Rendu TP06

Rendu de TP06 effectué par `Thomas PEUGNET`.

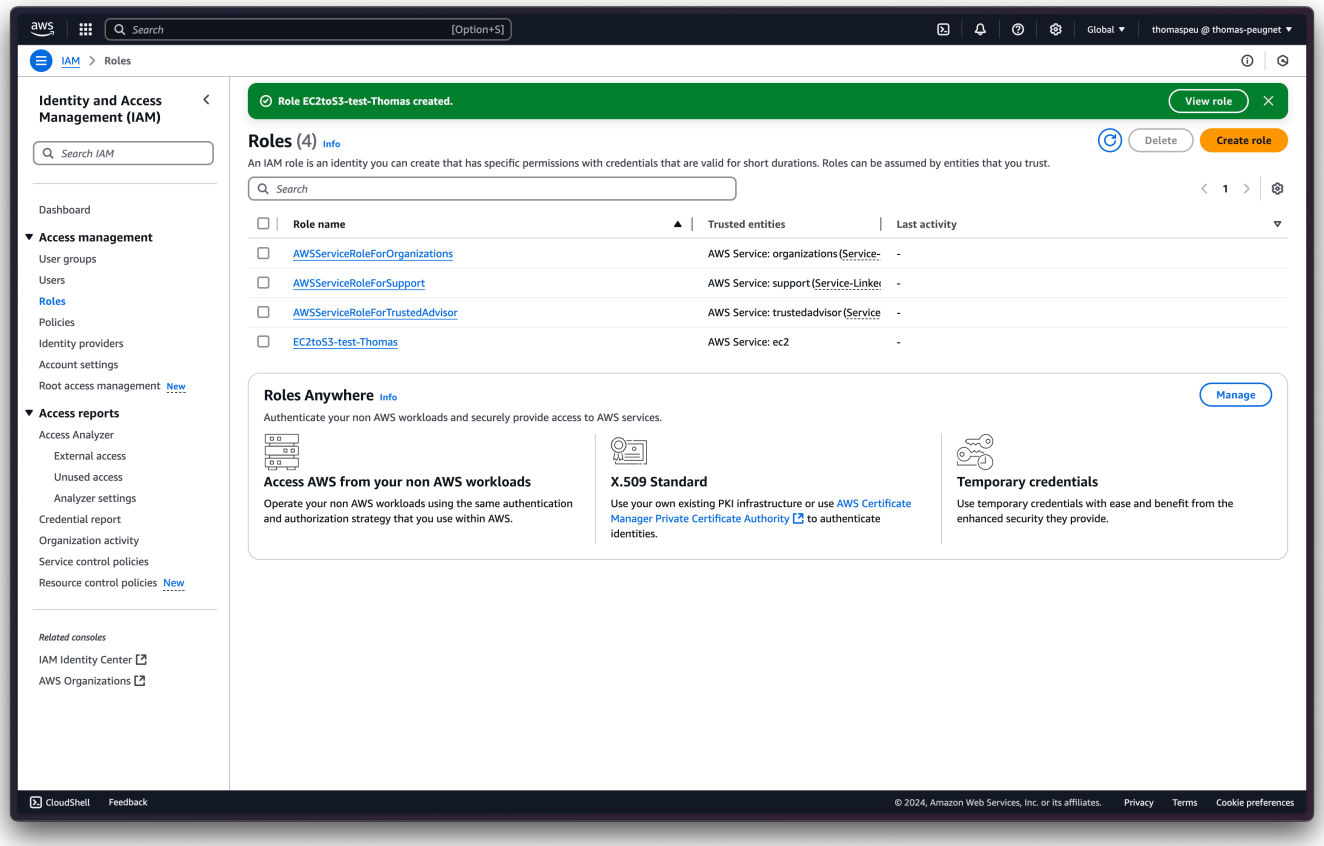
Nous créons notre instance.

Nous nous connectons en SSH à la VM.

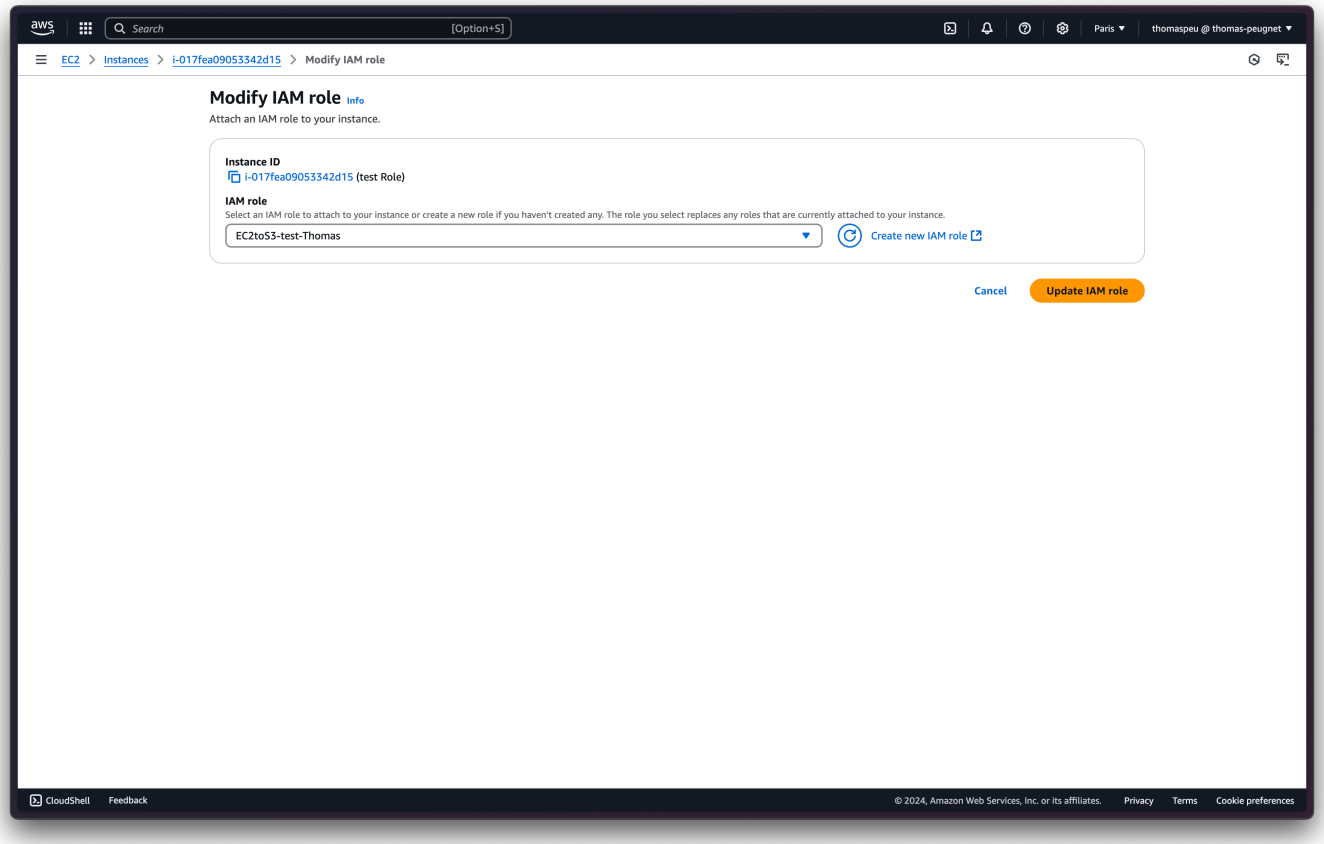
Nous tentons de lister les `s3`.

```
⌥⌘2                    ec2-user@ip-172-31-47-175:~

.amazonaws.com
The authenticity of host 'ec2-15-188-50-217.eu-west-3.compute.amazonaws.com (15
.188.50.217)' can't be established.
ED25519 key fingerprint is SHA256:Ayc9yKc+0w0YHurCONyoH3Z1HGOcLthwMCPbIaIpiTI.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ec2-15-188-50-217.eu-west-3.compute.amazonaws.com'
(ED25519) to the list of known hosts.
   ,     #_
   ~\_  ####_        Amazon Linux 2023
  ~~  \_#####\
  ~~     \###|
  ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
   ~~       V~' '->
    ~~~         /
      ~~._.   _/
         _/ _/
       _/m/'
[ec2-user@ip-172-31-47-175 ~]$ aws s3 ls

Unable to locate credentials. You can configure credentials by running "aws con
figure".
[ec2-user@ip-172-31-47-175 ~]$
```

