Ajoutez un groupe

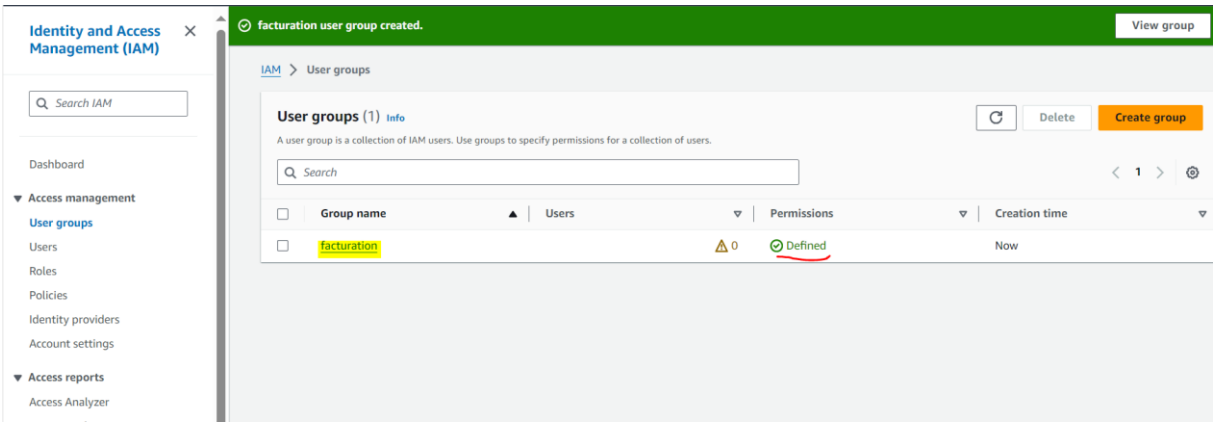
.



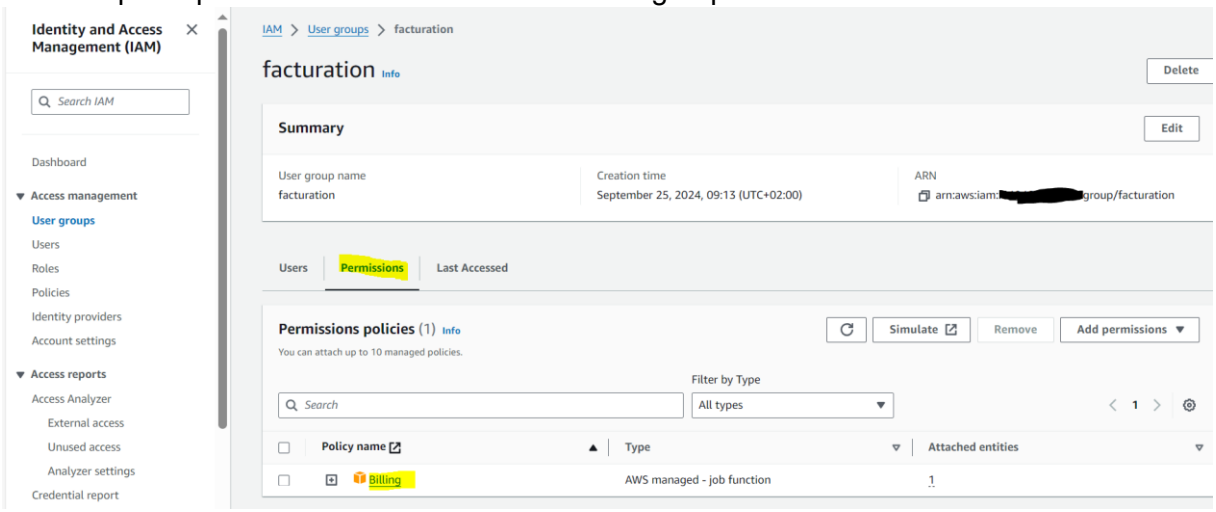


Attacher la policy *Billing* au groupe facturation

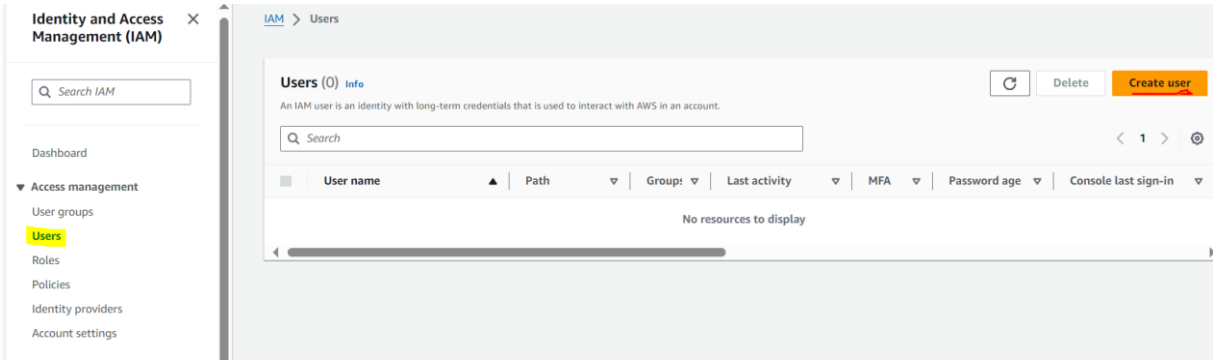


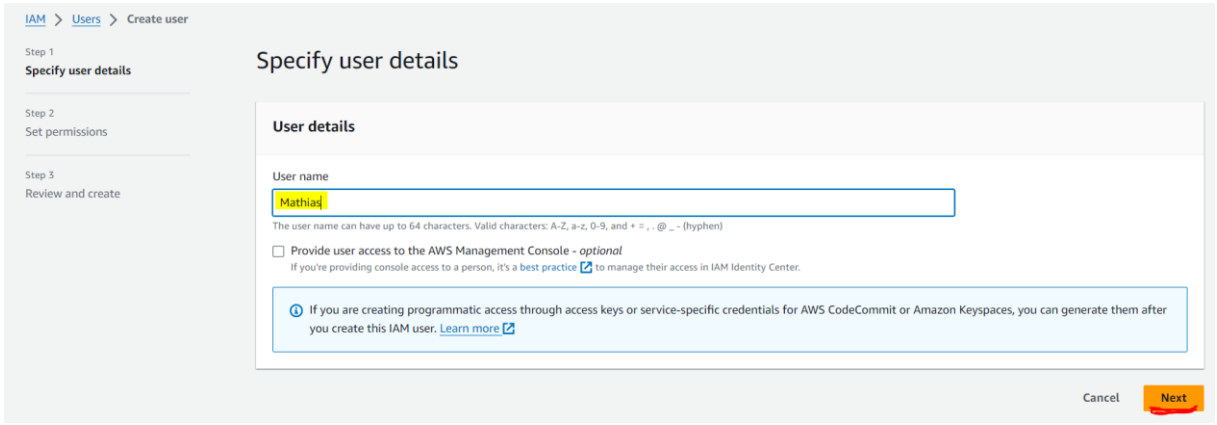


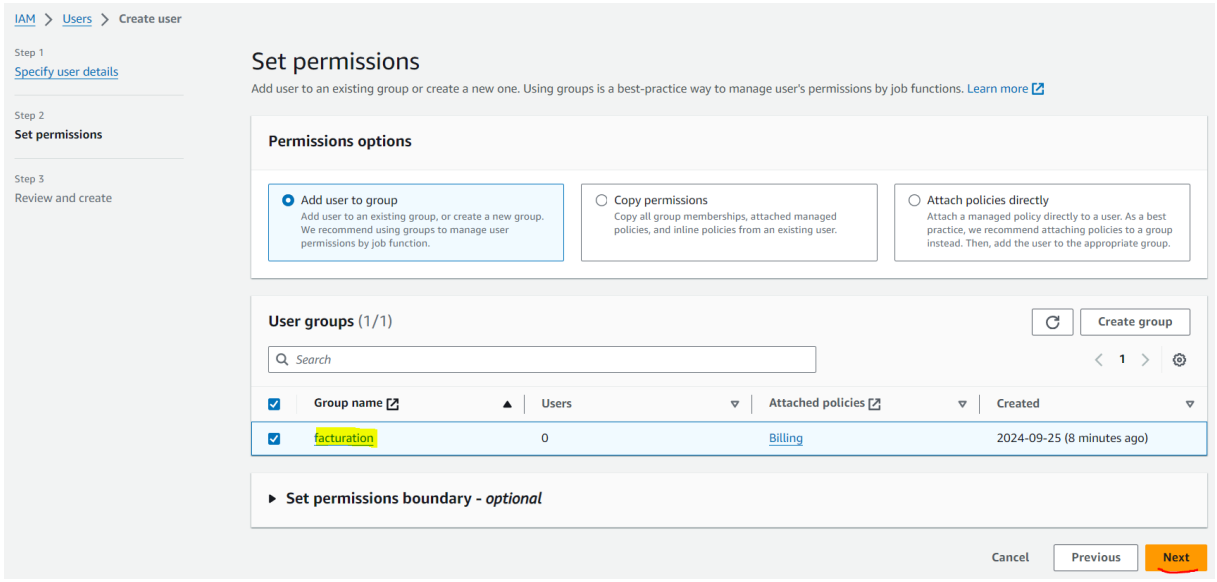
Vérifiez que la permission a bien été accordée au groupe.

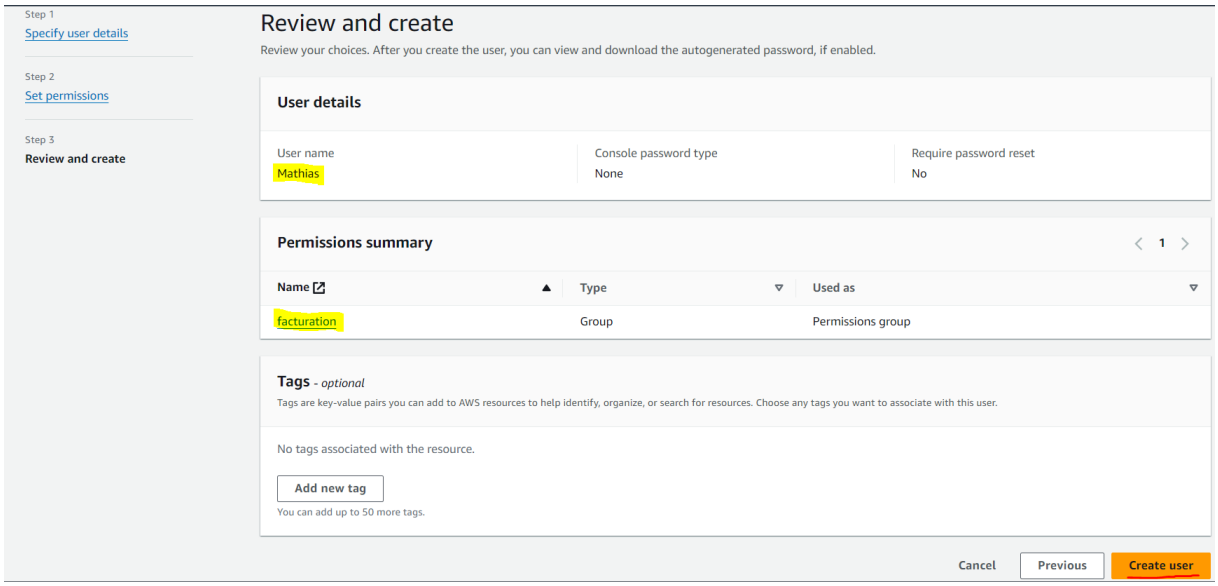


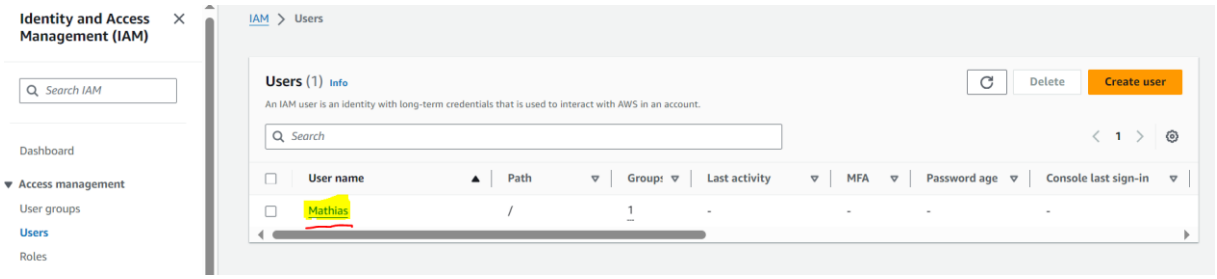
Ajoutez un utilisateur nommé **Mathias** et associez-le au groupe **facturation**.



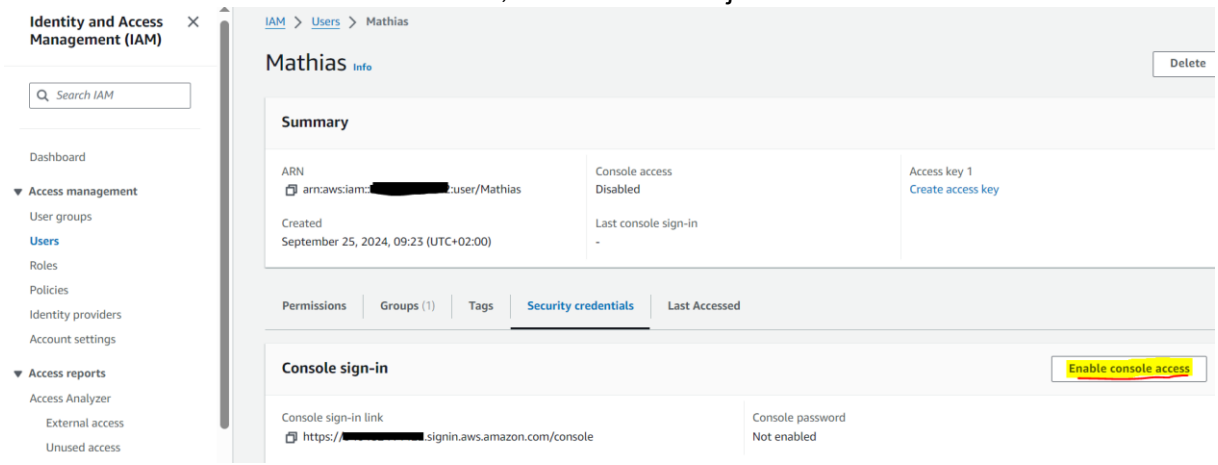

IAM > Users > Create user
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Specify user details
User details
User name
Mathias
The user name can have up to 64 characters. Valid characters: A-Z, a-z, 0-9, and + = , . @ _ - (hyphen)
Provide user access to the AWS Management Console - 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
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)
Create group
Search
1
Group name
Users
Attached policies
Created
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
Mathias
Console password type
None
Require password reset
No
Permissions summary
1
Name
Type
Used as
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



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



Enable console access

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

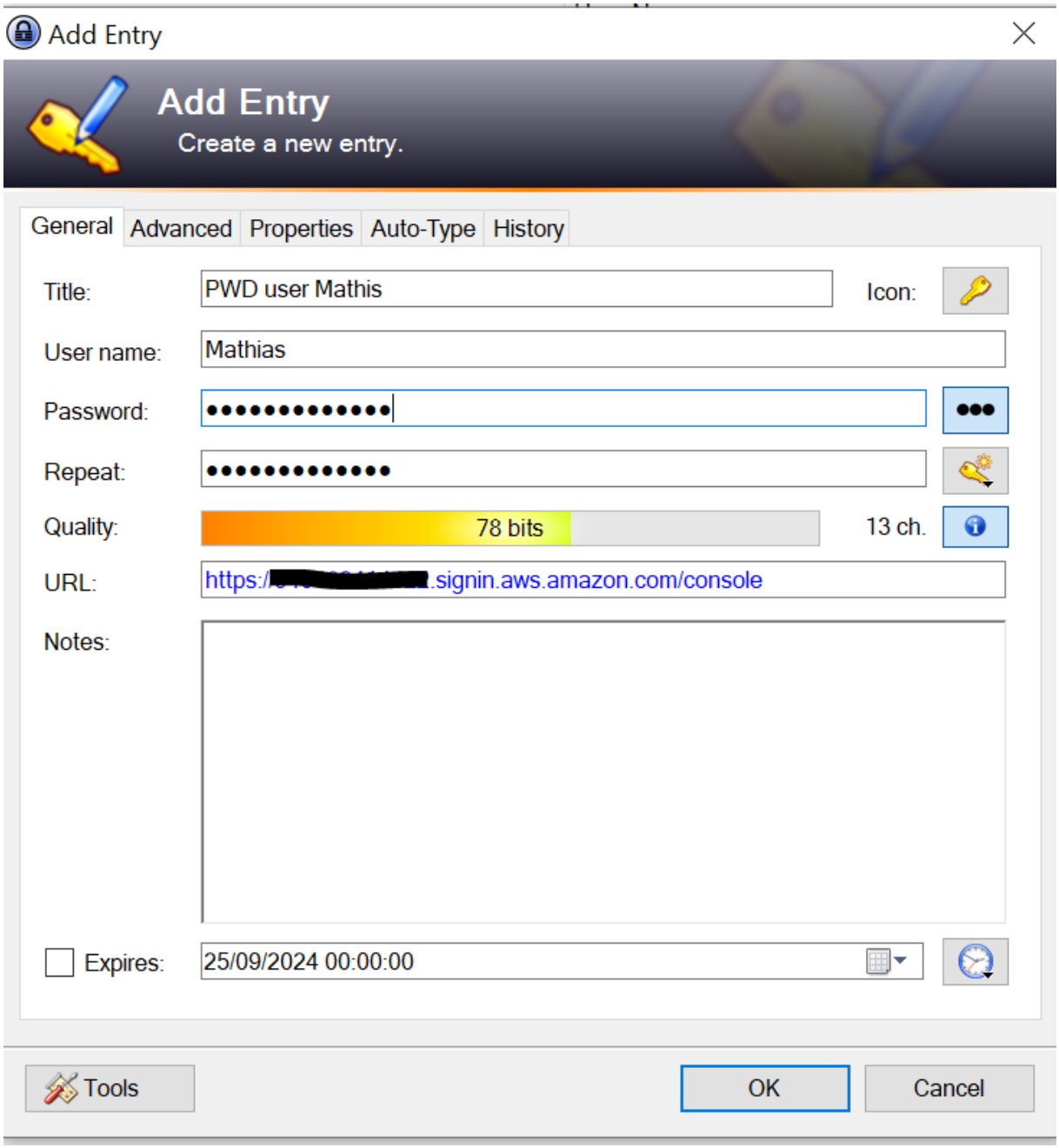
User name

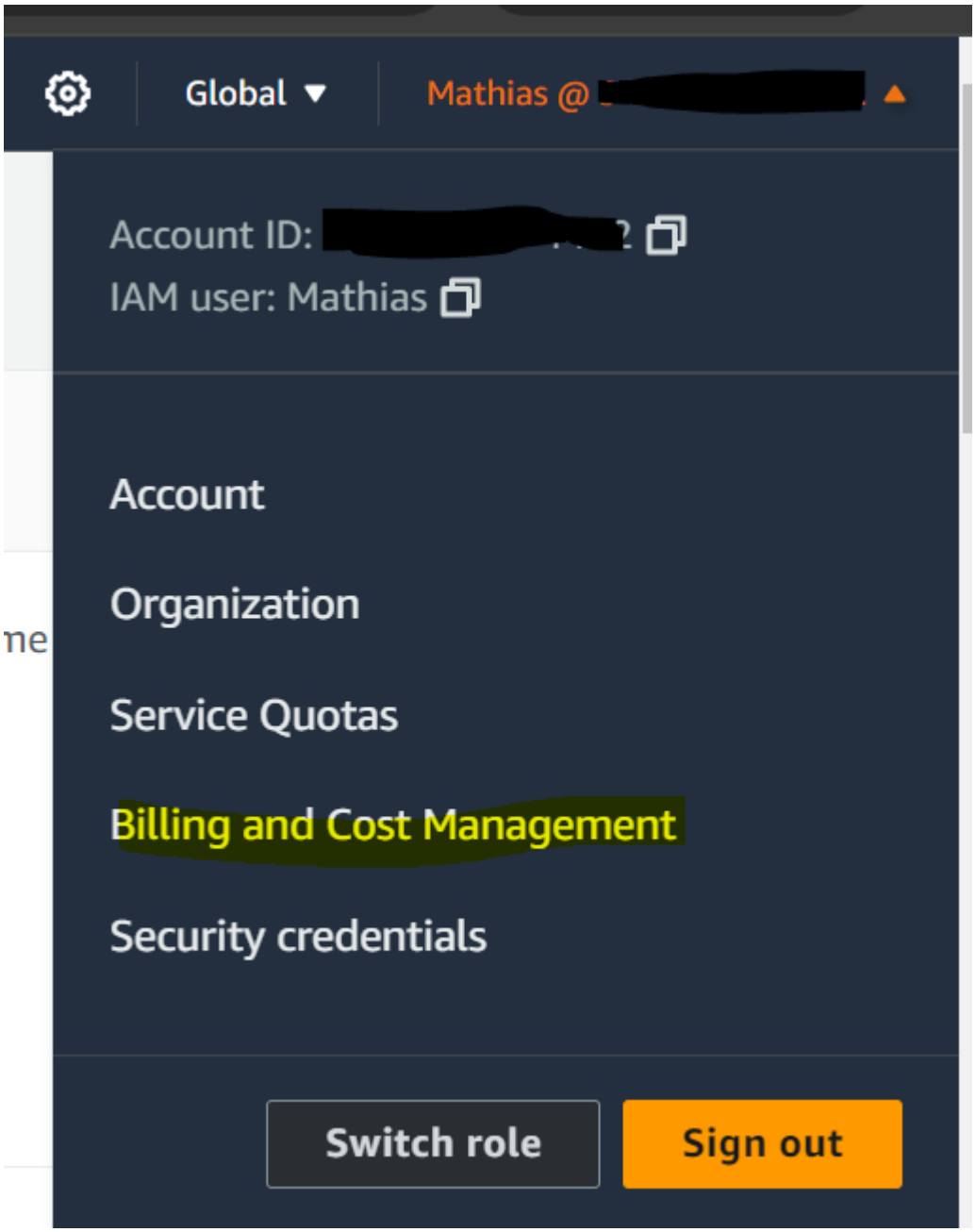
Mathias

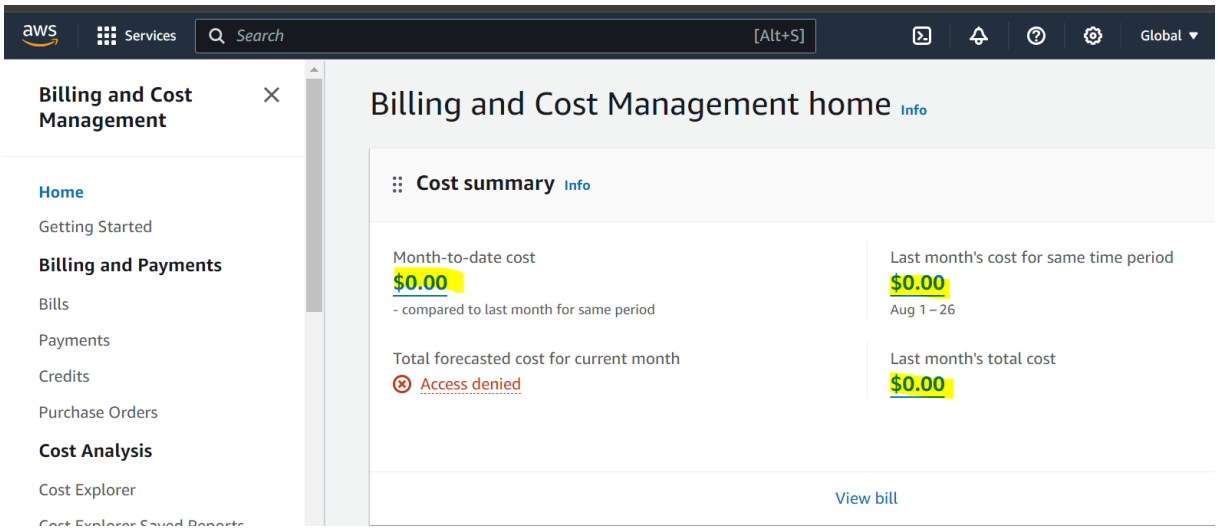
Console password

********** Show

Download .csv file | Close

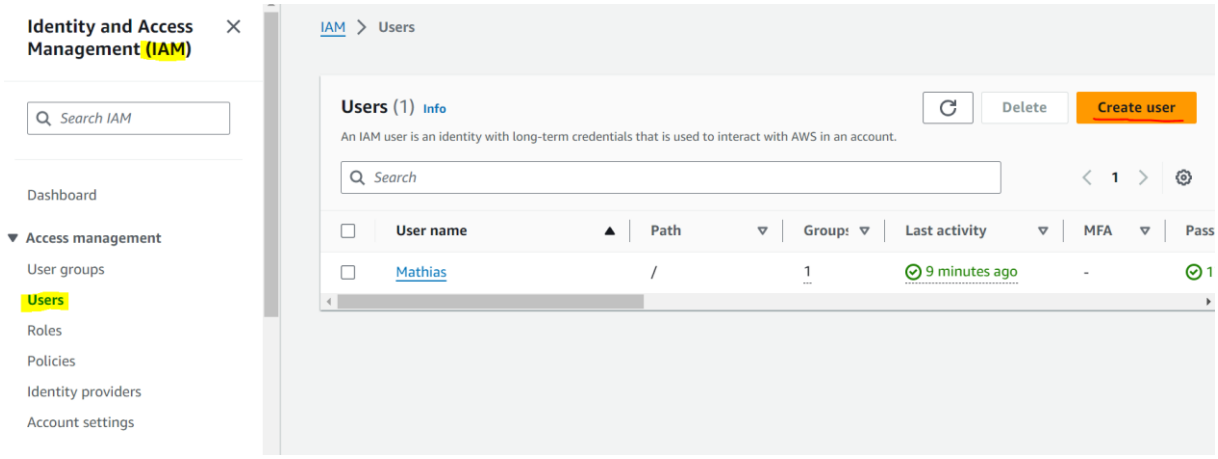

Add Entry
Add Entry
Create a new entry.
General
Advanced
Properties
Auto-Type
History
Title:
PWD user Mathis
Icon:
User name:
Mathias
Password:
Repeat:
Quality:
78 bits
13 ch.
URL:
https:[redacted].signin.aws.amazon.com/console
Notes:
Expires:
25/09/2024 00:00:00
Tools
OK
Cancel