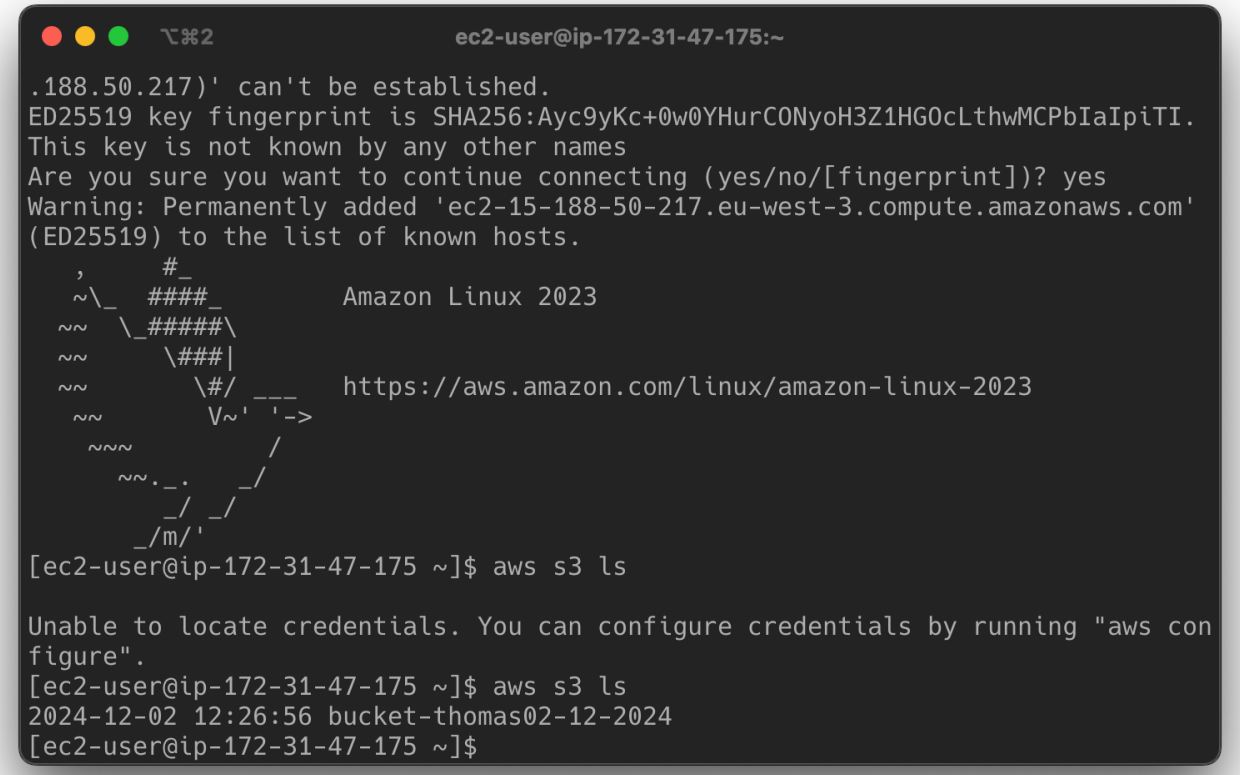
Nous créons notre rôle `EC2toS3-test-Thomas`.



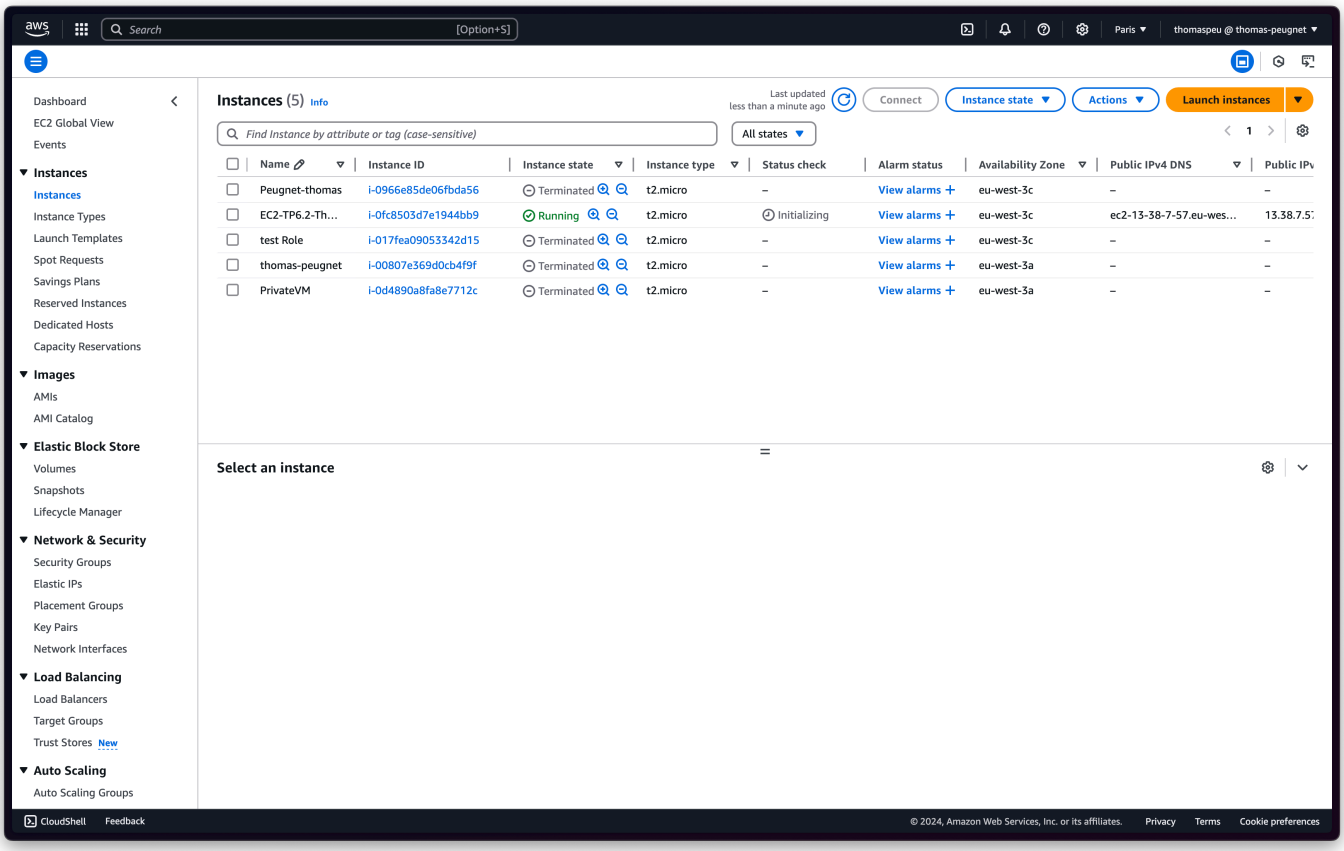
Nous modifions le rôle IAM pour mettre celui nouvellement créé.



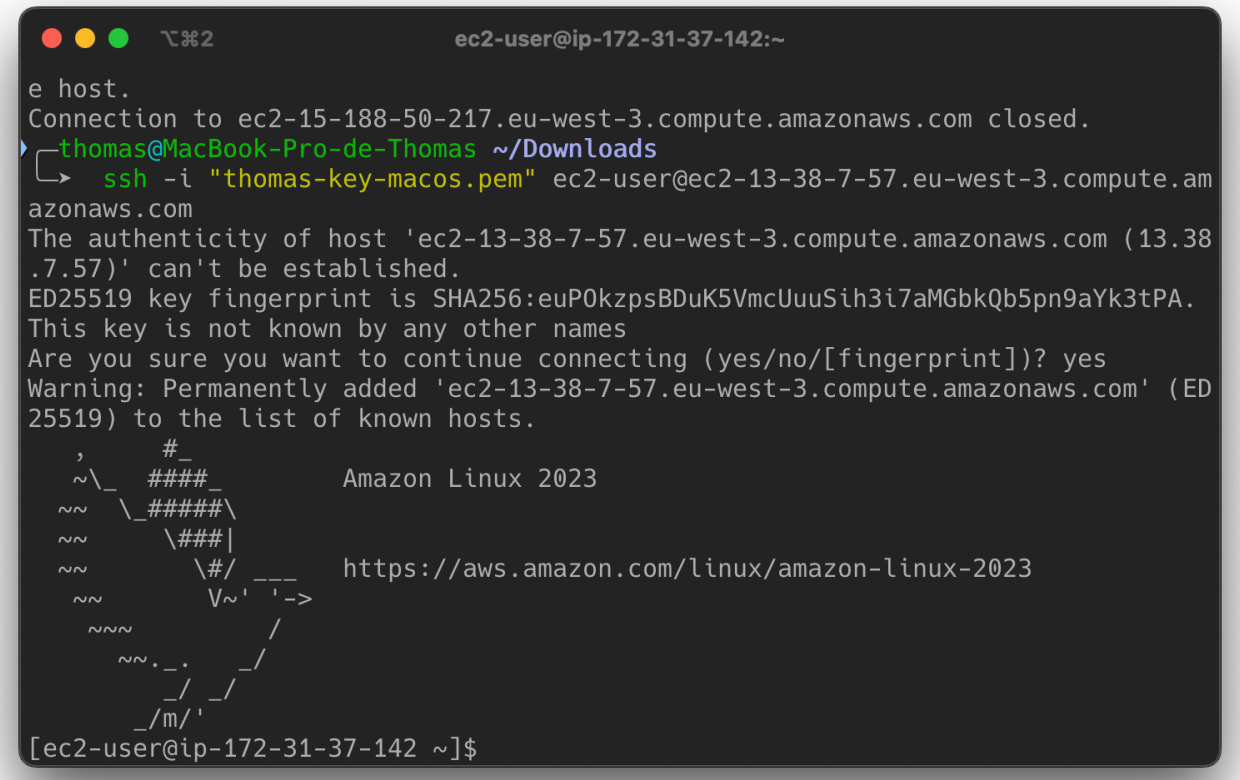
Nous pouvons constater que le `ls` fonctionne désormais.