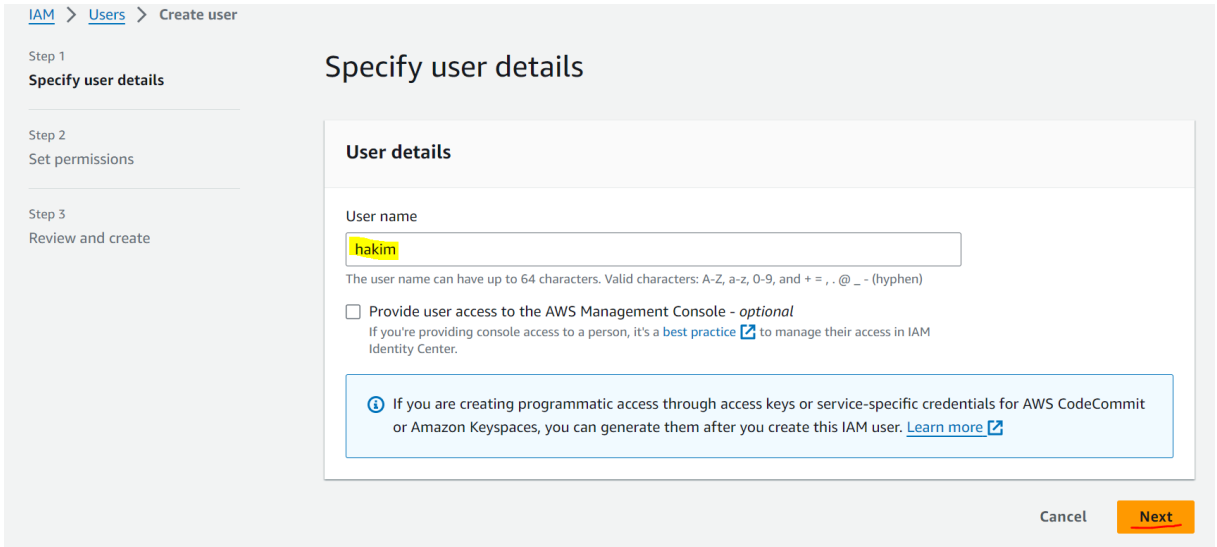

Global
Mathias @
Account ID:
IAM user: Mathias
Account
Organization
Service Quotas
Billing and Cost Management
Security credentials
Switch role
Sign out

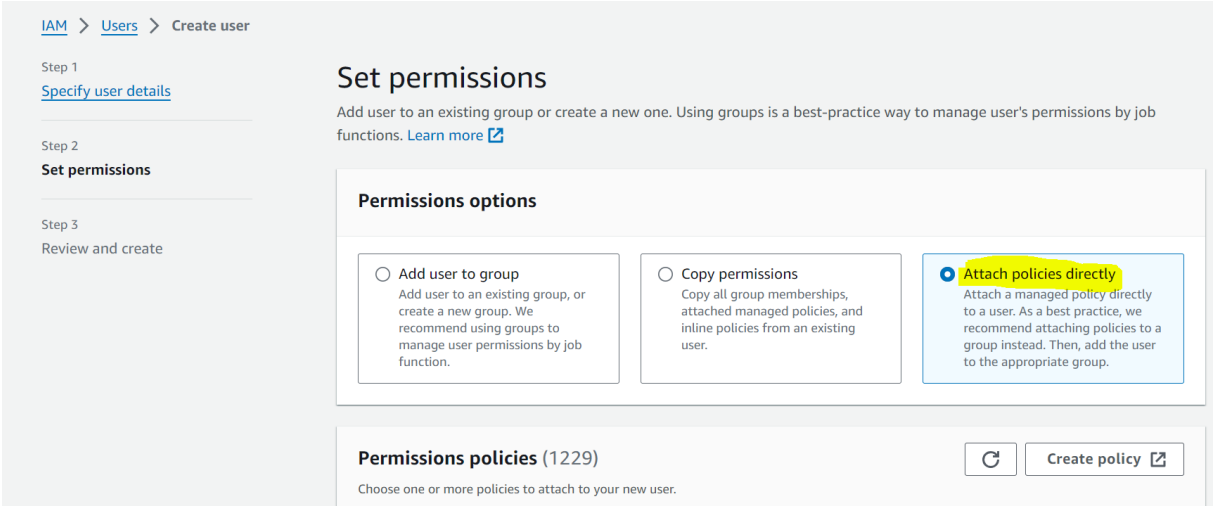


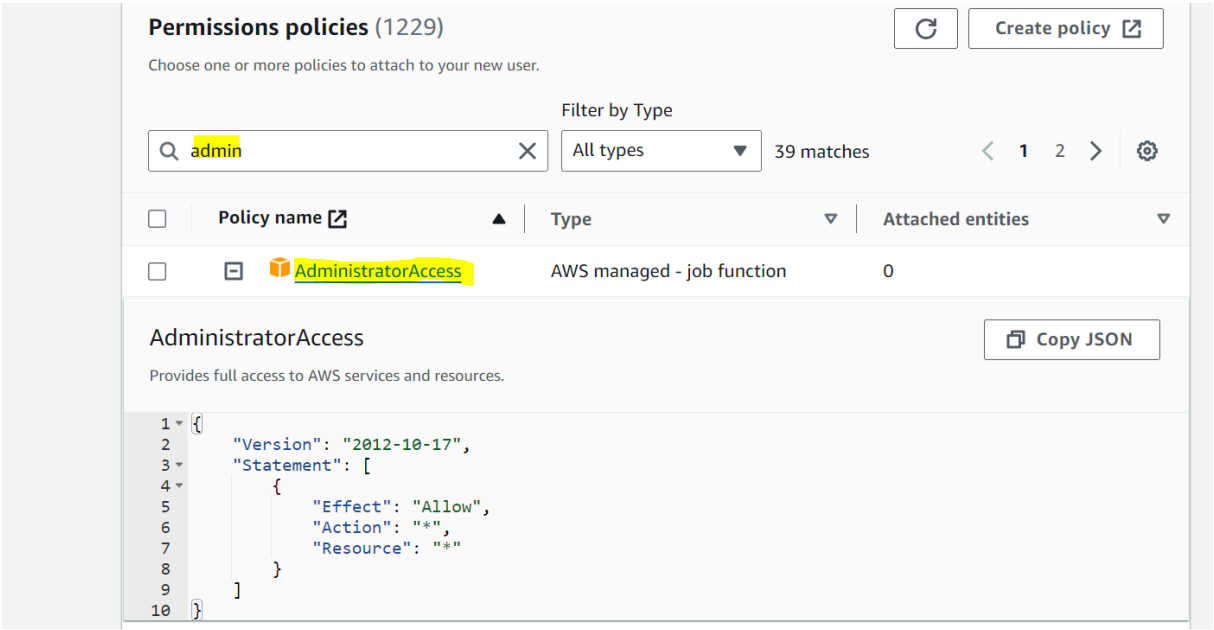
Identity-Based Policy

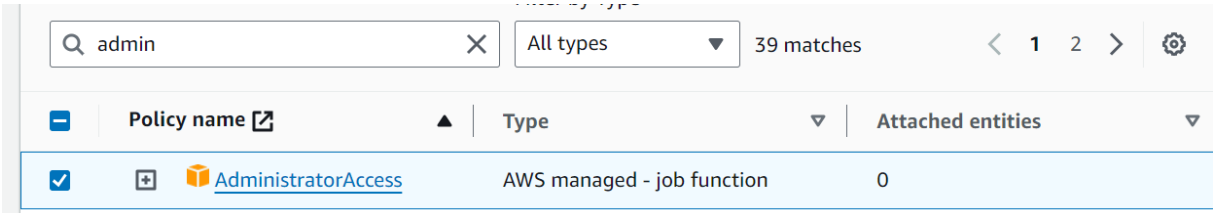
Ajoute un utilisateur nommé « votre nom » et lui attribue le rôle d'administrateur.

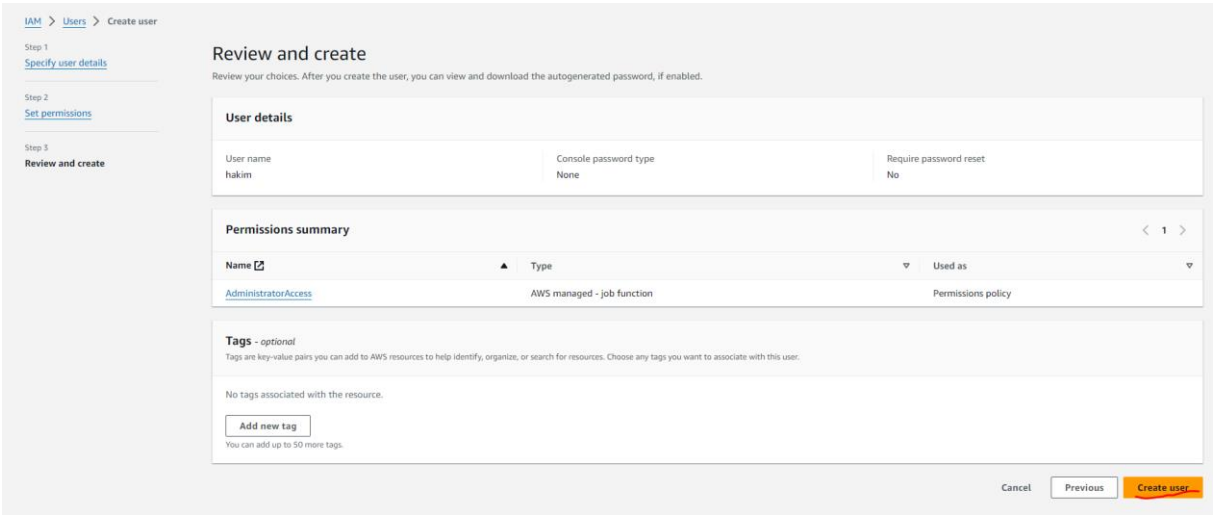


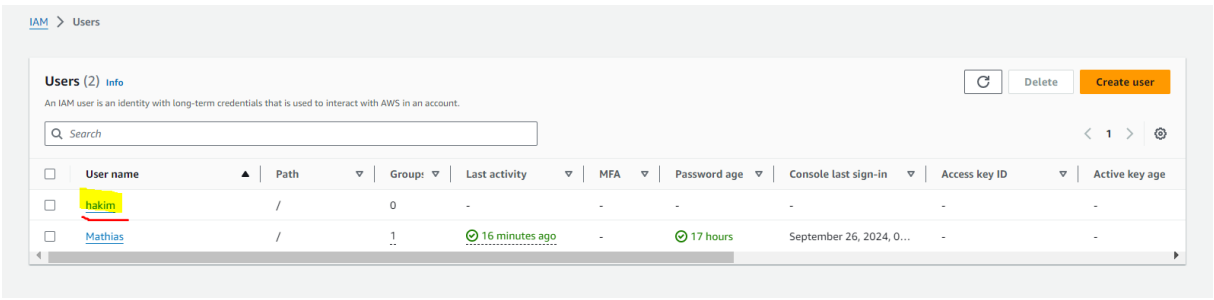


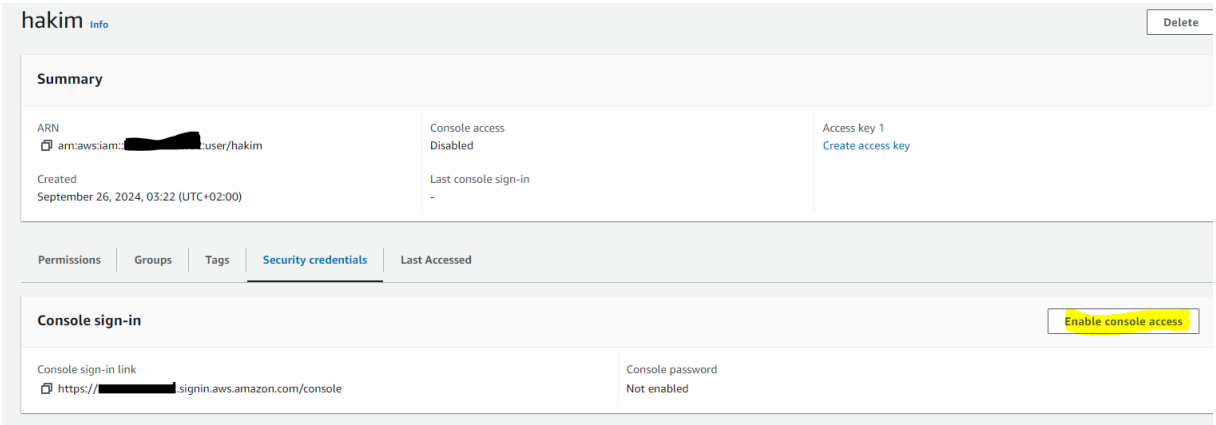

IAM > Users > Create user
Step 1
Specify user details
Step 2
Set permissions
Step 3
Review and create
Set permissions
Add user to an existing group or create a new one. Using groups is a best-practice way to manage user's permissions by job functions. Learn more
Permissions options
Add user to group
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 (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.
Create policy
Filter by Type
admin
All types
39 matches
1
2
Policy name
Type
Attached entities
AdministratorAccess
AWS managed - job function
0
AdministratorAccess
Provides full access to AWS services and resources.
Copy JSON
{
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Action": "*",
"Resource": "*"
}
]
}


admin
All types
39 matches
1
2
Policy name
Type
Attached entities
AdministratorAccess
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
hakim
Console password type
None
Require password reset
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.
Delete
Create user
Search
User name
Path
Groups
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
Delete
Summary
ARN
arn:aws:iam::[redacted]: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
Enable console access
Console sign-in link
https://[redacted].signin.aws.amazon.com/console
Console password
Not enabled

Enable console access

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

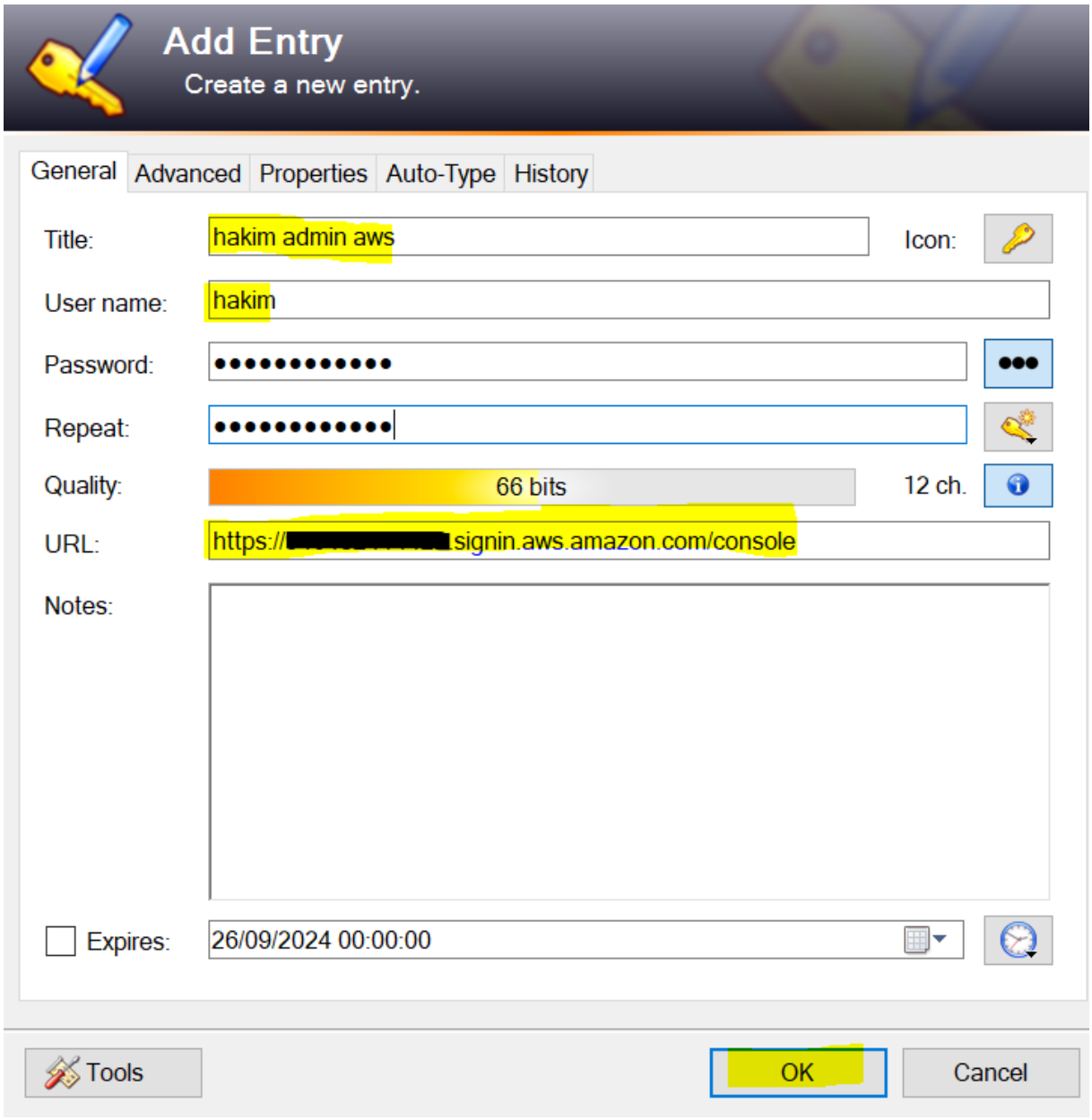
User name

hakim

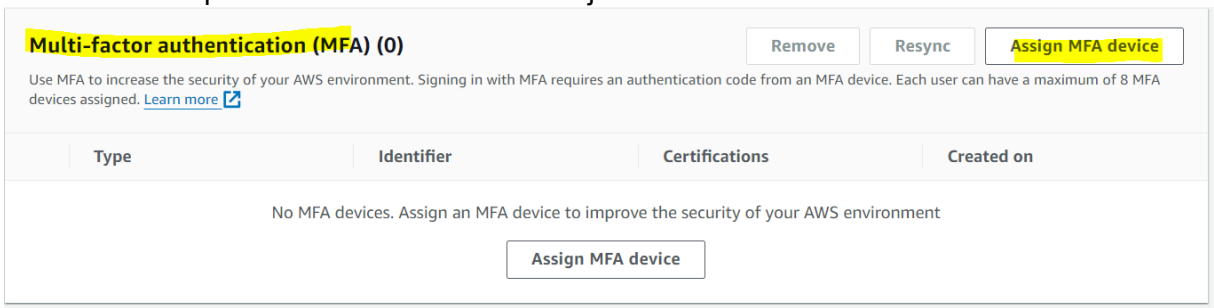
Console password

********** Show

Download .csv file | Close



Activez le MFA pour l'utilisateur récemment ajouté.