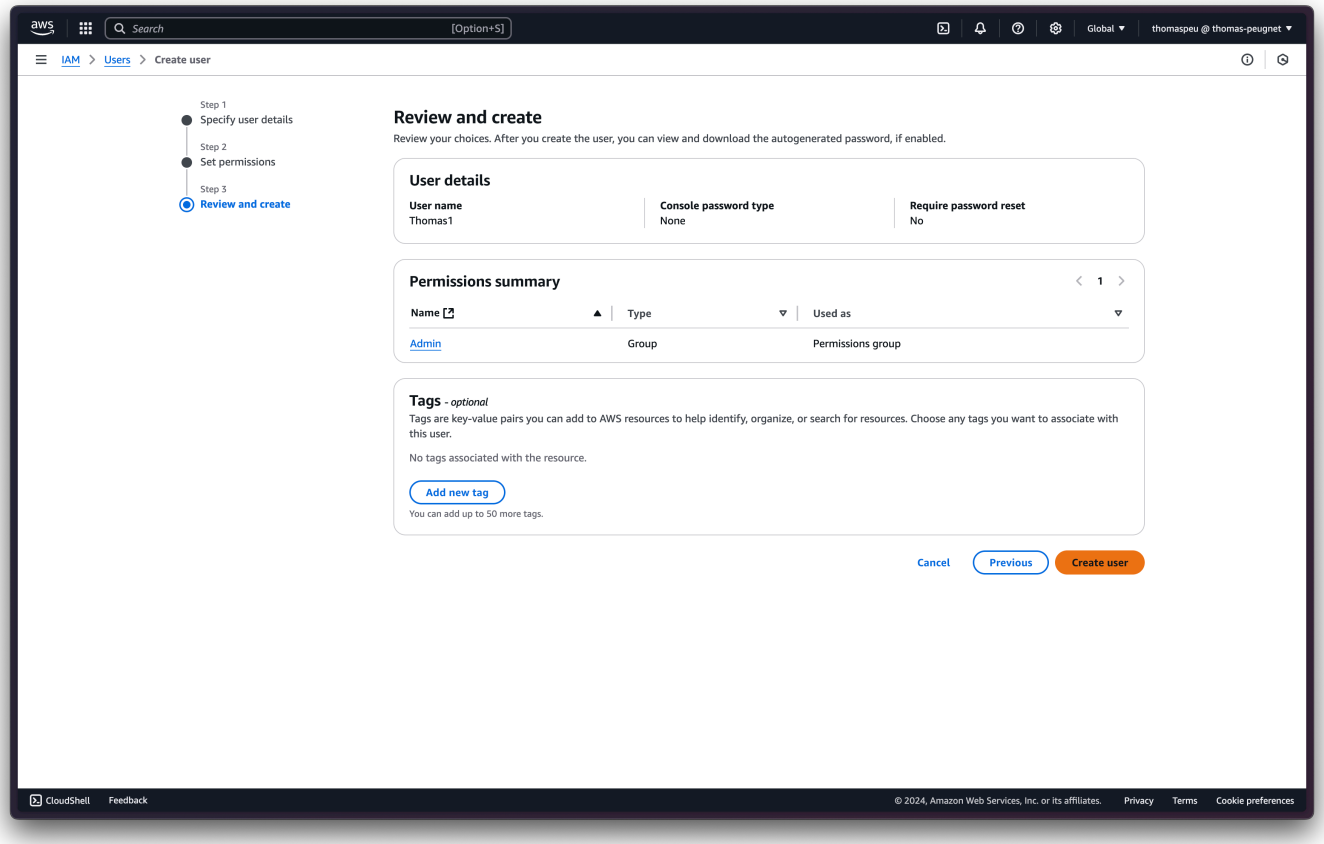
Nous créons une nouvelle instance `EC2-TP6.2-Thomas`.



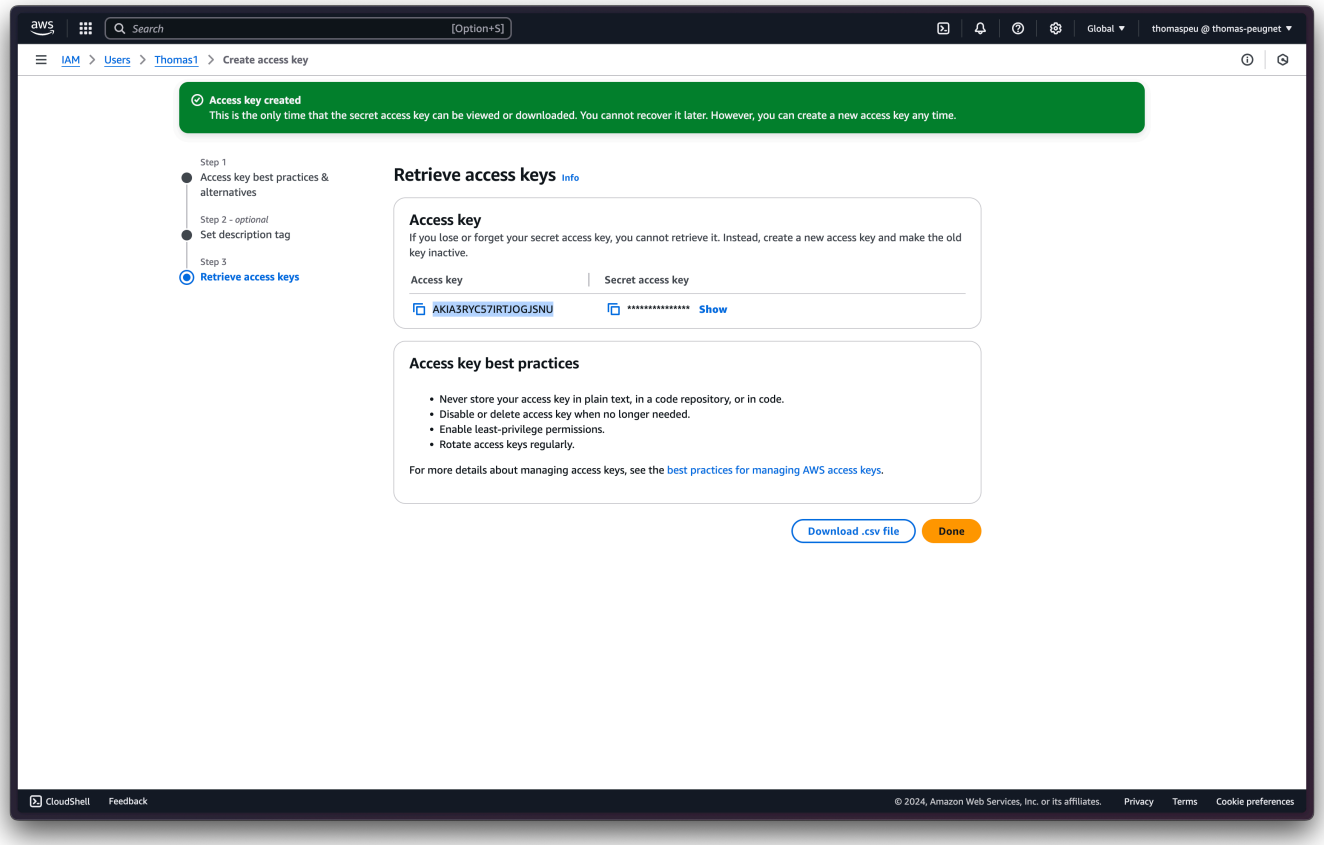
Nous nous connectons à cette nouvelle instance.



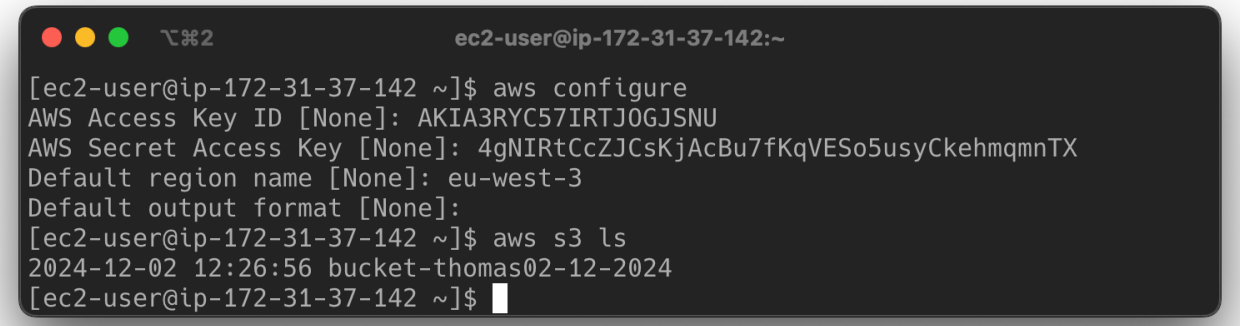
Nous créons un nouvel utilisateur `Thomas1`.



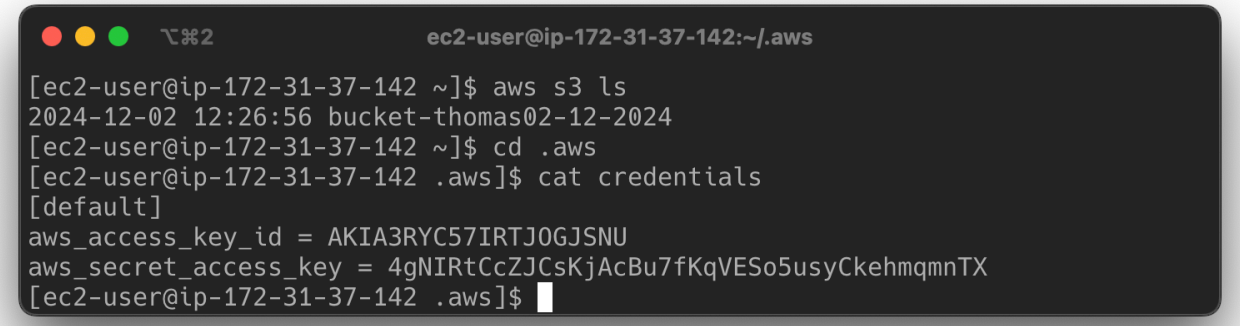
Nous créons une access key pour notre utilisateur.



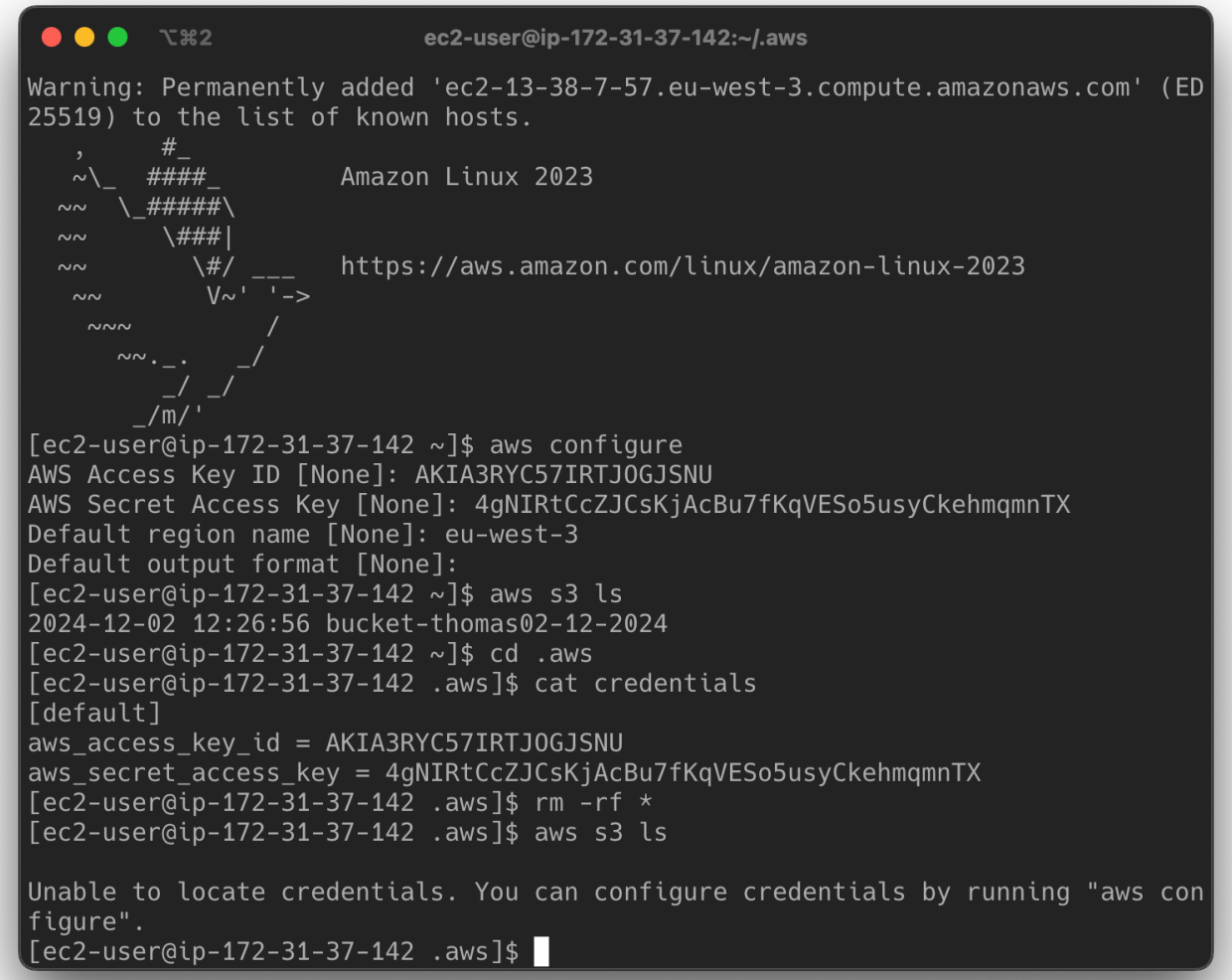
Après avoir enregistré nos Access Keys (détruites avant publication de ce TP donc visibles en clair sur les captures.) nous constatons que cela fonctionne.