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

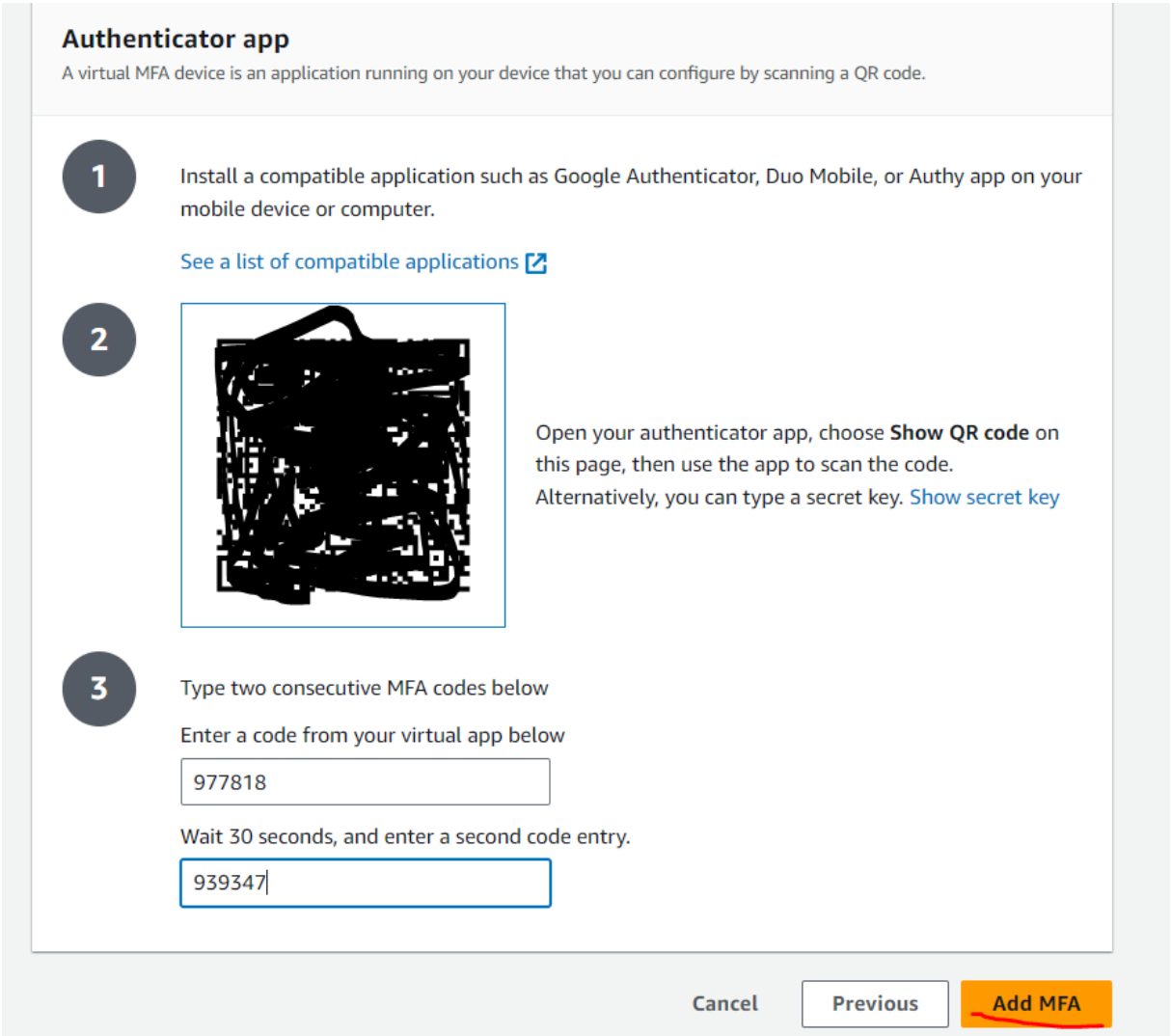
   Enter a code from your virtual app below

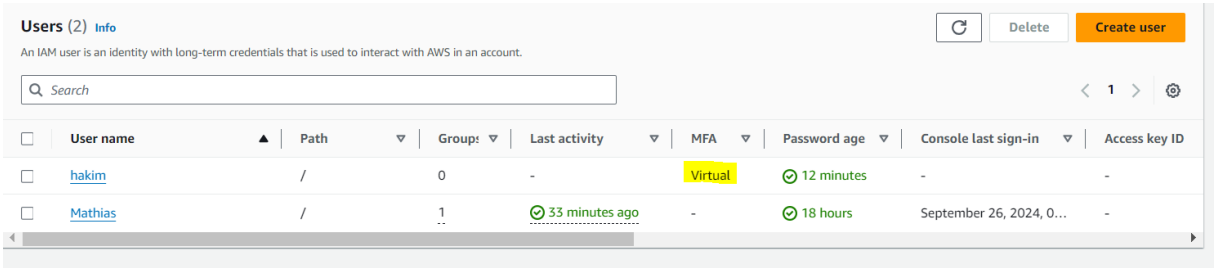
   MFA Code 1

   Wait 30 seconds, and enter a second code entry.

   MFA Code 2

Cancel | Previous | Add MFA





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

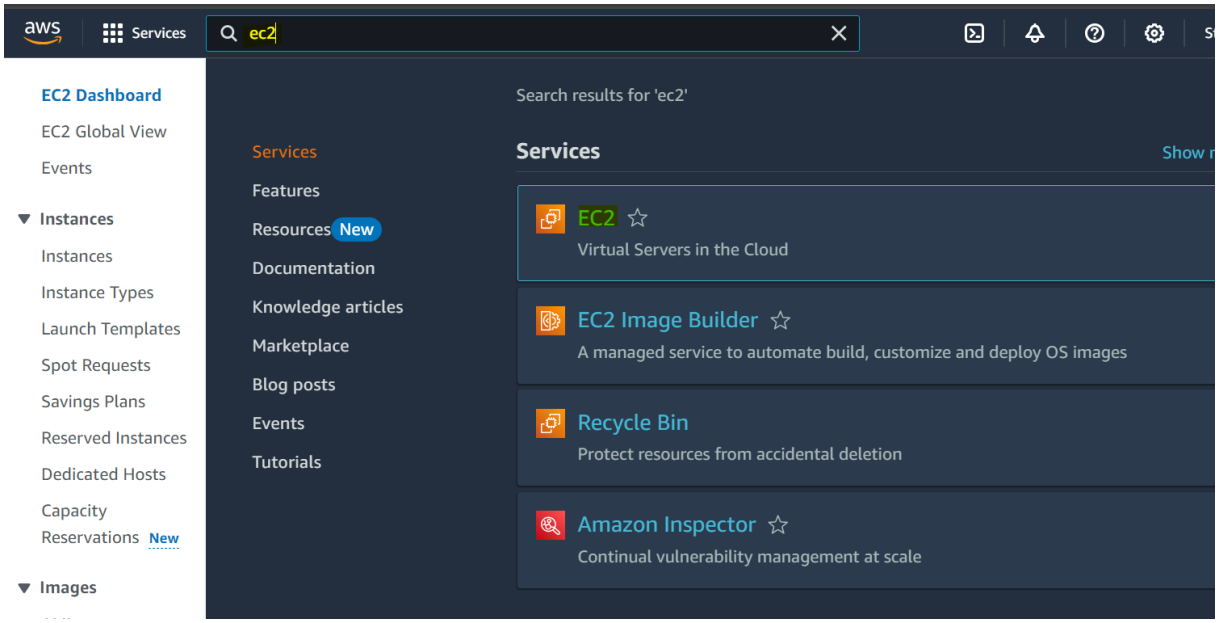
Saisissez un code MFA pour terminer la connexion.

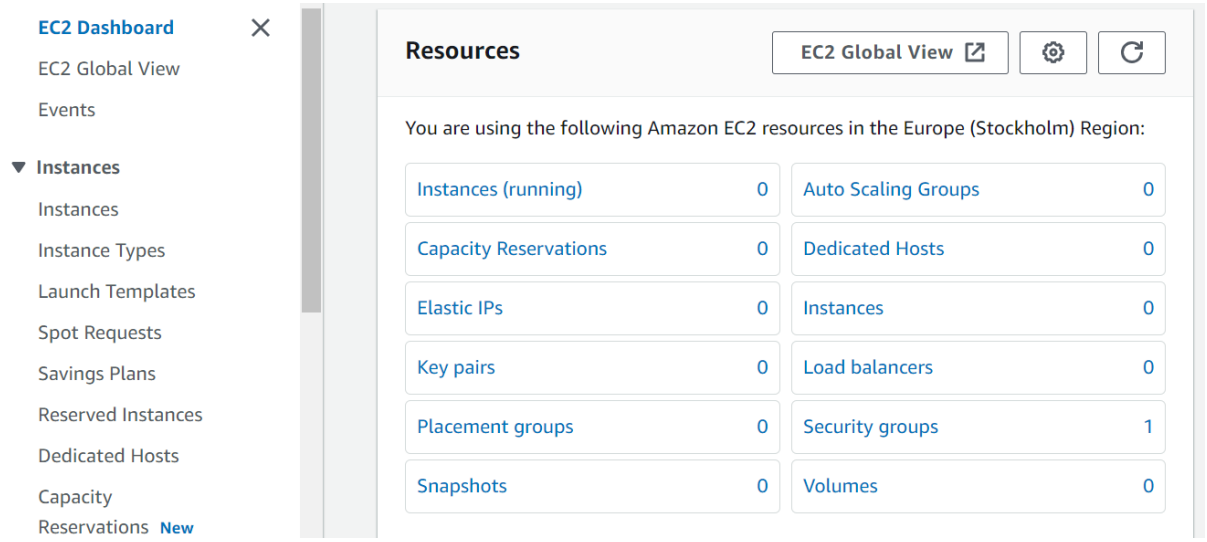
Code MFA :

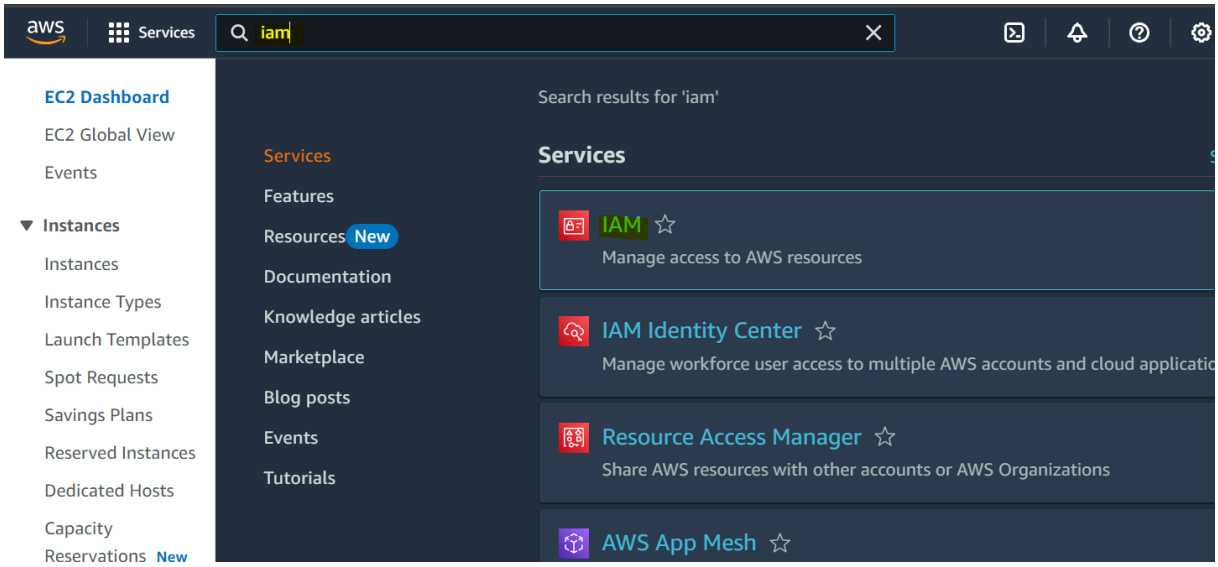
566501

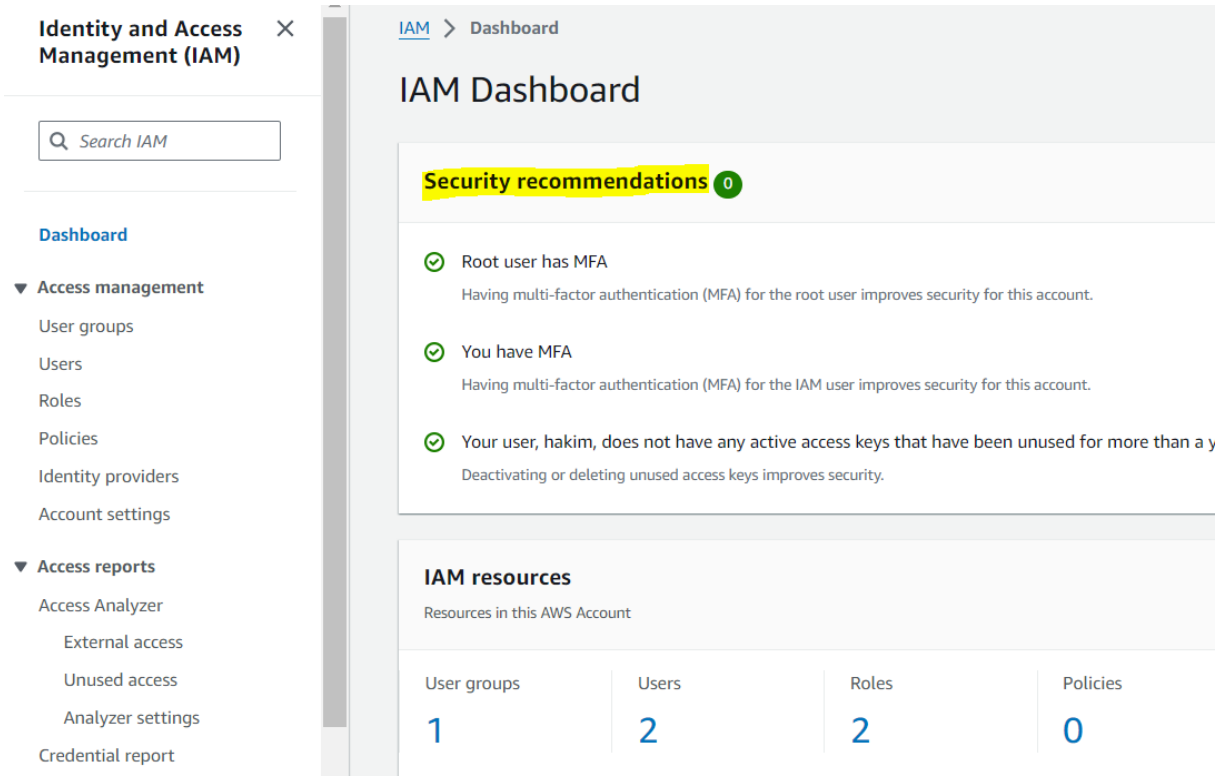
Envoyer

Annuler

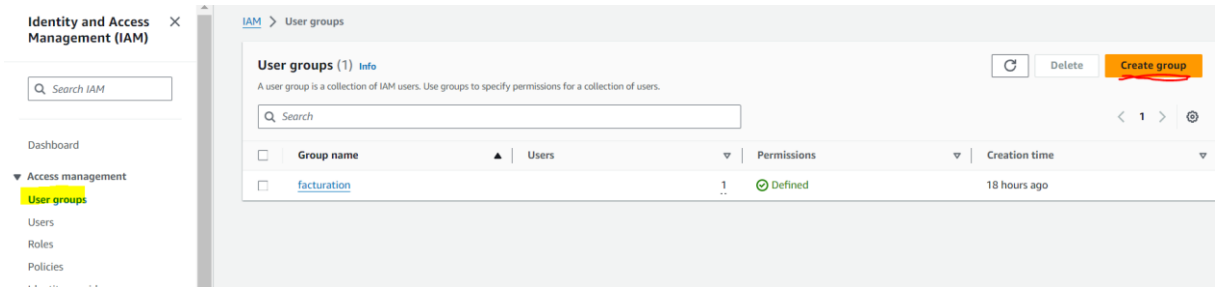



EC2 Dashboard
EC2 Global View
Events
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations New
Resources
EC2 Global View
You are using the following Amazon EC2 resources in the Europe (Stockholm) Region:
Instances (running) 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
iam
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 applicatic
Resource Access Manager
Share AWS resources with other accounts or AWS Organizations
AWS App Mesh

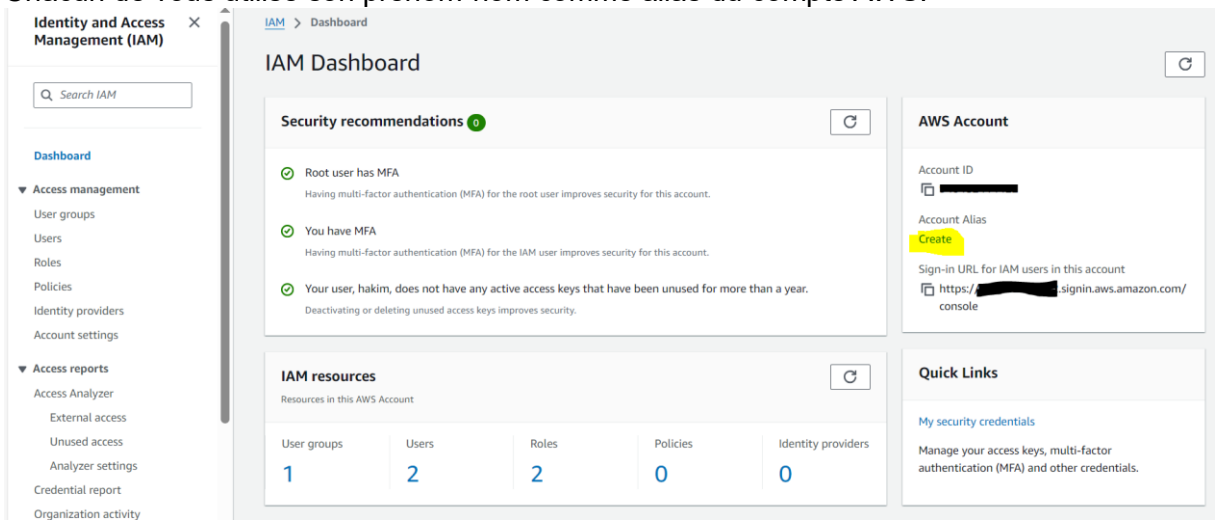


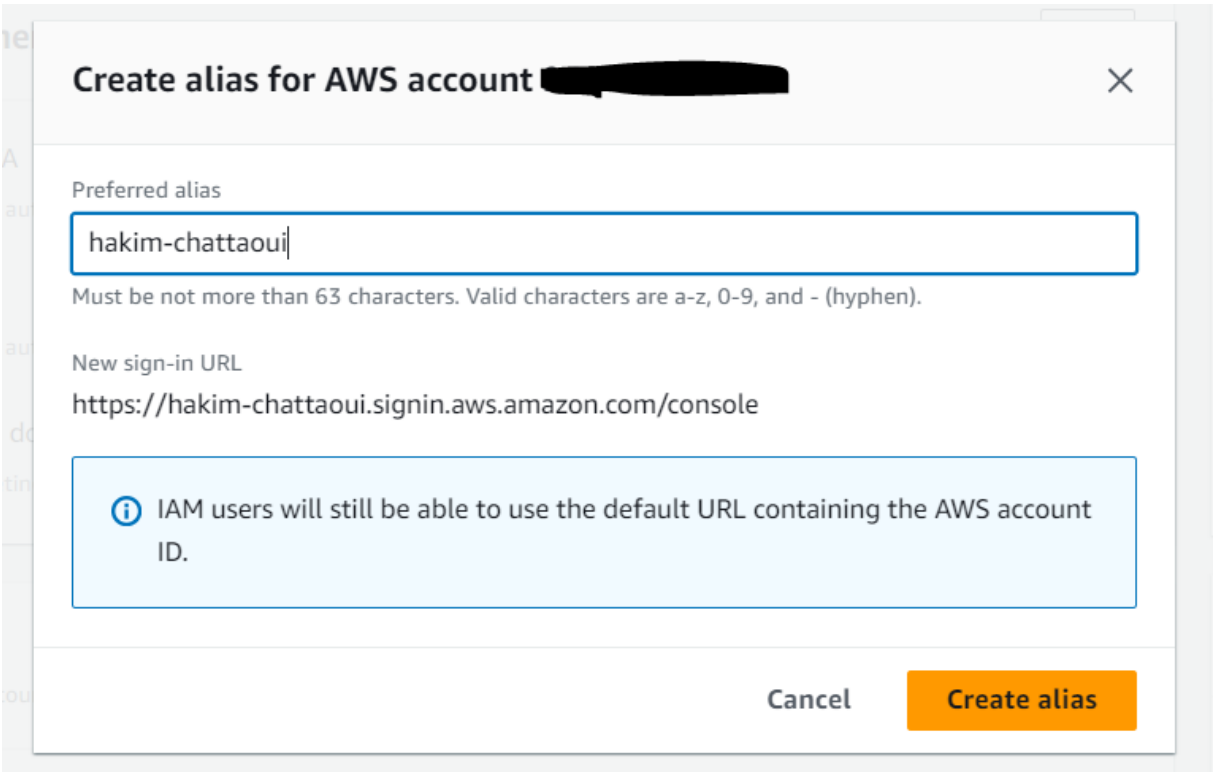
****

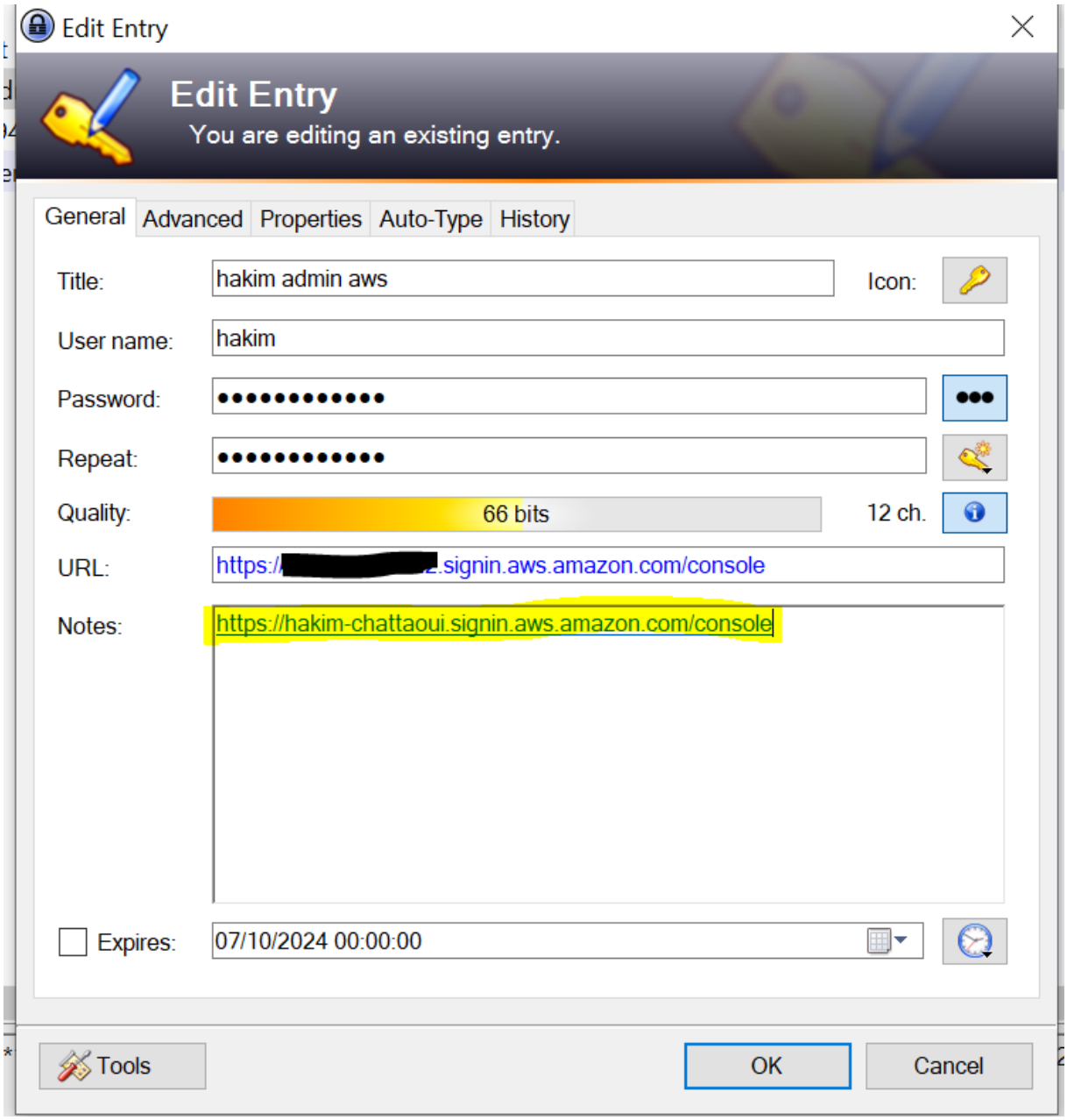


6- Ajoutez un alias au compte AWS (au lieu de se connecter avec un ID de compte, nous allons nous connecter avec un alias qui est unique dans le monde).