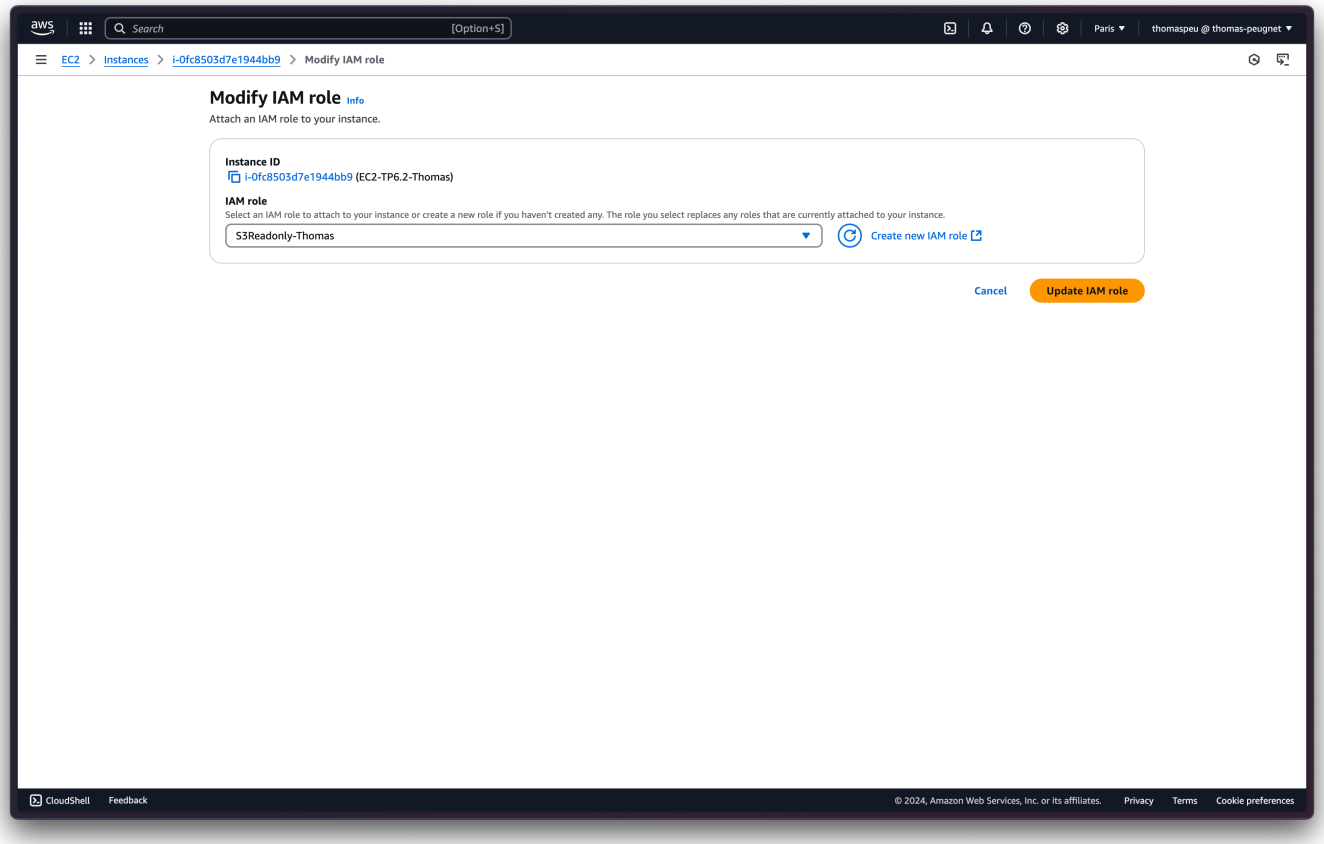
Nous constatons également que ces informations sont stockées en clair sur la VM.



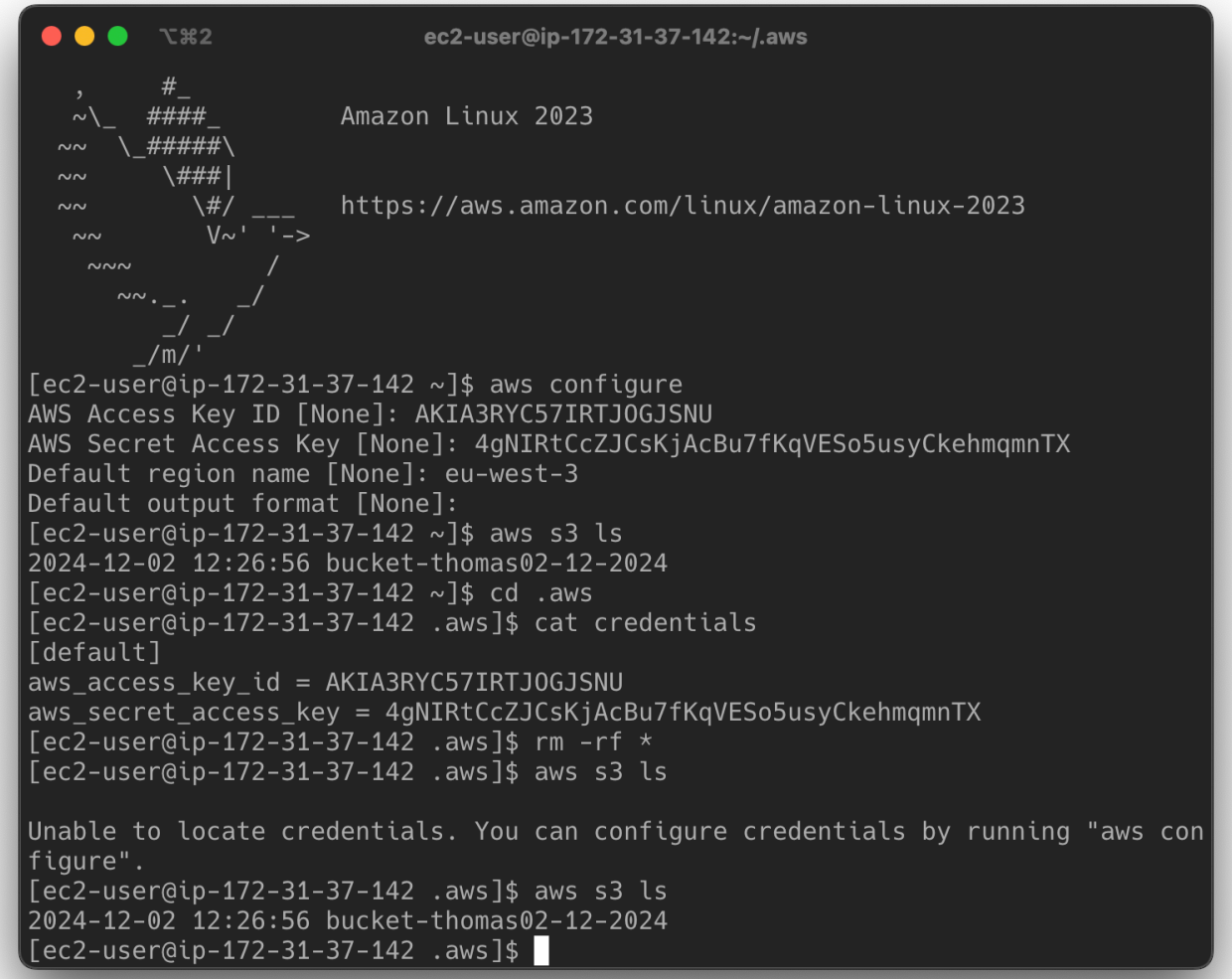
Nous supprimons ce fichier.



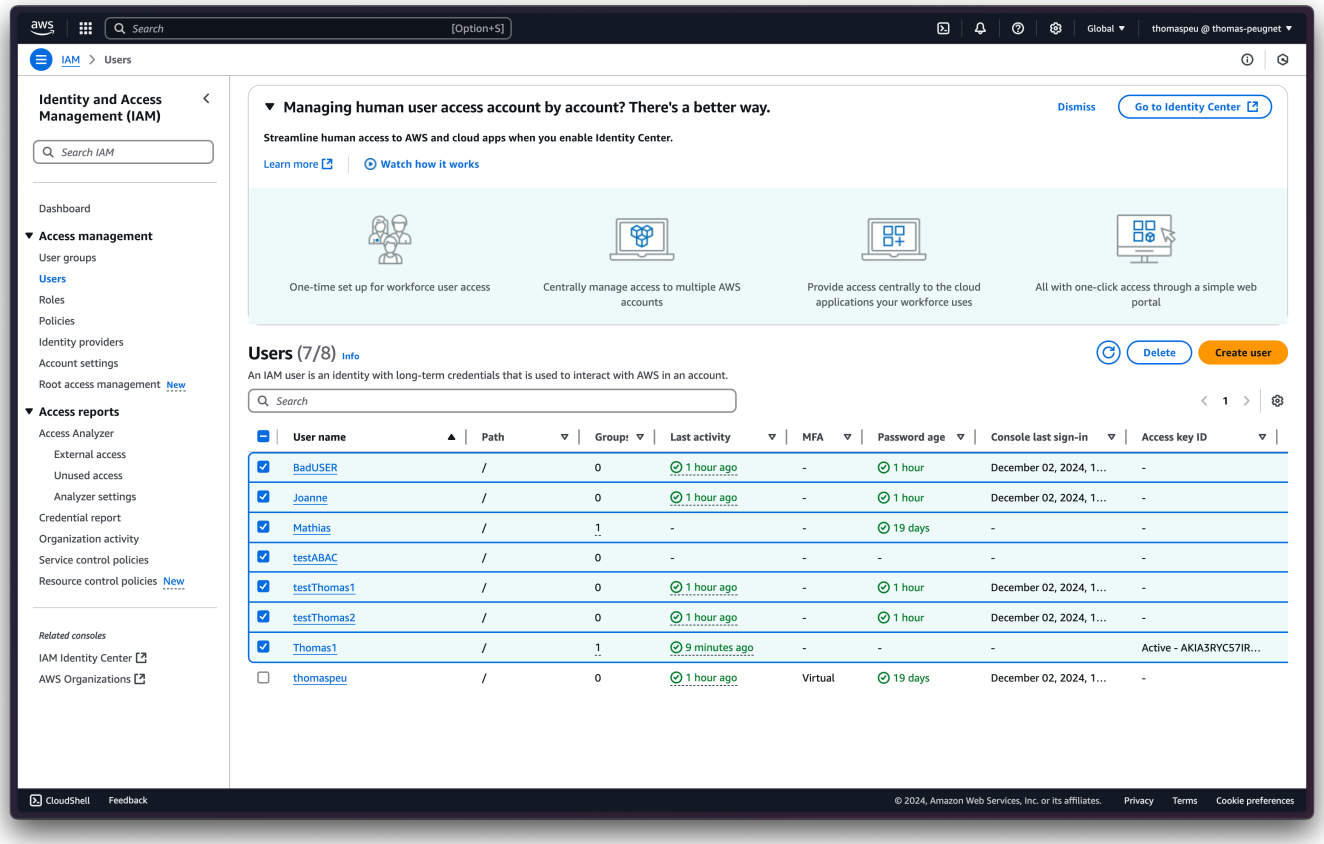
Nous modifions le role IAM.