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




Create alias for AWS account [redacted]
Preferred alias
hakim-chattaoui
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
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.signin.aws.amazon.com/oauth?client_id=arn%3Aaw

aws

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

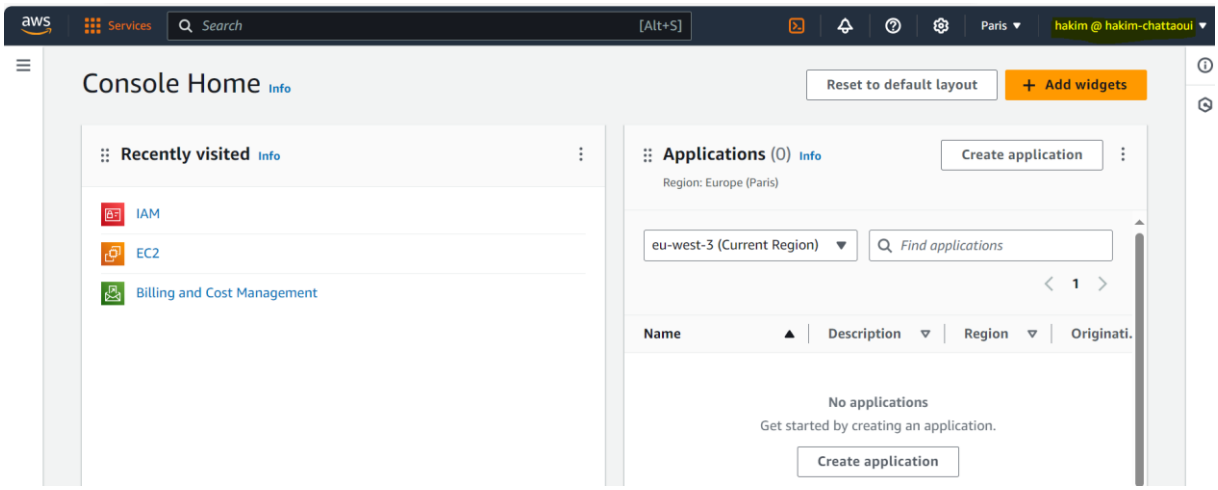
Mot de passe :

••••••••••••

☐ Se souvenir de ce compte

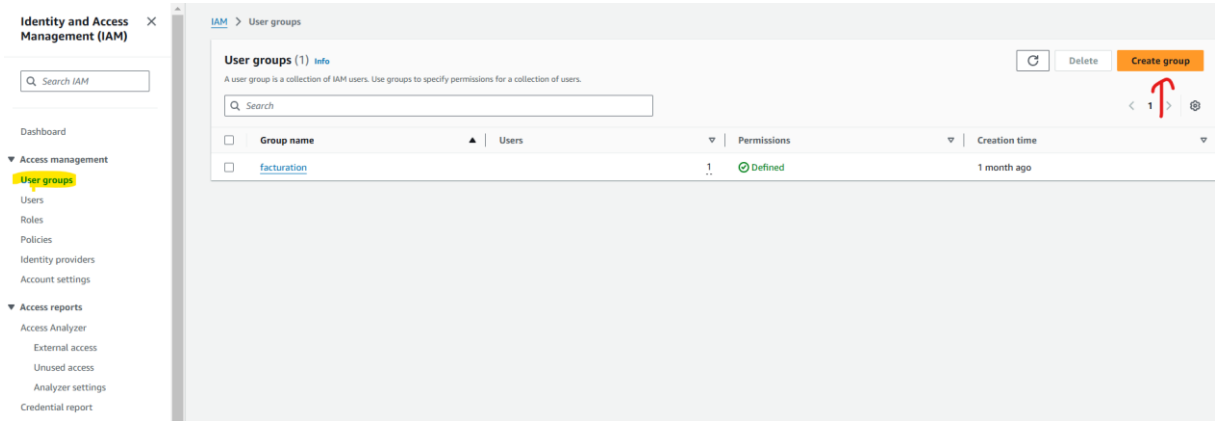
Connexion

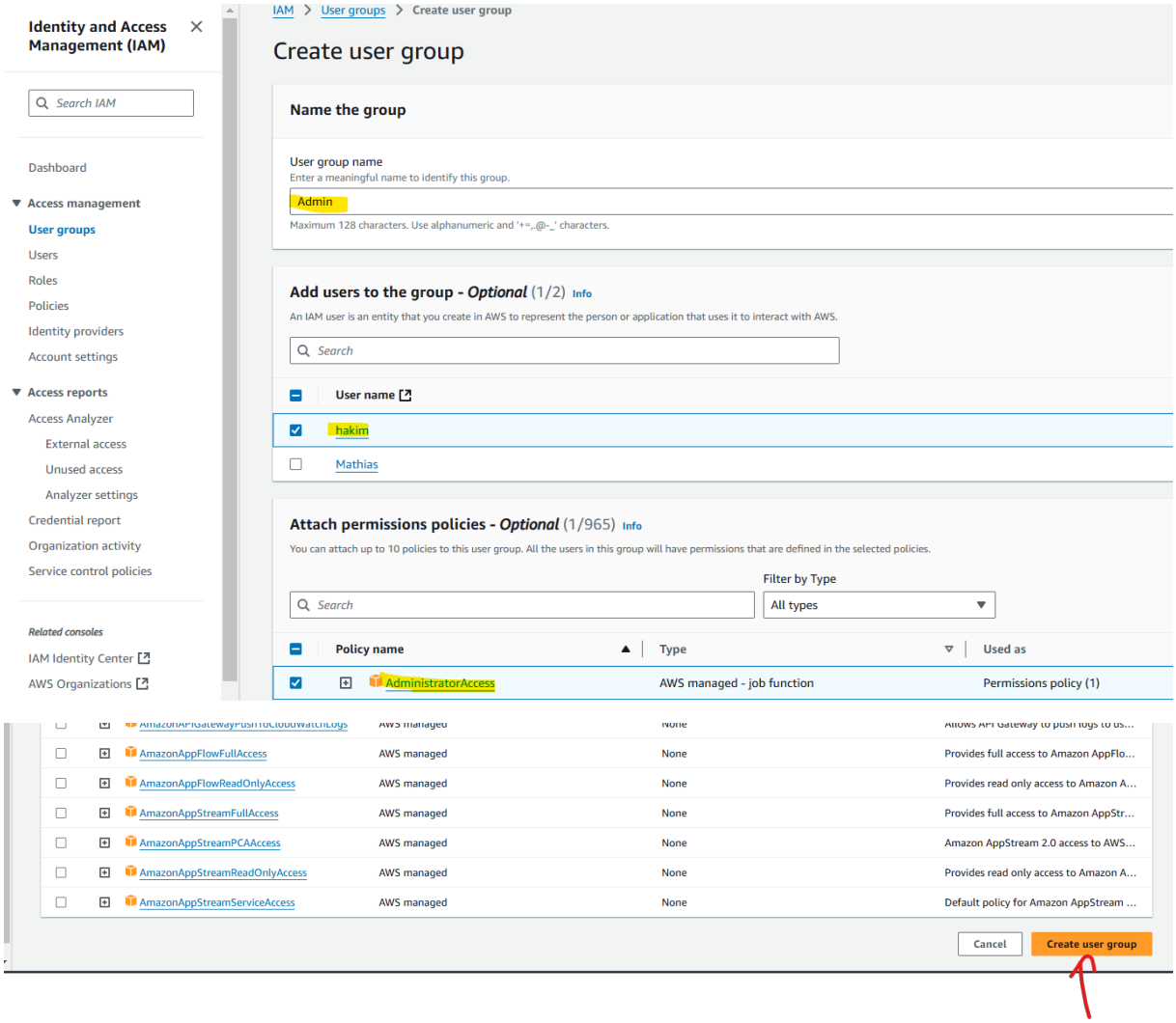
Vérifiez que vous avez actuellement accès par l'alias récemment ajouté.

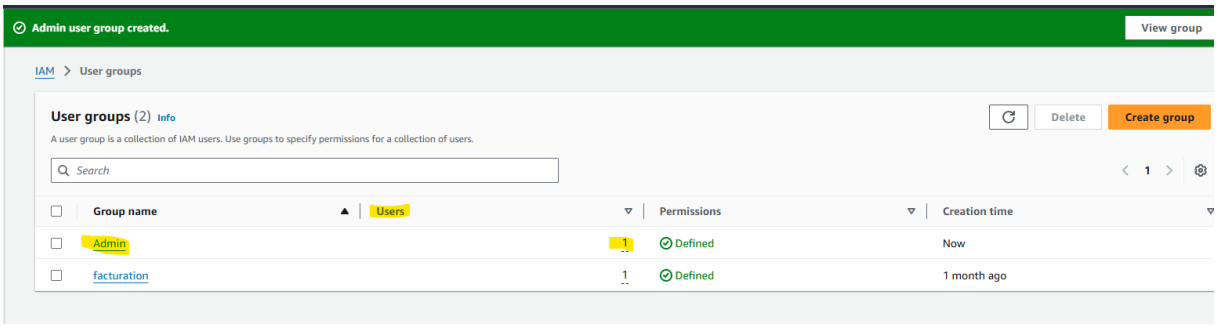


RBAC

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)
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
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.
Search
Delete
Create group
Group name
Users
Permissions
Creation time
facturation
1
Defined
1 month ago

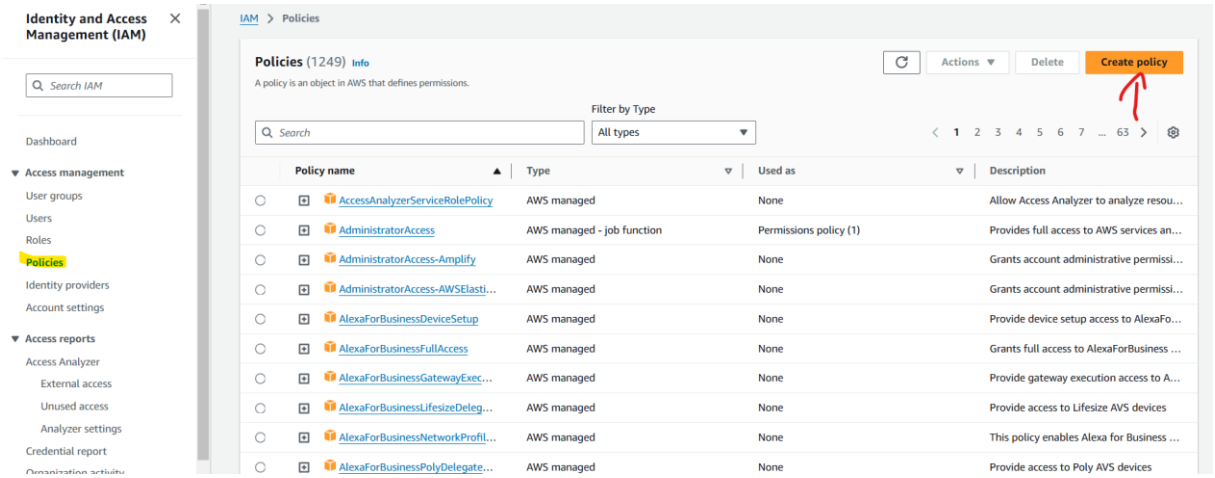

Identity and Access Management (IAM)
Search IAM
Dashboard
Access management
User groups
Users
Roles
Policies
Identity providers
Account settings
Access reports
Access Analyzer
External access
Unused access
Analyzer settings
Credential report
Organization activity
Service control policies
Related consoles
IAM Identity Center
AWS Organizations
IAM > User groups > Create user group
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.
Search
User name
hakim
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
Search
All types
Policy name
Type
Used as
AdministratorAccess
AWS managed - job function
Permissions policy (1)
AmazonAppFlowFullAccess
AWS managed
None
Provides full access to Amazon AppFlo...
AmazonAppFlowReadOnlyAccess
AWS managed
None
Provides read only access to Amazon A...
AmazonAppStreamFullAccess
AWS managed
None
Provides full access to Amazon AppStr...
AmazonAppStreamPCAAccess
AWS managed
None
Amazon AppStream 2.0 access to AWS...
AmazonAppStreamReadOnlyAccess
AWS managed
None
Provides read only access to Amazon A...
AmazonAppStreamServiceAccess
AWS managed
None
Default policy for Amazon AppStream ...
Cancel
Create user group

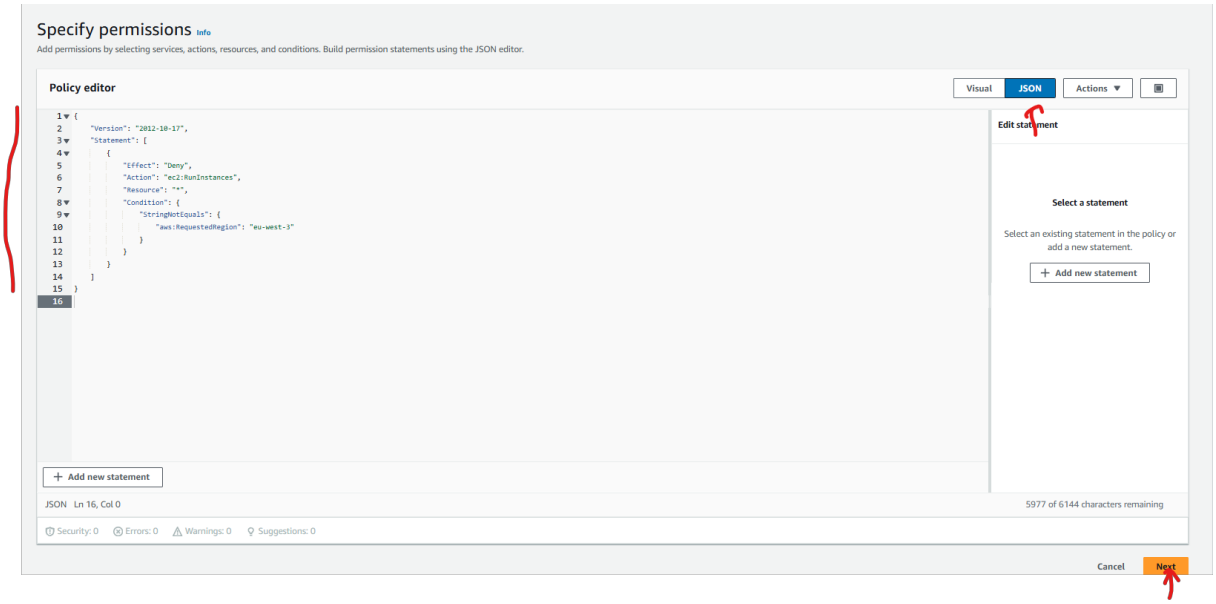


Pour sécuriser notre environnement et rester dans le **Free Tier**, nous allons ajouter les deux conditions suivantes :

- 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».





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)

Show remaining 426 services

Add tags - *optional* Info

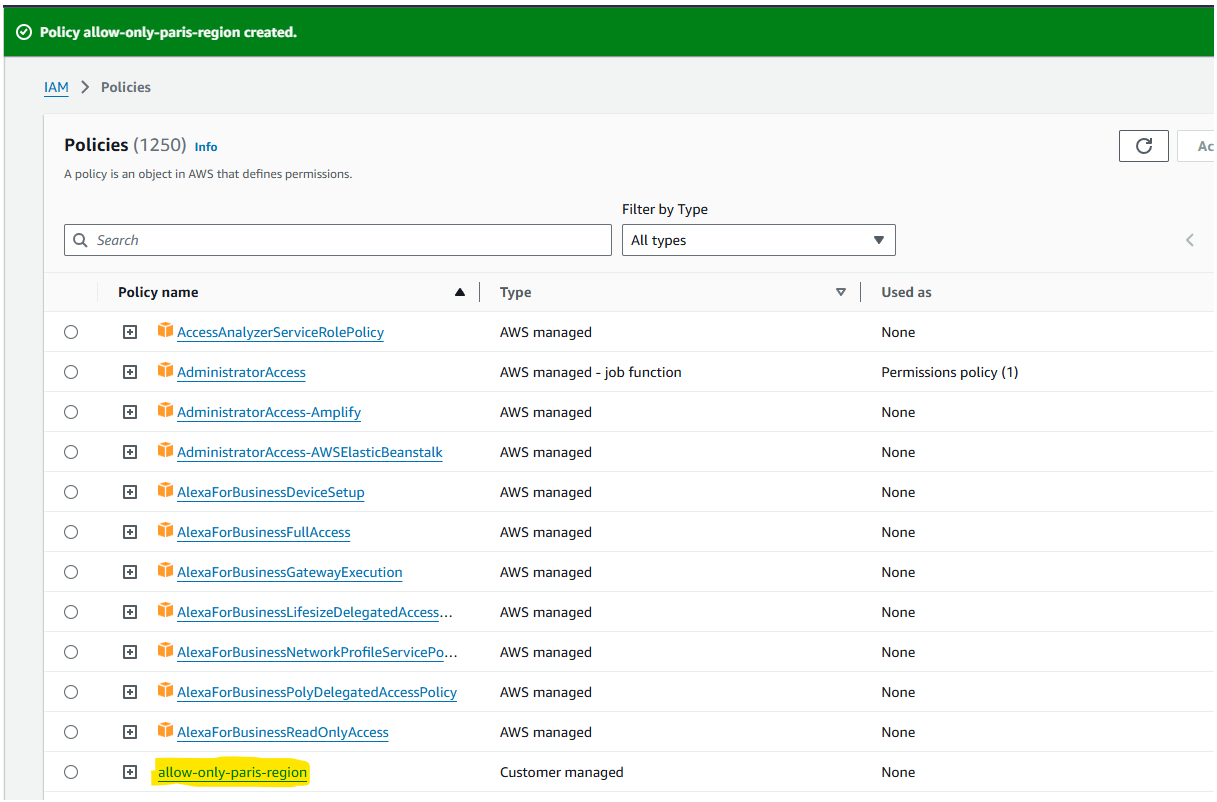
Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

No tags associated with the resource.

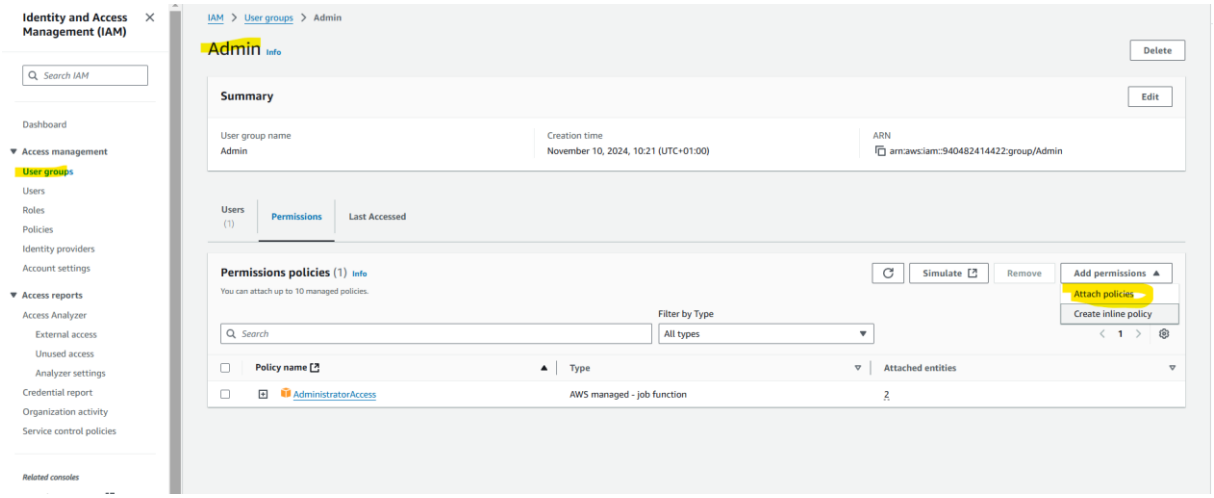
Add new tag

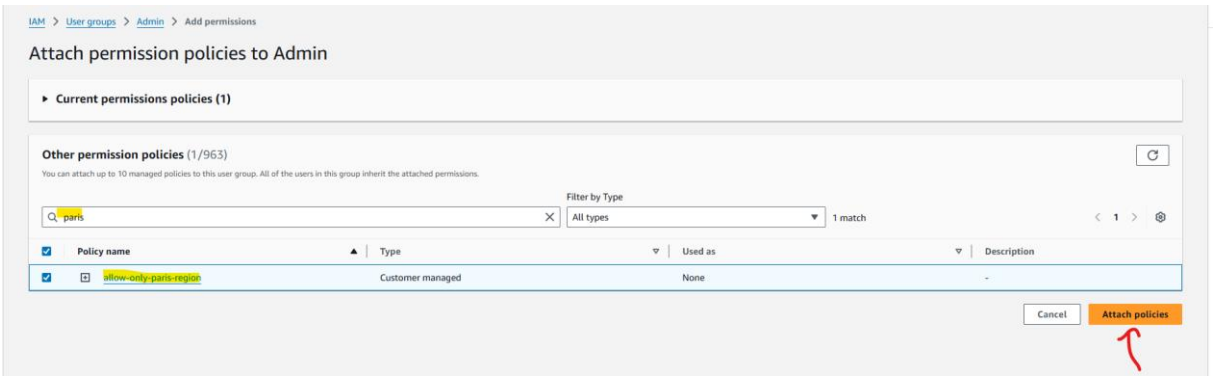
You can add up to 50 more tags.

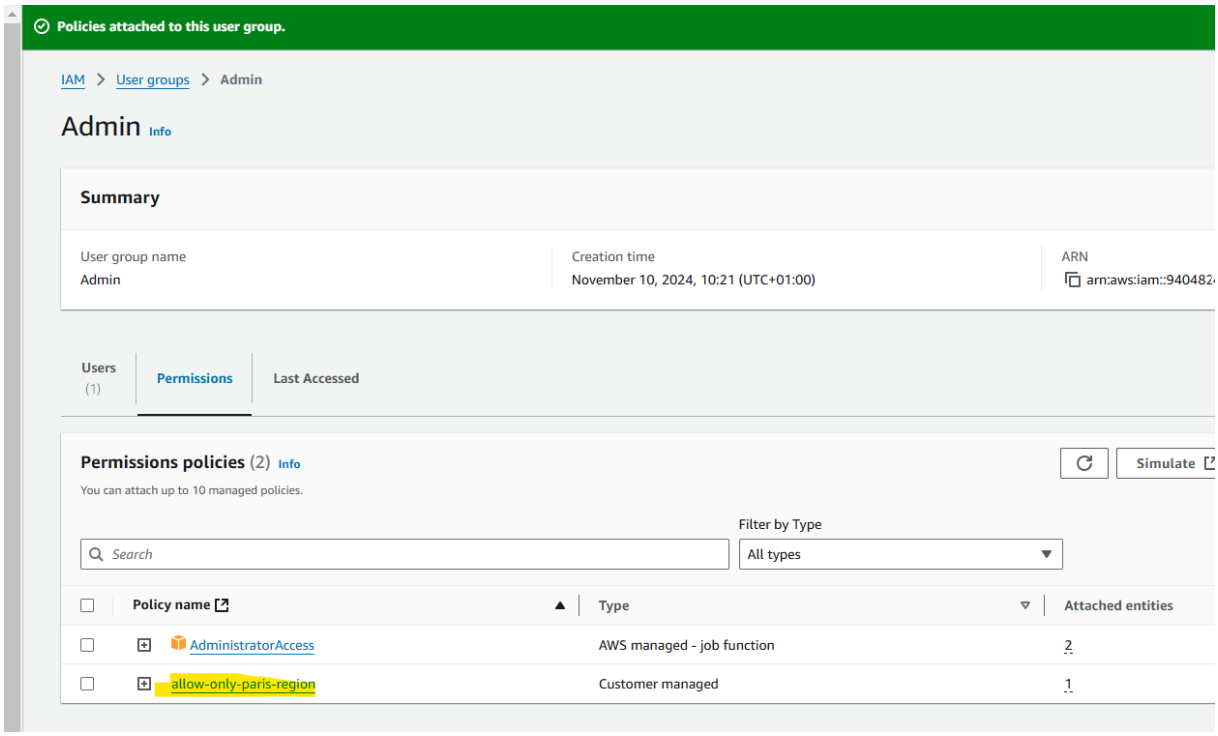
Cancel Previous Create policy



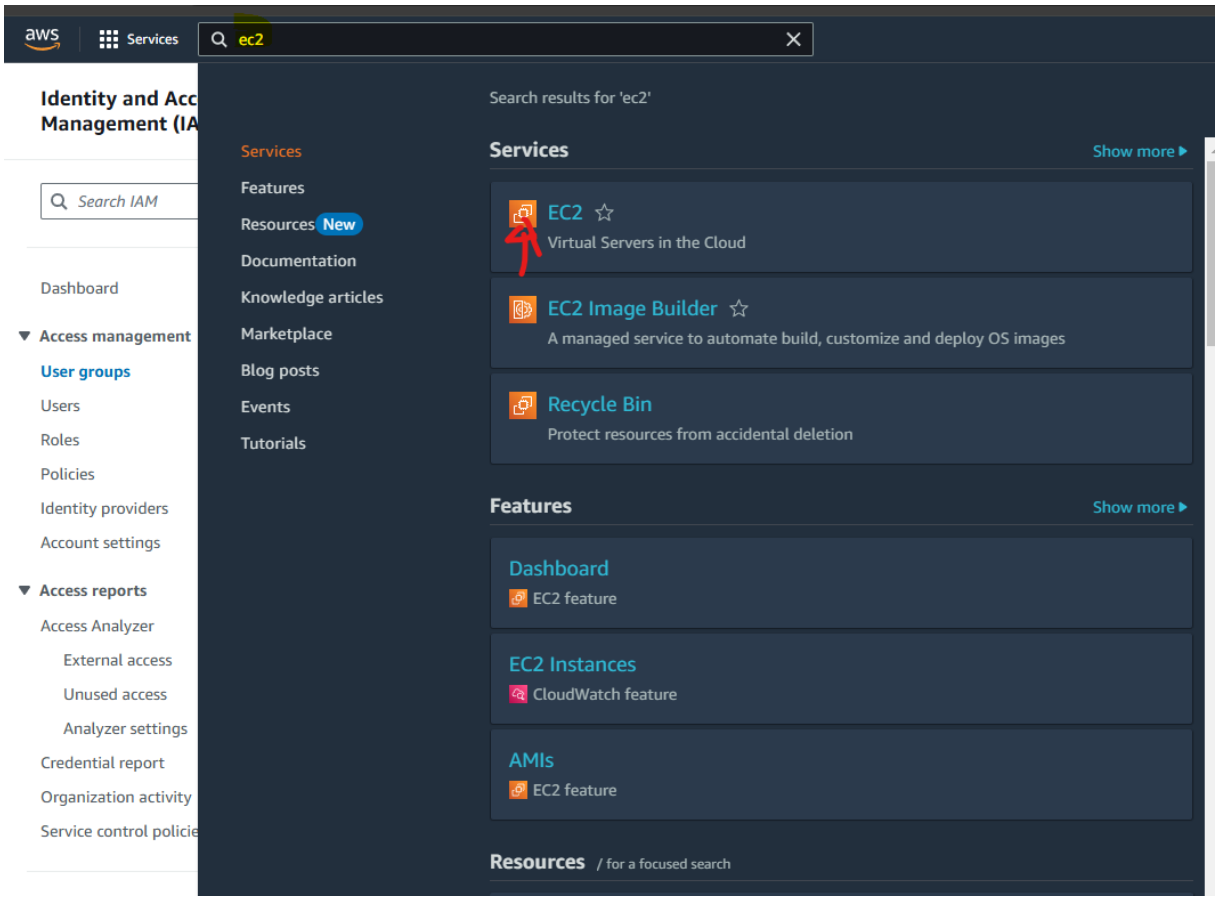
Appliquez cette policy au groupe *admin* qui contient l'utilisateur portant votre nom.

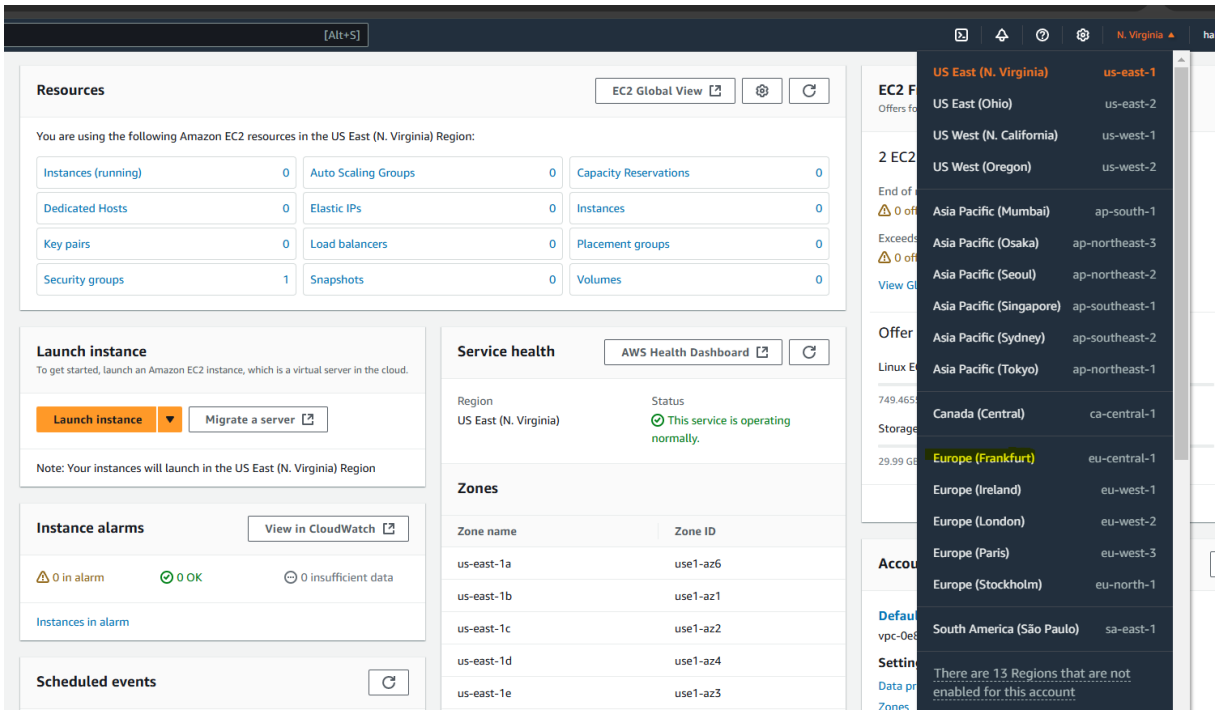


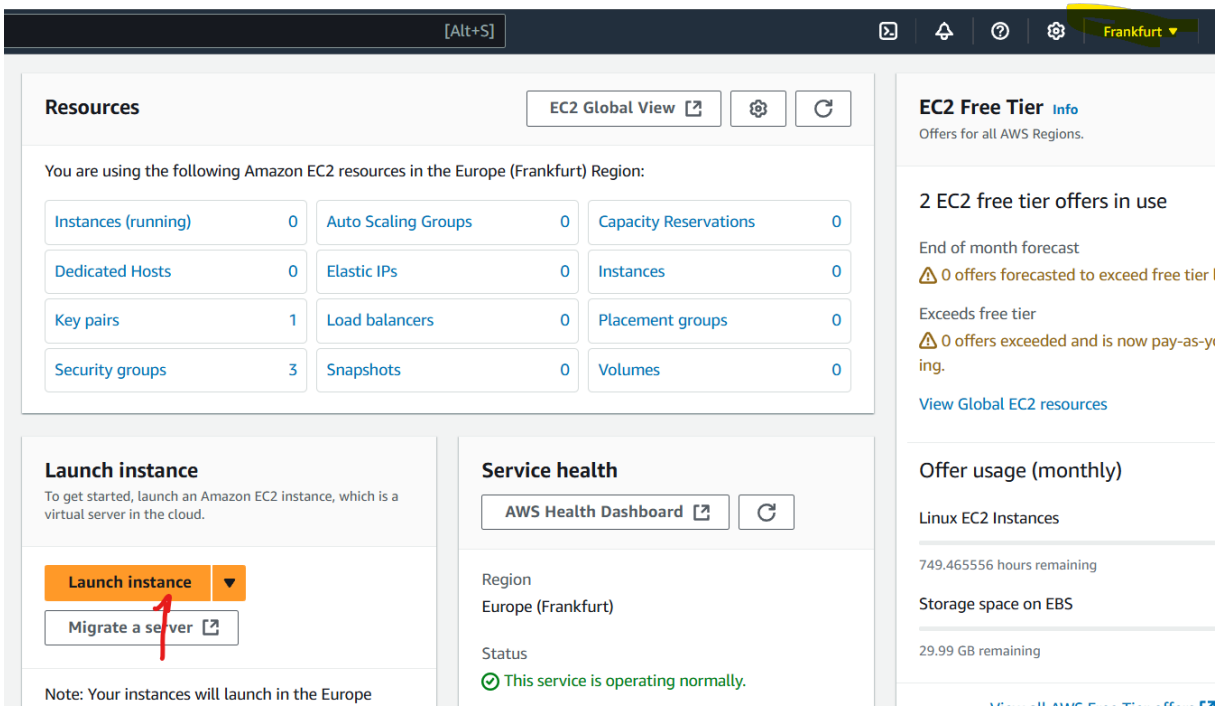


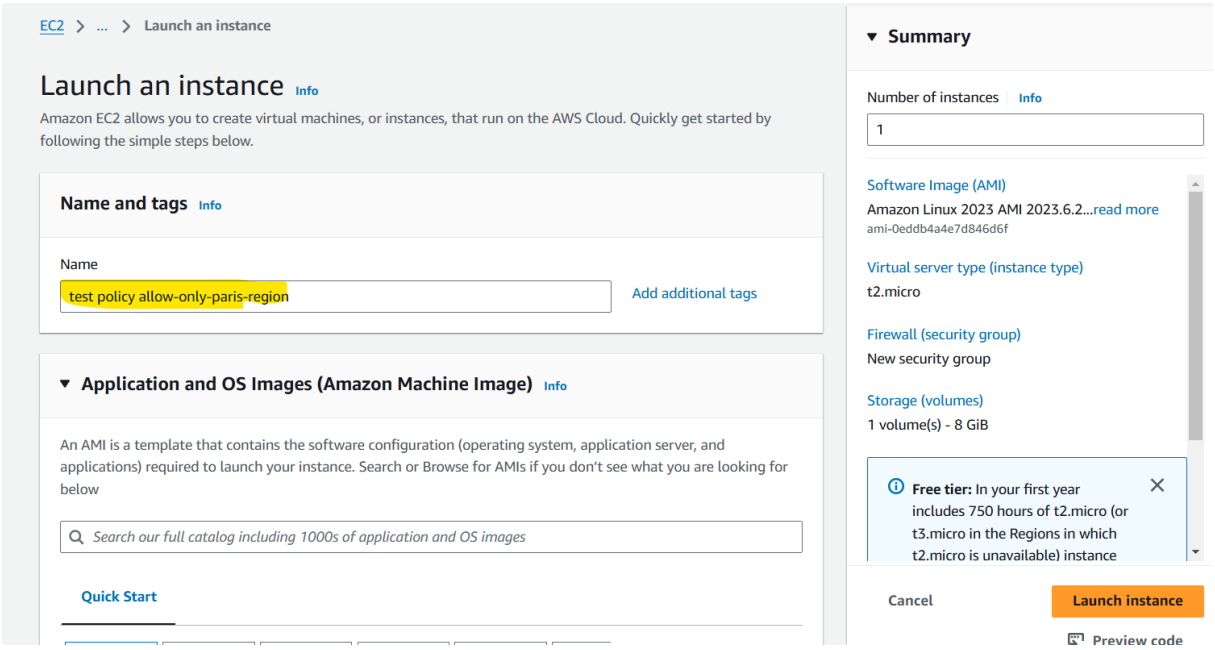


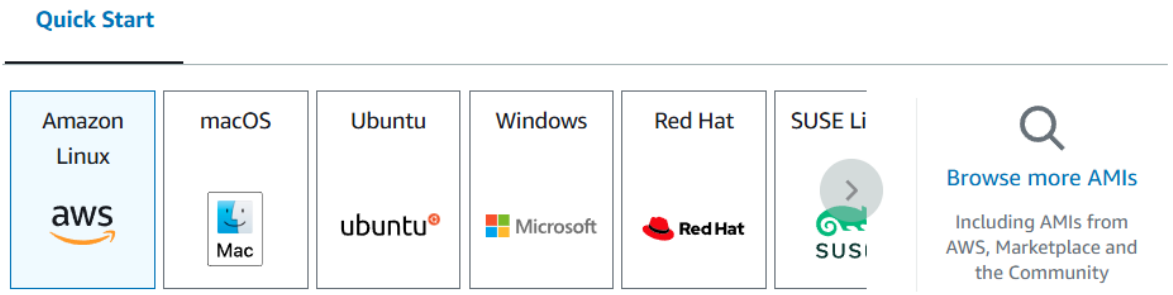
Test de lancement d'une VM *t2.micro* en dehors de la région de Paris (eu-west-3).




[Alt+S]
N. Virginia
Resources
EC2 Global View
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
US East (N. Virginia)
Status
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
Instance alarms
View in CloudWatch
0 in alarm
0 OK
0 insufficient data
Instances in alarm
Scheduled events
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]
Frankfurt
Resources
EC2 Global View
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
Europe (Frankfurt)
Status
This service is operating normally.
EC2 Free Tier Info
Offers for all AWS Regions.
2 EC2 free tier offers in use
End of month forecast
0 offers forecasted to exceed free tier
Exceeds free tier
0 offers exceeded and is now pay-as-y
ing.
View Global EC2 resources
Offer usage (monthly)
Linux EC2 Instances
749.465556 hours remaining
Storage space on EBS
29.99 GB remaining





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
Free tier eligible

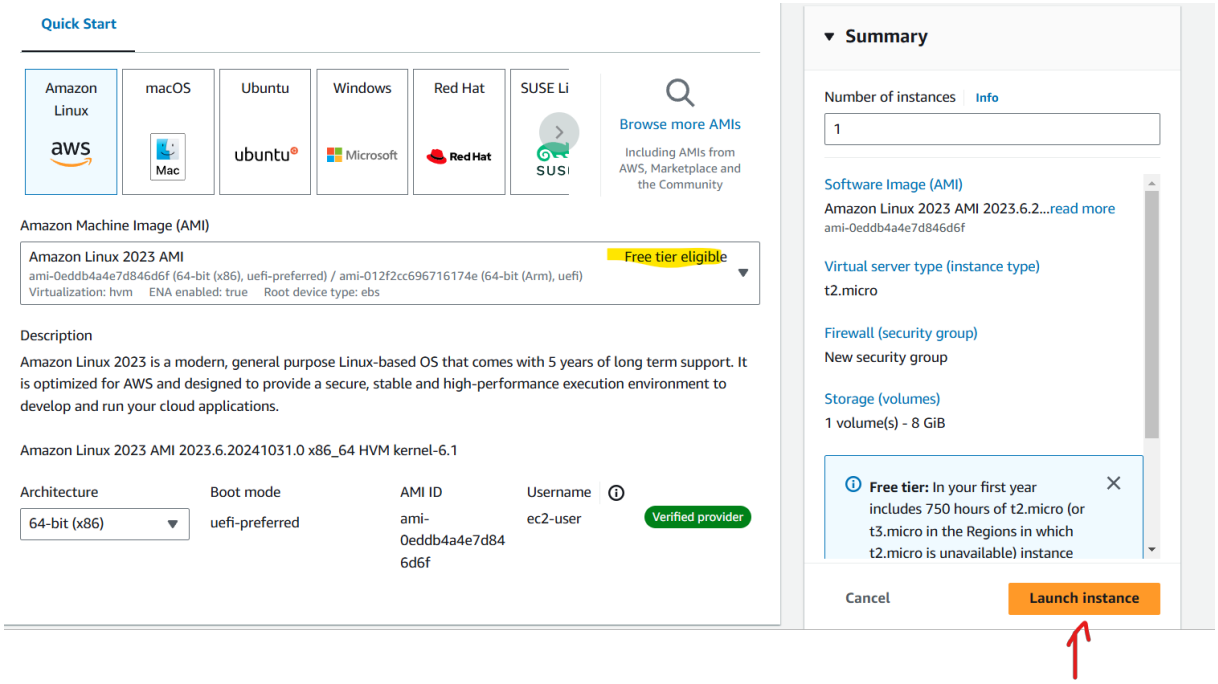
Description

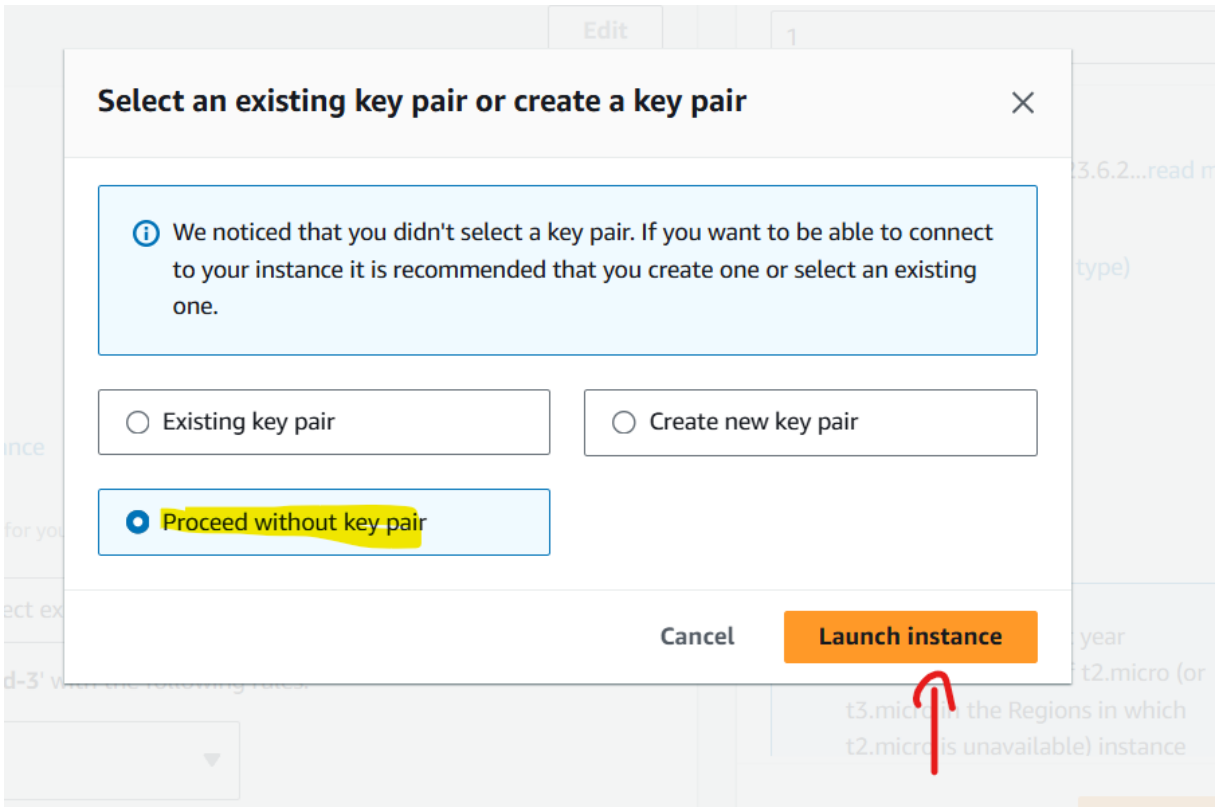
Amazon Linux 2023 is a modern, general purpose Linux-based OS that comes with 5 years of long term support. It is optimized for AWS and designed to provide a secure, stable and high-performance execution environment to develop and run your cloud applications.

Amazon Linux 2023 AMI 2023.6.20241031.0 x86_64 HVM kernel-6.1

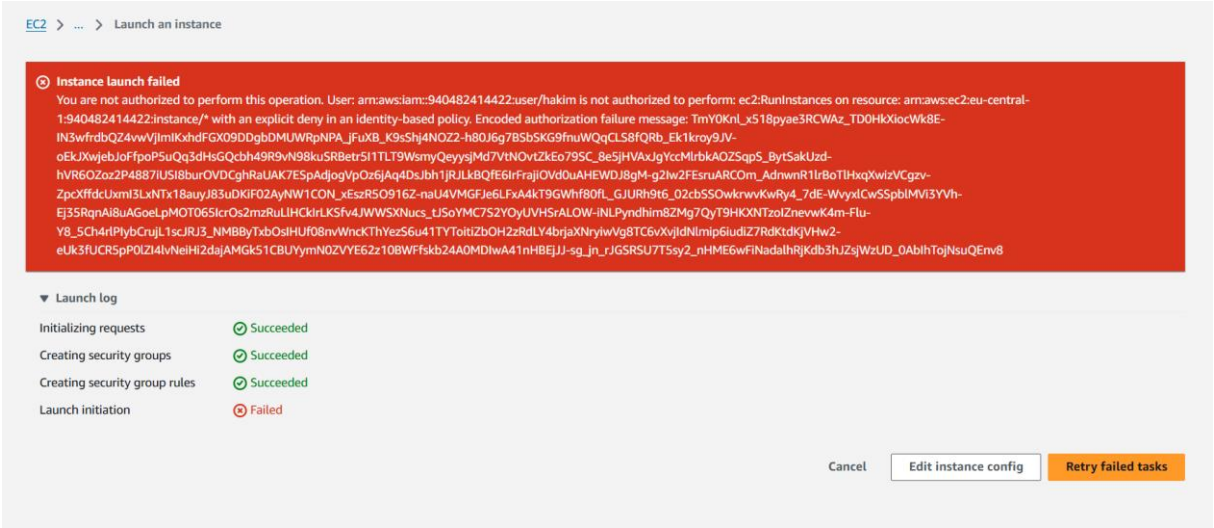
Architecture	Boot mode	AMI ID	Username
64-bit (x86)	uefi-preferred	ami-0eddb4a4e7d846d6f	ec2-user

Verified provider


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-0eddb4a4e7d846d6f (64-bit (x86), uefi-preferred) / ami-012f2cc696716174e (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
64-bit (x86)
Boot mode
uefi-preferred
AMI ID
ami-0eddb4a4e7d846d6f
Username
ec2-user
Verified provider
Summary
Number of instances Info
1
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
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

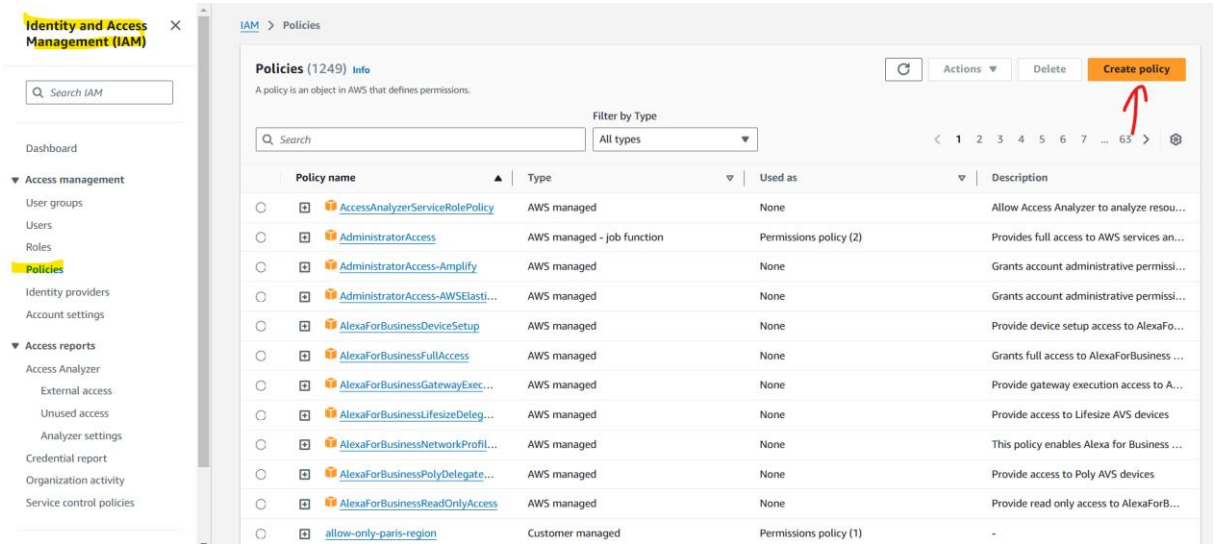
Vous devez avoir ce message d'erreur.



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).

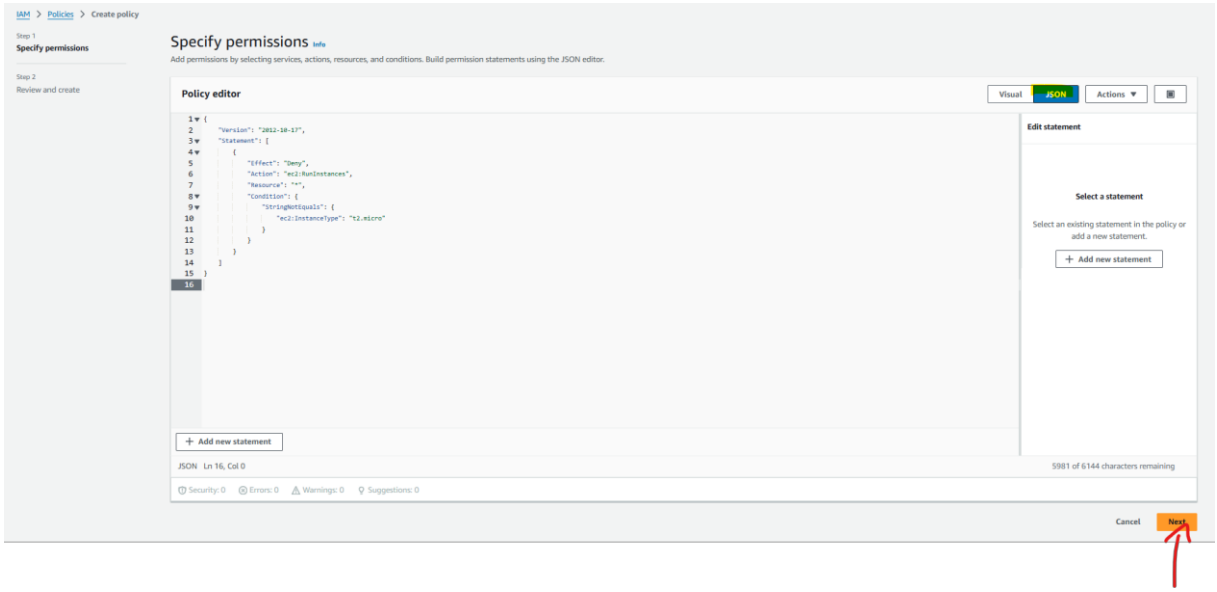
Creation de la policy « allow-only-t2.micro».

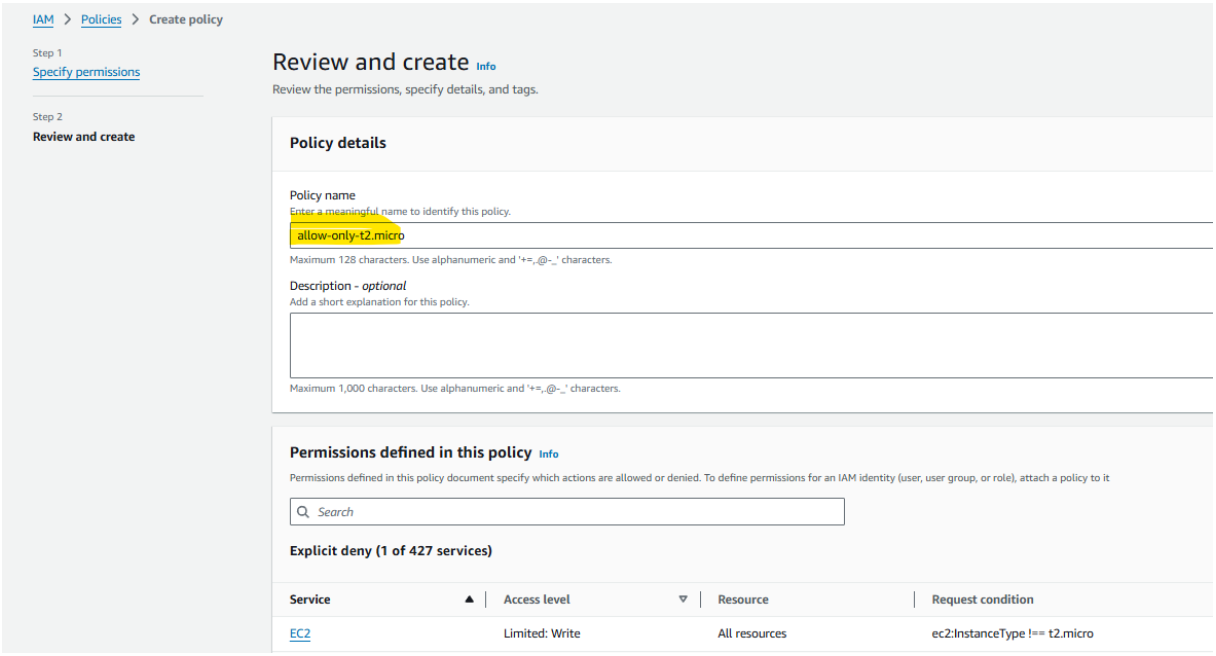


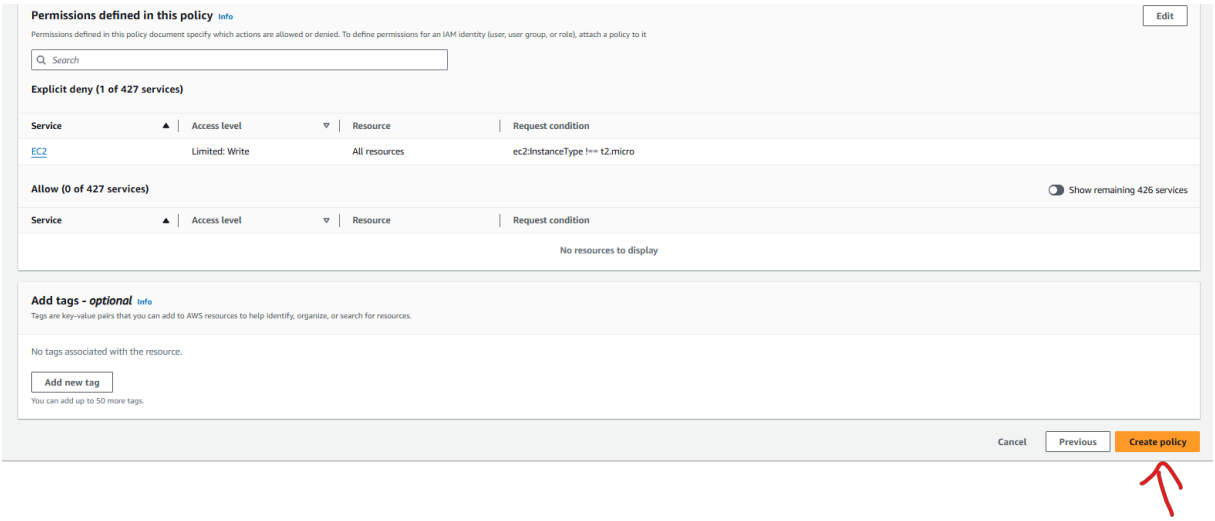
Utilise le code JSON ci-après

```
{
    "Version": "2012-10-17",
    "Statement": [
```

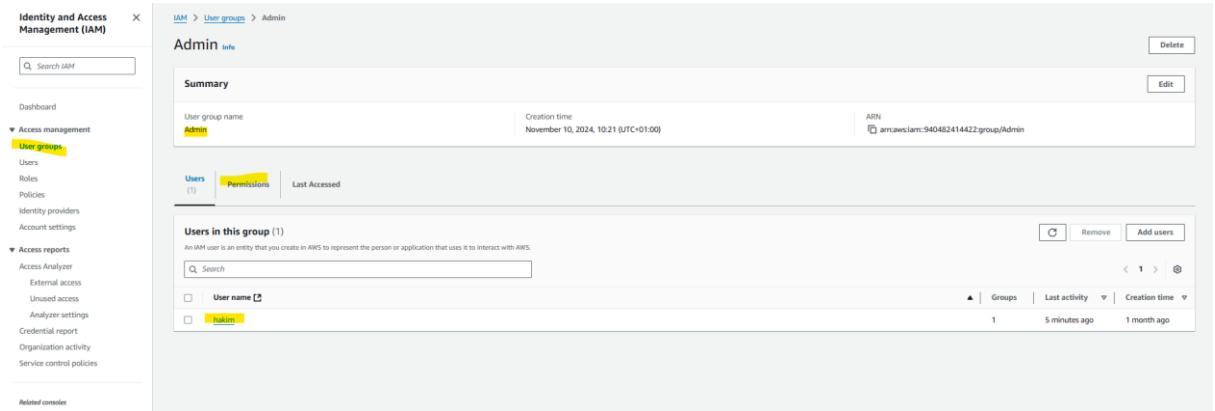
```
        {
            "Effect": "Deny",
            "Action": "ec2:RunInstances",
            "Resource": "*",
            "Condition": {
                "StringNotEquals": {
                    "ec2:InstanceType": "t2.micro"
                }
            }
        }
    ]
}
```

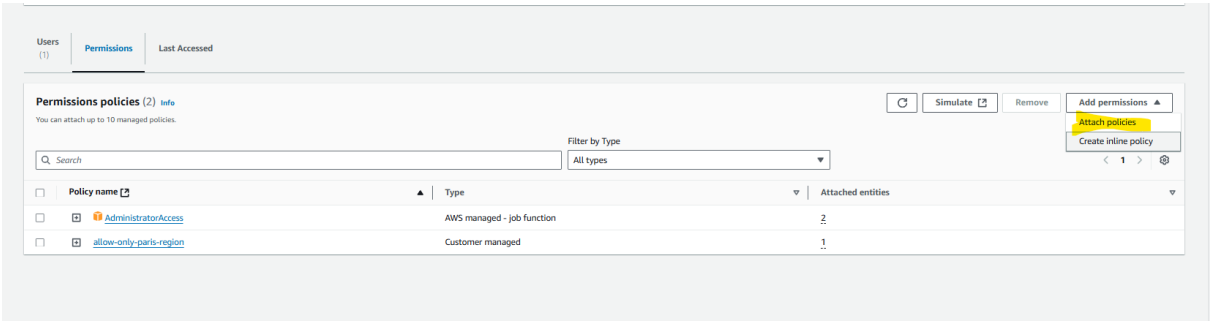


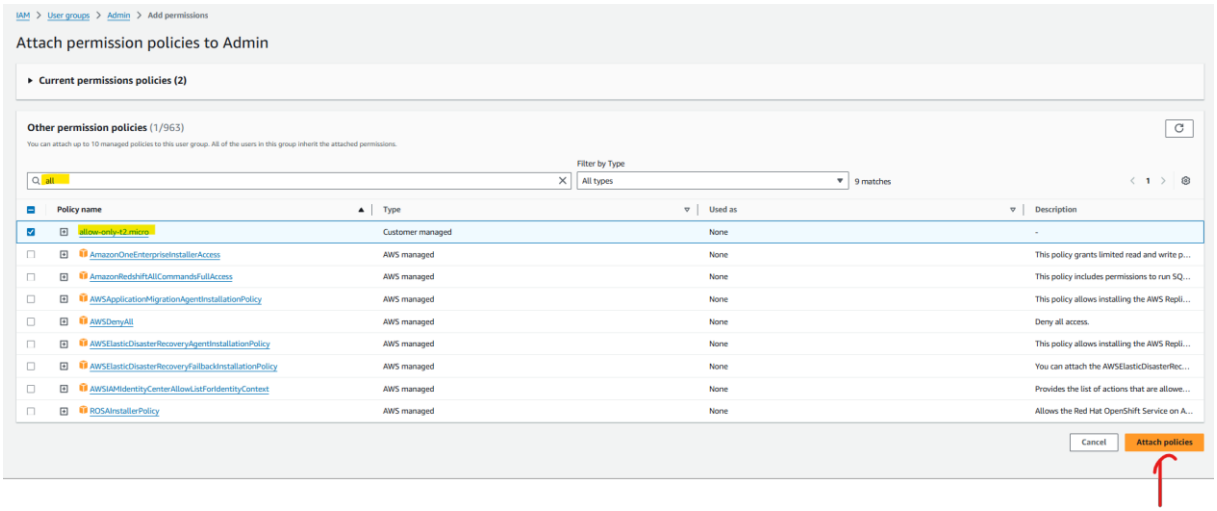


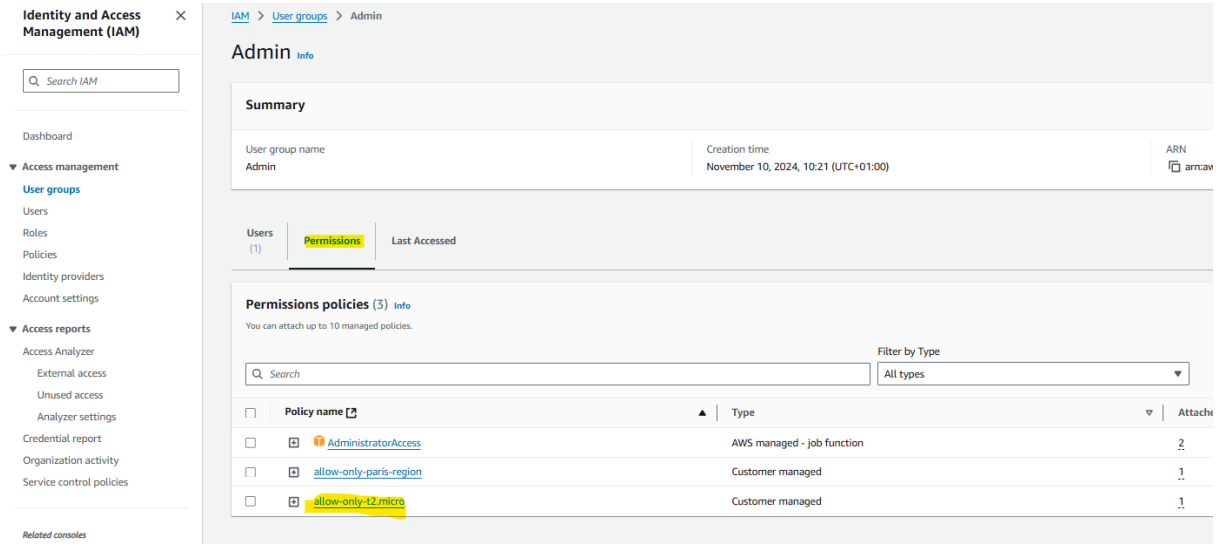


Appliquez cette policy au groupe *admin* qui contient l'utilisateur portant votre nom.

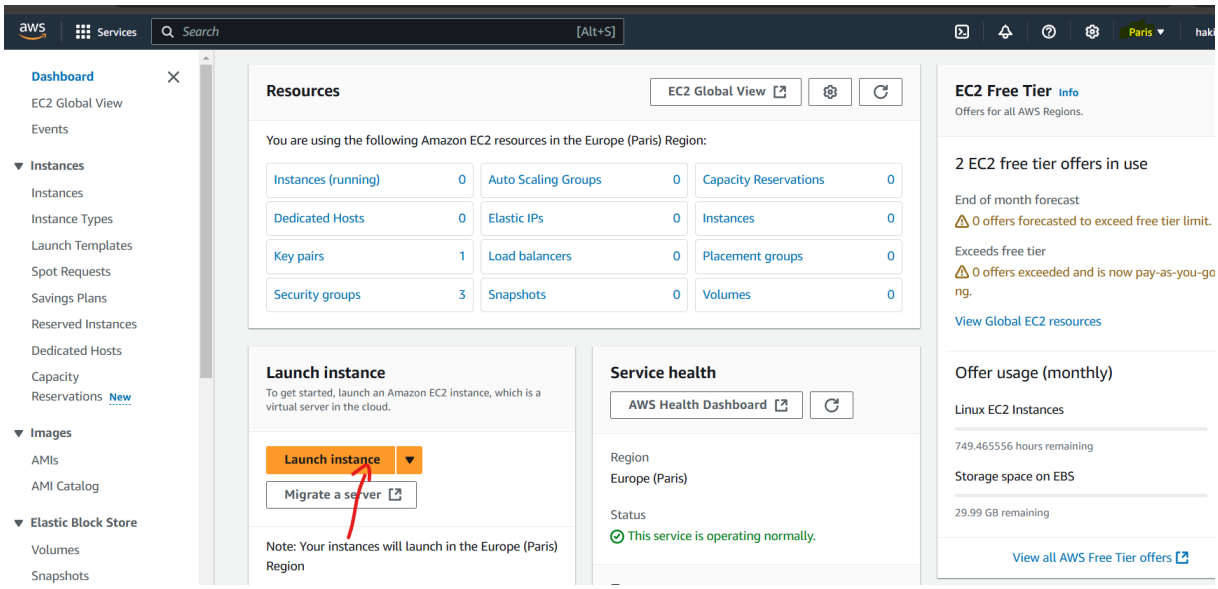


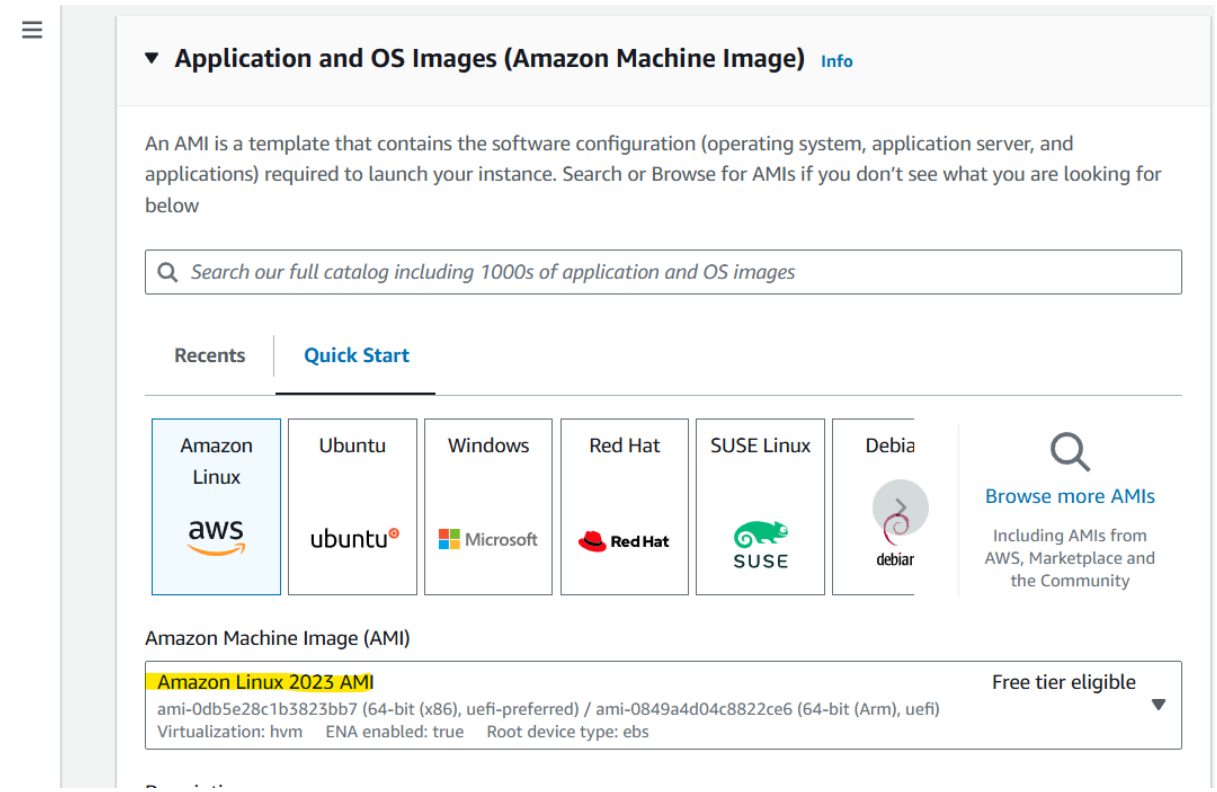






Test de lancement d'une VM *t2.nano* dans la région de Paris (eu-west-3).


Services
Search
[Alt+S]
Paris
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
Resources
EC2 Global View
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.
Launch instance
Migrate a server
Note: Your instances will launch in the Europe (Paris) Region
Service health
AWS Health Dashboard
Region
Europe (Paris)
Status
This service is operating normally.
EC2 Free Tier Info
Offers for all AWS Regions.
2 EC2 free tier offers in use
End of month forecast
0 offers forecasted to exceed free tier limit.
Exceeds free tier
0 offers exceeded and is now pay-as-you-go ng.
View Global EC2 resources
Offer usage (monthly)
Linux EC2 Instances
749.465556 hours remaining
Storage space on EBS
29.99 GB remaining
View all AWS Free Tier offers


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
Debia
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

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
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

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

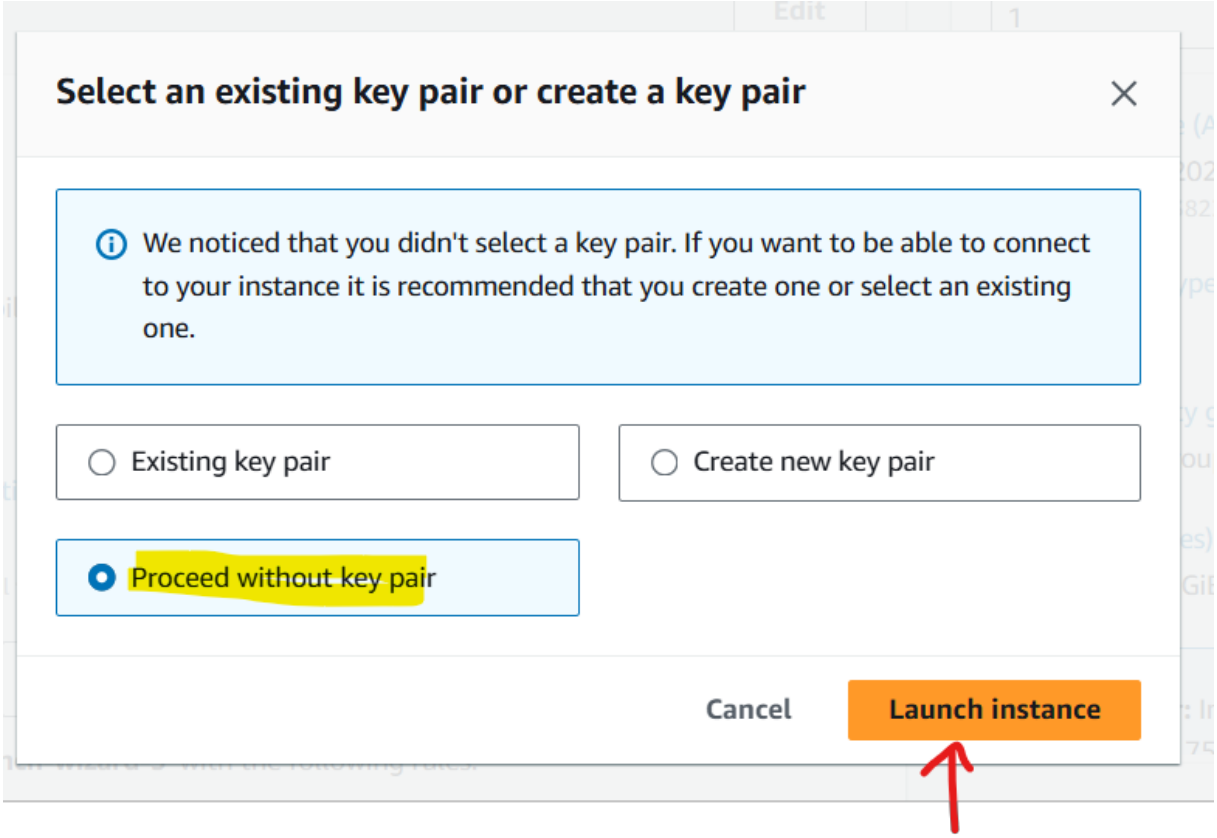
Firewall (security group)
New security group

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

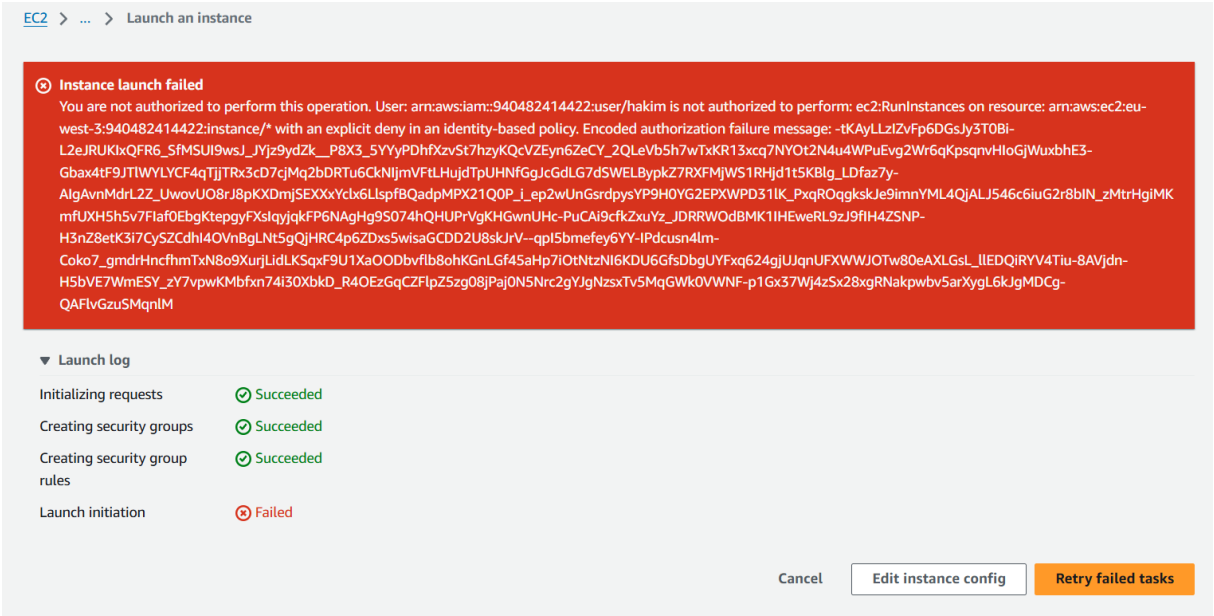
Free tier: In your first year includes 750 hours of t2.micro (or

Cancel Launch instance

Preview code



Vous devez avoir ce message d'erreur.

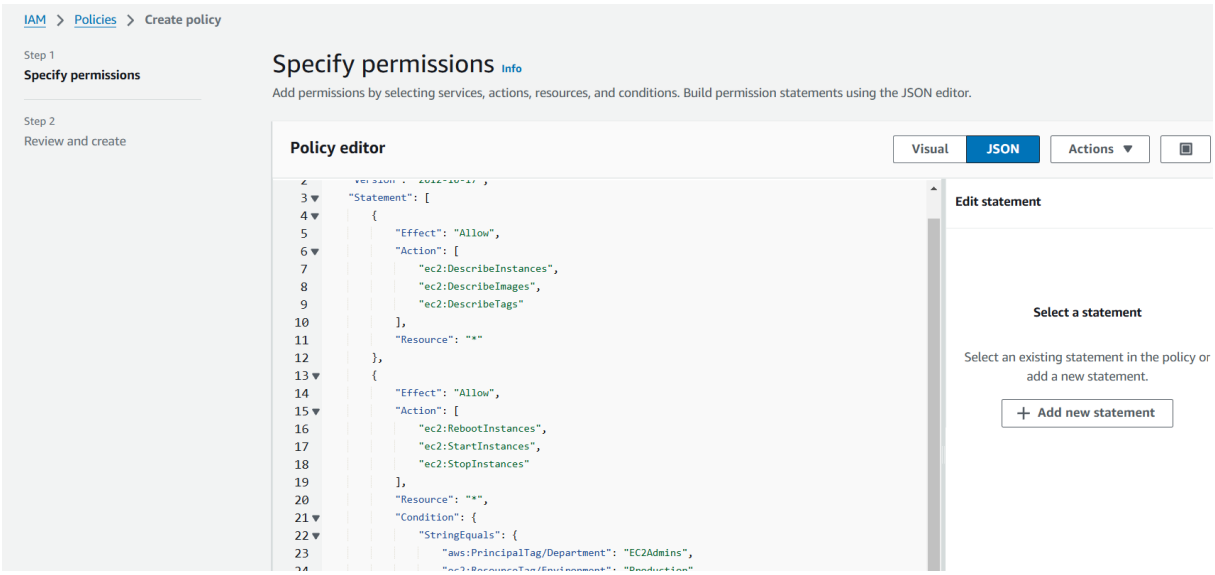


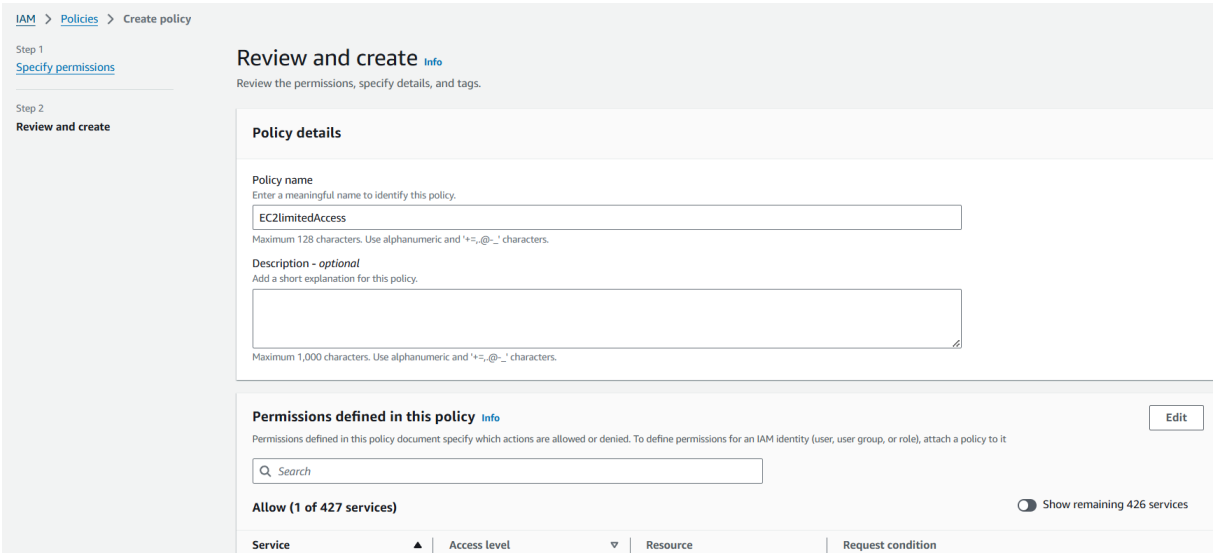
Si ce n'est pas le cas et que l'instance parvient à se lancer, merci de m'informer afin que je puisse vous aider à arrêter cette instance.

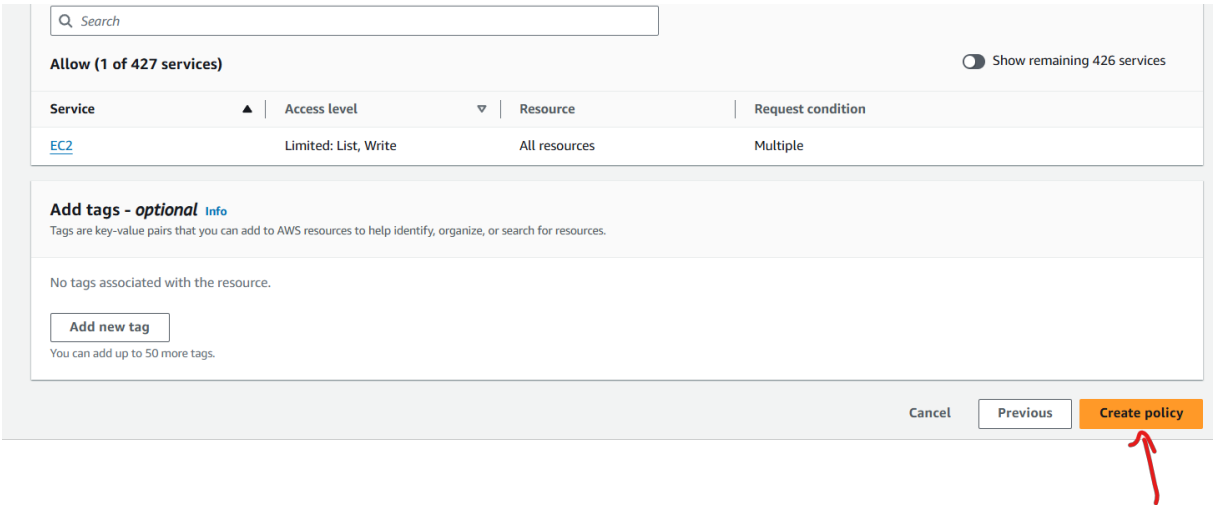
7 **ABAC :** Nous allons gérer les autorisations AWS en nous basant sur les attributs

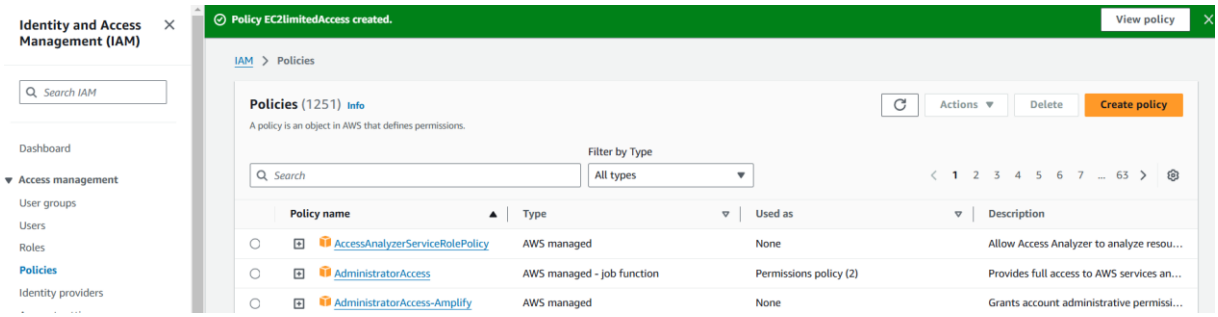
Ajoutez une policy nommée **EC2limitedAccess** avec le code JSON ci-après.

```
{
    "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"
                }
            }
        }
    ]
}
```

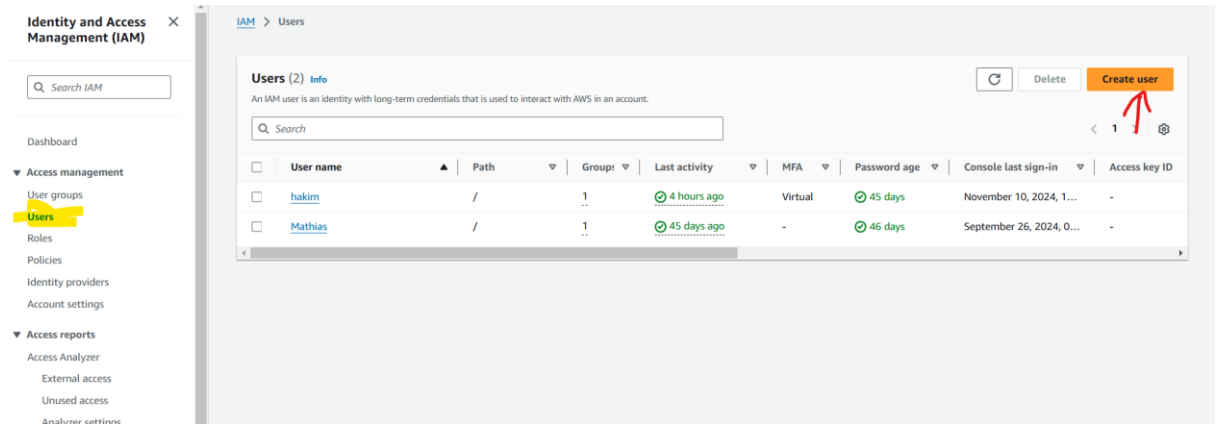

IAM > Policies > Create policy
Step 1
Specify permissions
Step 2
Review and create
Specify permissions Info
Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.
Policy editor
Visual
JSON
Actions
"Statement": [
{
"Effect": "Allow",
"Action": [
"ec2:DescribeInstances",
"ec2:DescribeImages",
"ec2:DescribeTags"
],
"Resource": "*"
},
{
"Effect": "Allow",
"Action": [
"ec2:RebootInstances",
"ec2:StartInstances",
"ec2:StopInstances"
],
"Resource": "*",
"Condition": {
"StringEquals": {
"aws:PrincipalTag/Department": "EC2Admins",
Edit statement
Select a statement
Select an existing statement in the policy or add a new statement.
Add new statement

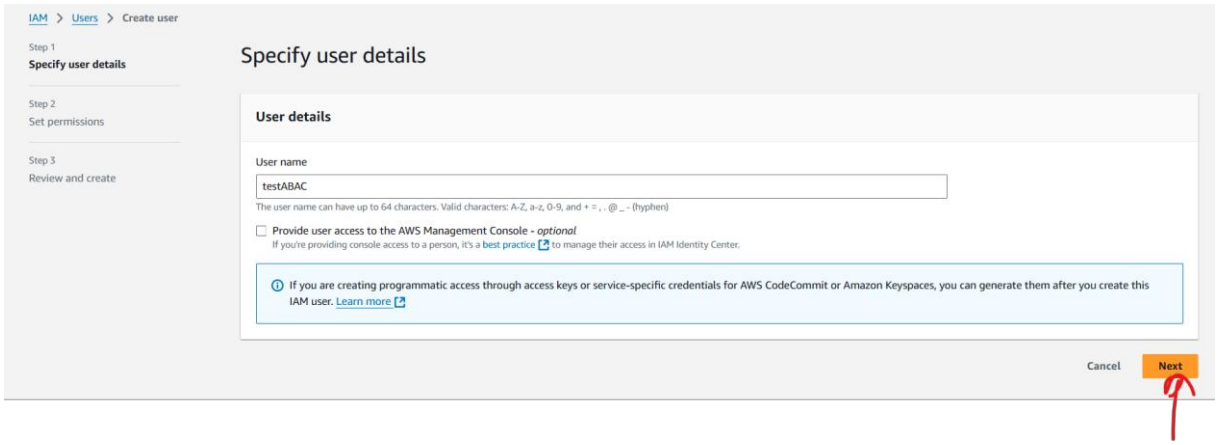

IAM > Policies > Create policy
Step 1
Specify permissions
Step 2
Review and create
Review and create Info
Review the permissions, specify details, and tags.
Policy details
Policy name
Enter a meaningful name to identify this policy.
EC2limitedAccess
Maximum 128 characters. Use alphanumeric and '+=,.@-_' 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
Allow (1 of 427 services)
Show remaining 426 services
Service
Access level
Resource
Request condition

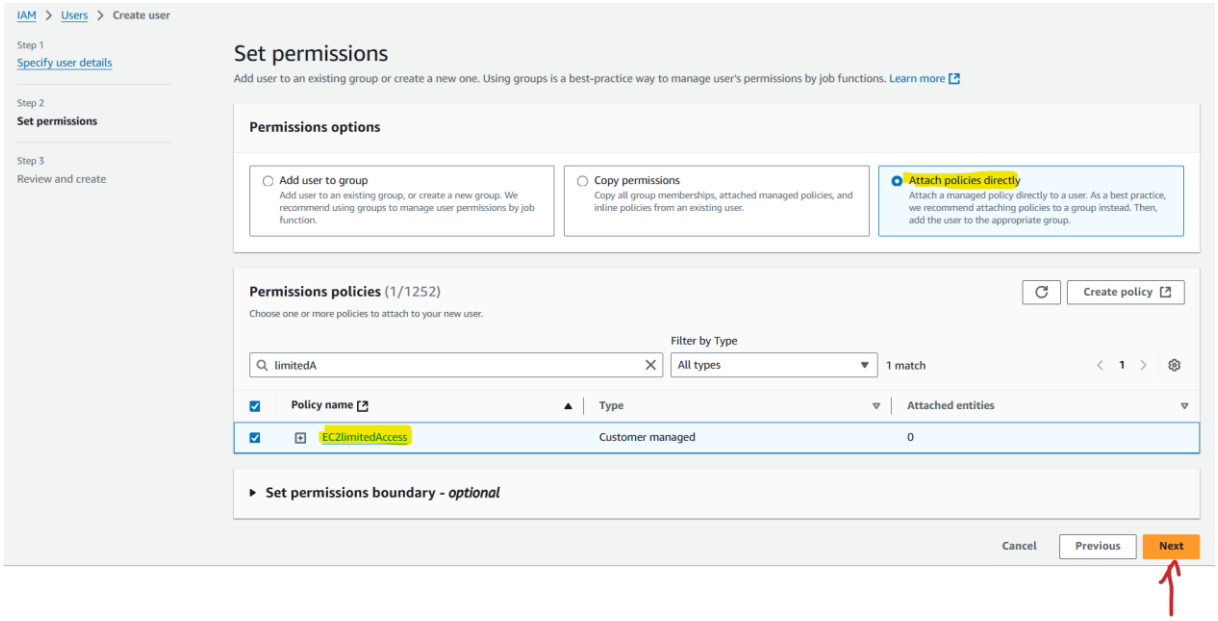

Search
Allow (1 of 427 services)
Show remaining 426 services
Service
Access level
Resource
Request condition
EC2
Limited: List, Write
All resources
Multiple
Add tags - optional Info
Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.
No tags associated with the resource.
Add new tag
You can add up to 50 more tags.
Cancel
Previous
Create policy



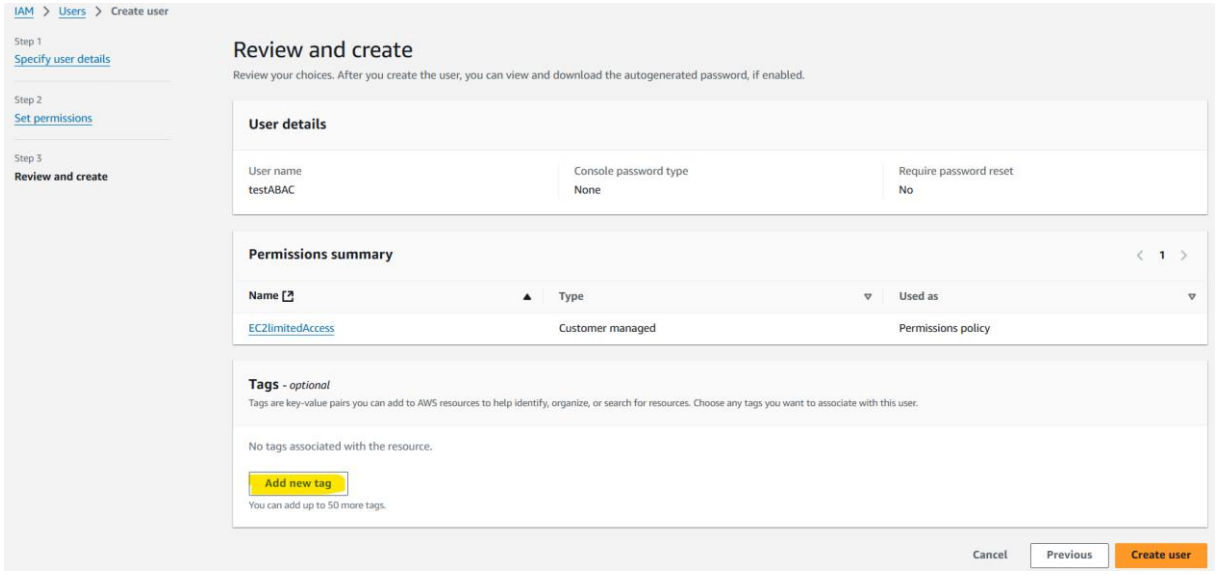
Ajoutez un utilisateur nommé **testABAC** et affectez-lui la policy **EC2limitedAccess**.

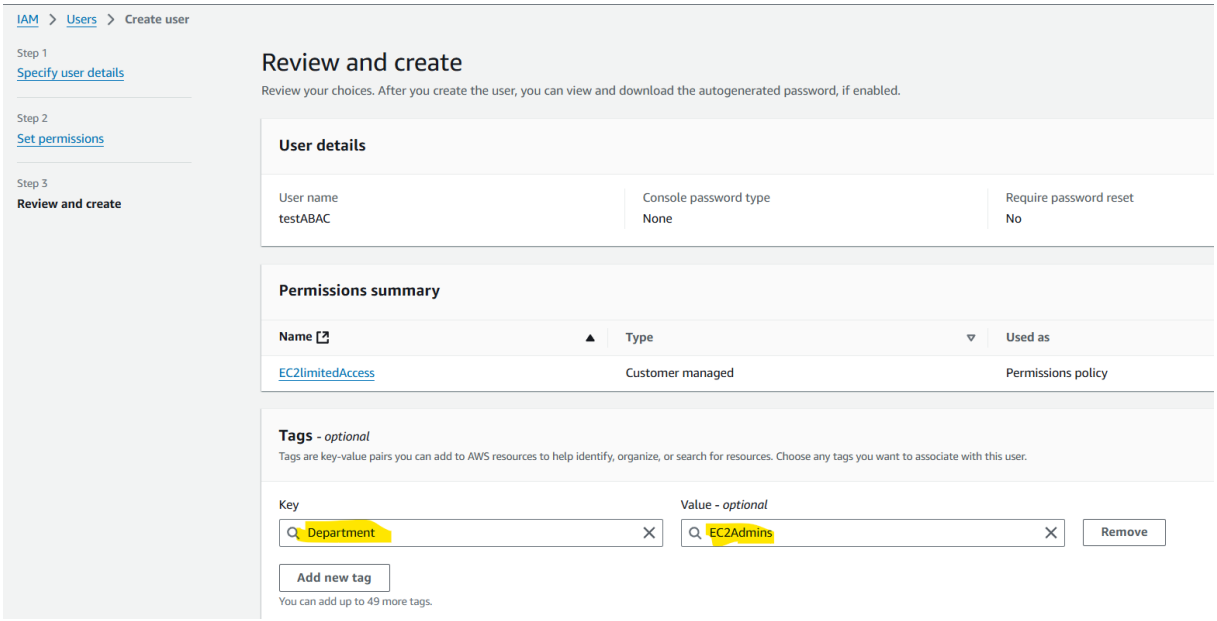




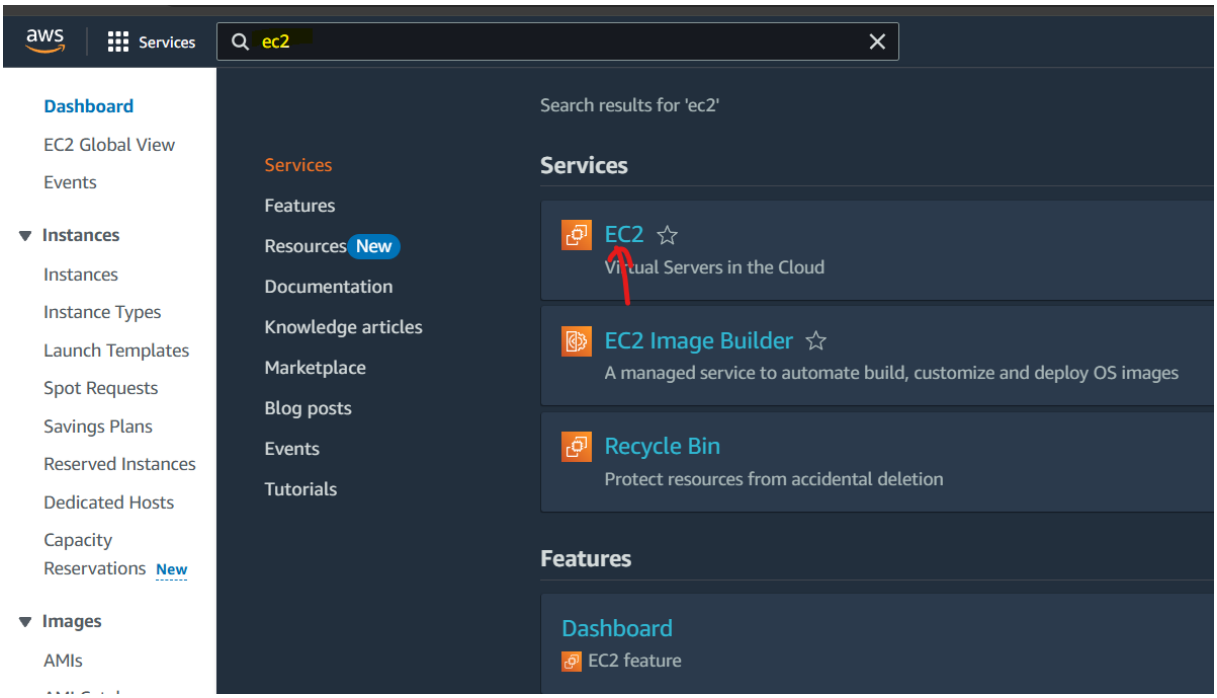


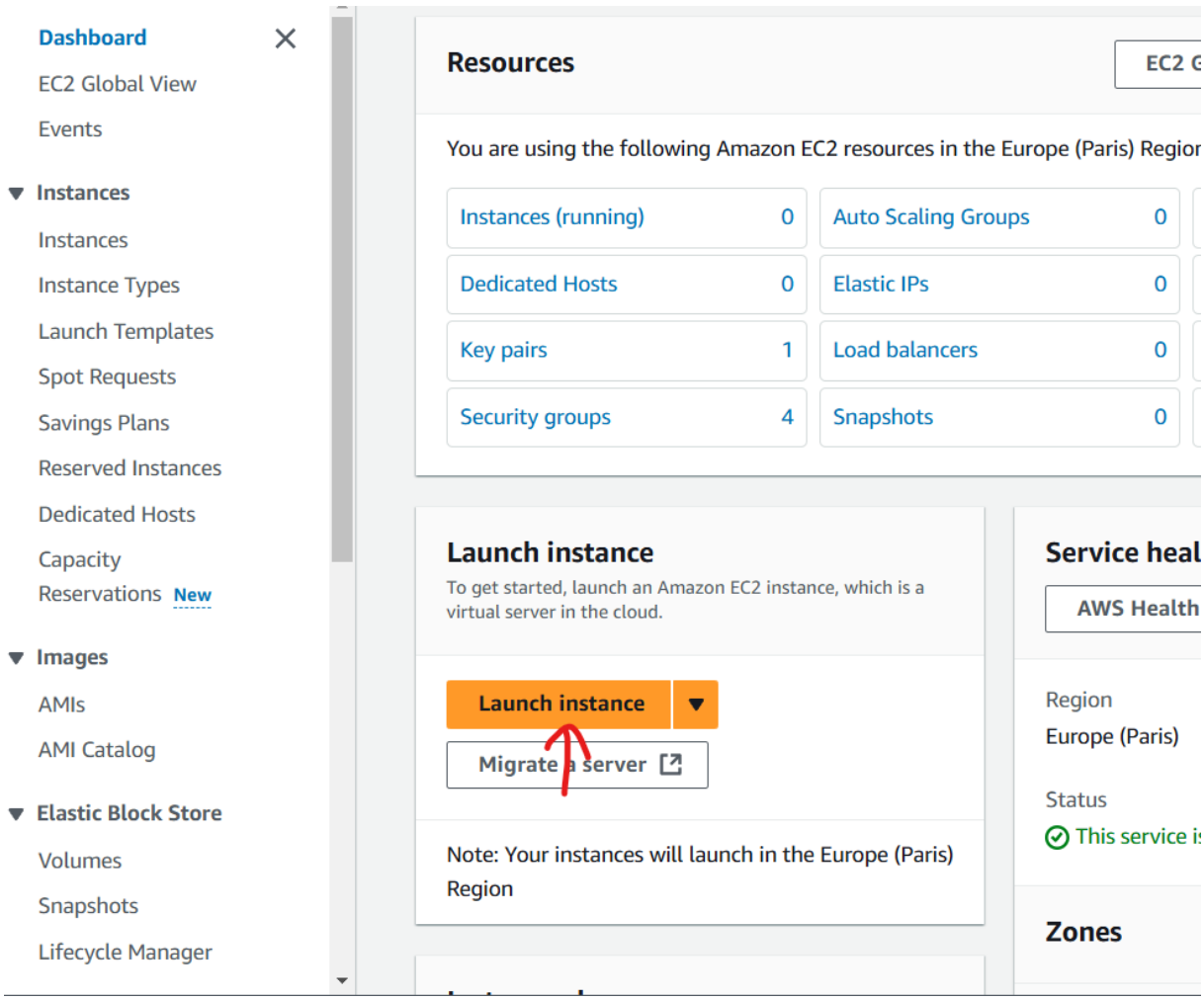
Ajoutez des tags à l'utilisateur testABAC avec key= Department et value= EC2Admins





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




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
EC2 G
You are using the following Amazon EC2 resources in the Europe (Paris) Regior
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 heal
AWS Health
Region
Europe (Paris)
Status
This service i
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 | Debia

Browse more AMIs

Including AMIs from AWS, Marketplace and the Community

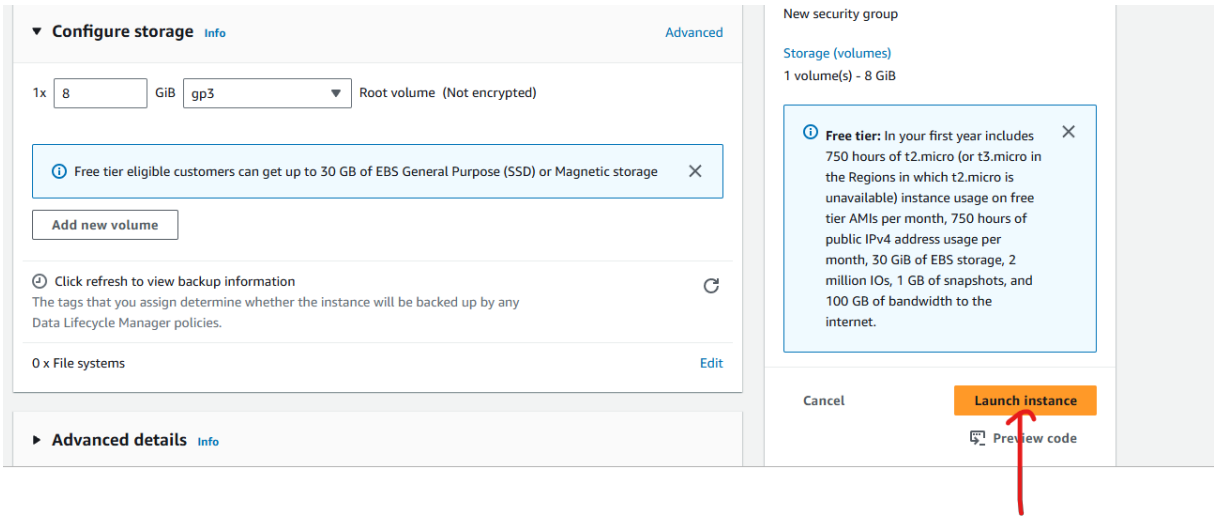
Amazon Machine Image (AMI)

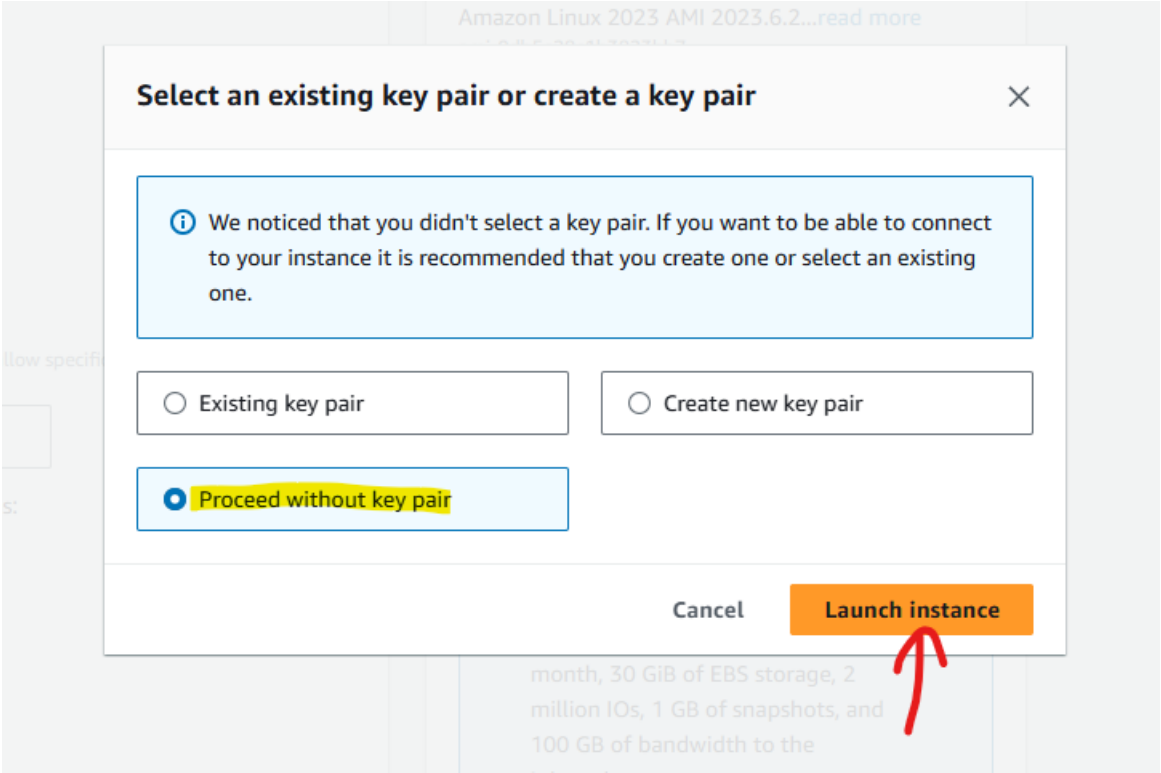
Amazon Linux 2023 AMI

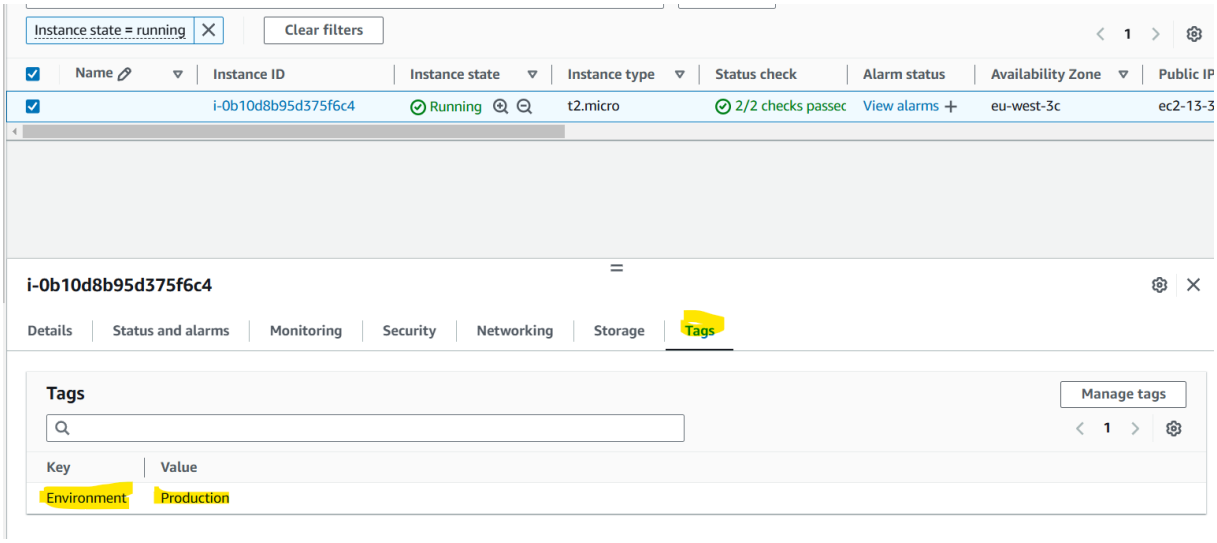
Free tier eligible

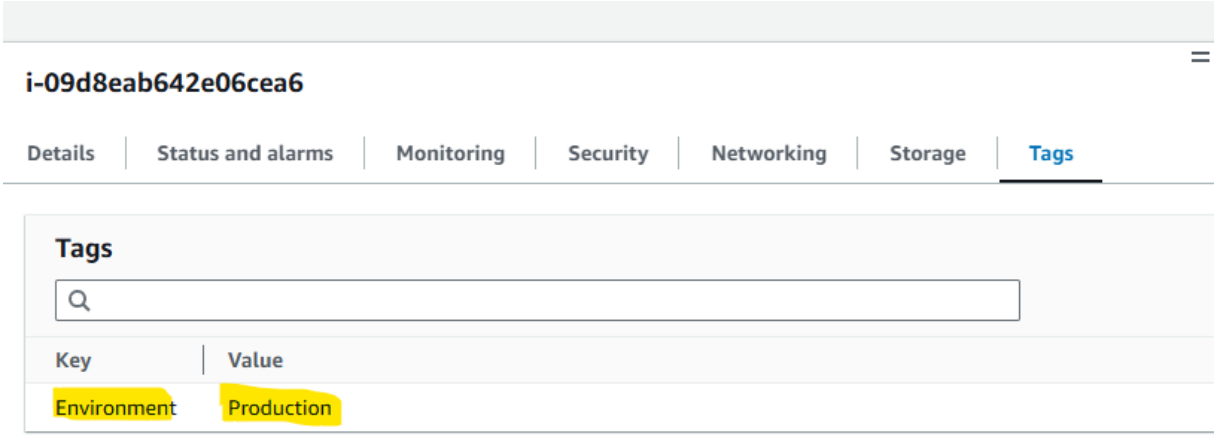
ami-0db5e28c1b3823bb7 (64-bit (x86), uefi-preferred) / ami-0849a4d04c8822ce6 (64-bit (Arm), uefi)

Virtualization: hvm ENA enabled: true Root device type: ebs

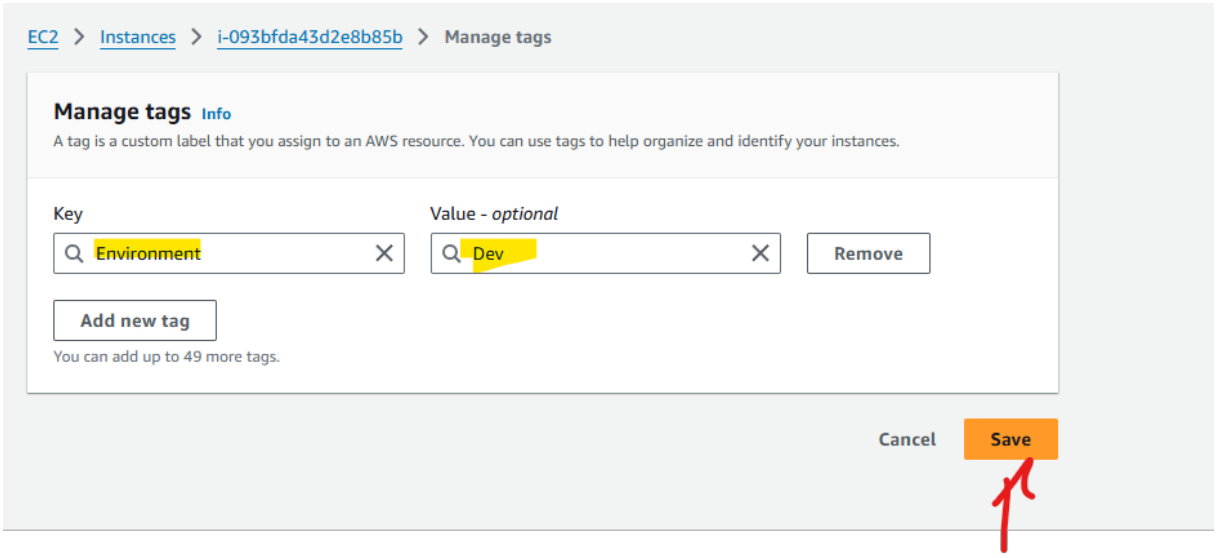



Amazon Linux 2023 AMI 2023.6.2...read more
Select an existing key pair or create a key pair
We noticed that you didn't select a key pair. If you want to be able to connect to your instance it is recommended that you create one or select an existing one.
Existing key pair
Create new key pair
Proceed without key pair
Cancel
Launch instance
month, 30 GiB of EBS storage, 2 million IOs, 1 GB of snapshots, and 100 GB of bandwidth to the


Instance state = running
Clear filters
1
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
Availability Zone
Public IP
i-0b10d8b95d375f6c4
Running
t2.micro
2/2 checks passec
View alarms
eu-west-3c
ec2-13-3
i-0b10d8b95d375f6c4
Details
Status and alarms
Monitoring
Security
Networking
Storage
Tags
Tags
Manage tags
1
Key
Value
Environment
Production

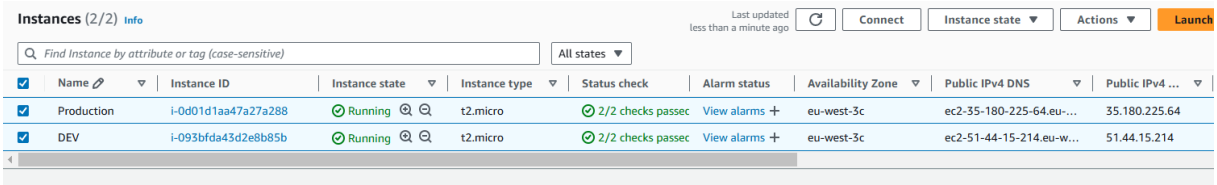


Lance une desiemme Instence EC2 avec la tag key= Environment value = Dev

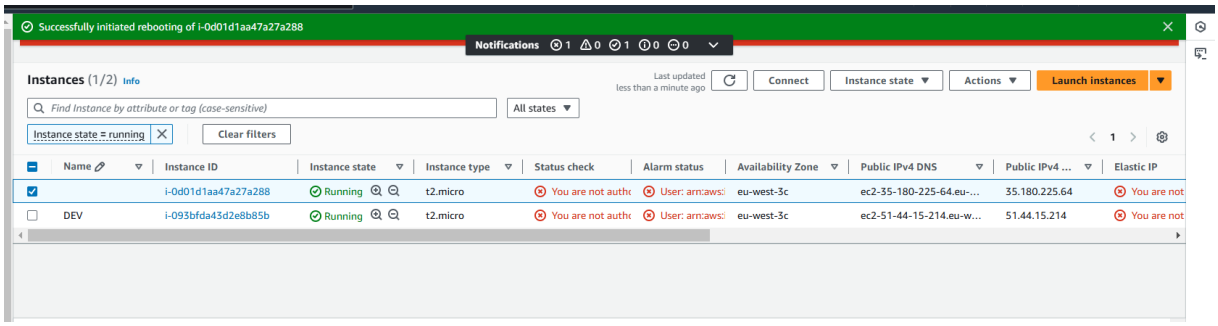


Connectez-vous en tant qu'utilisateur **testABAC**.

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



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



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