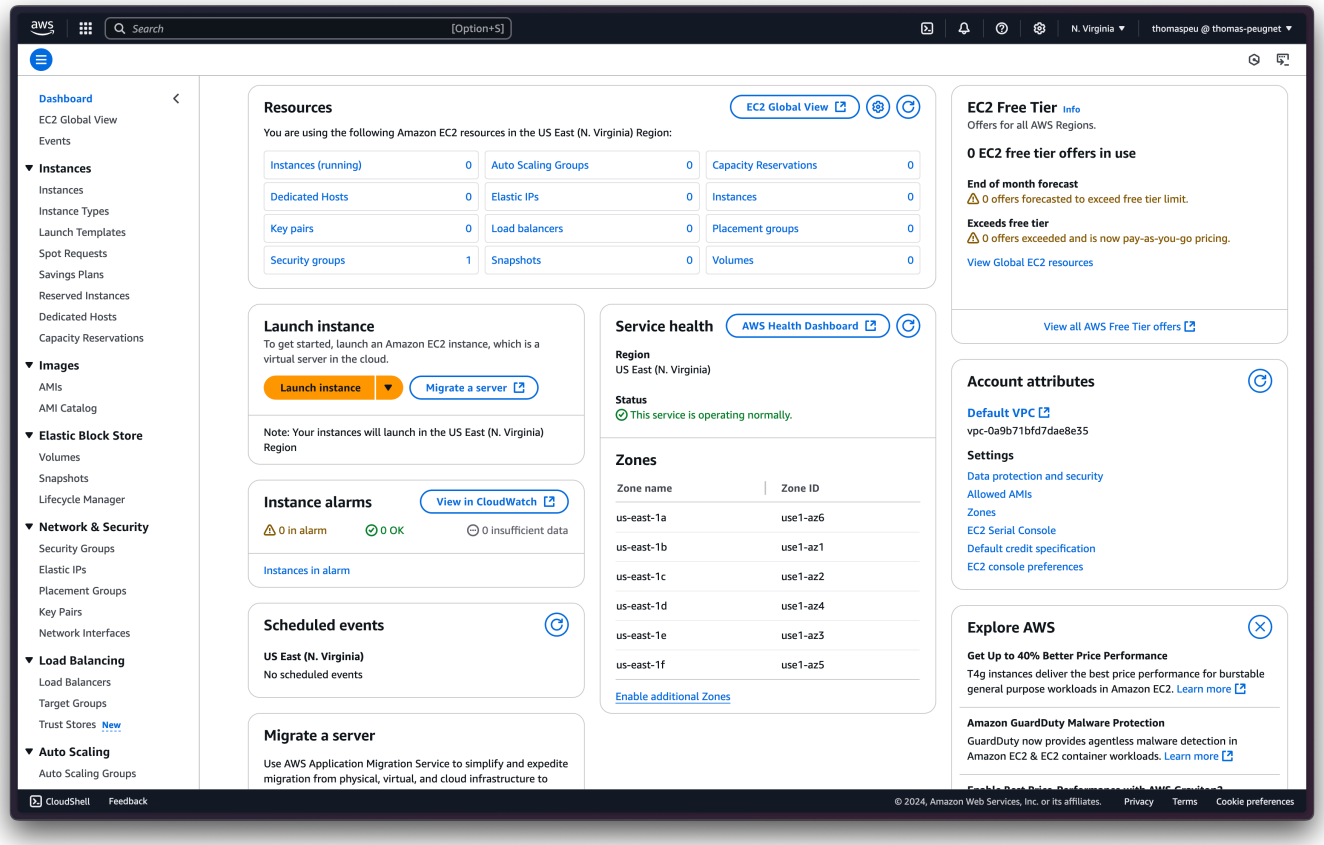
Nous pouvons voir le résultat suivant.



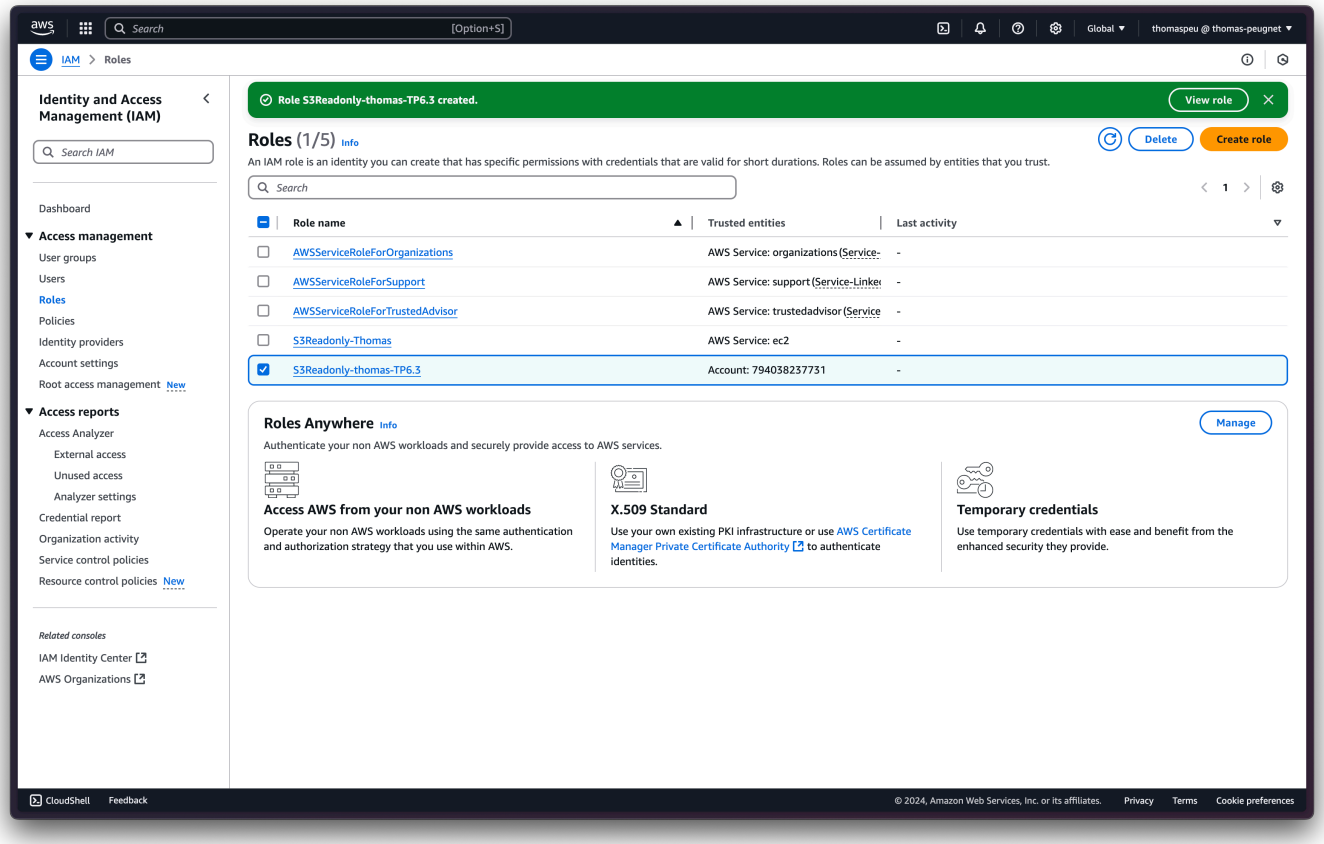
Nous supprimons tous les éléments du TP.



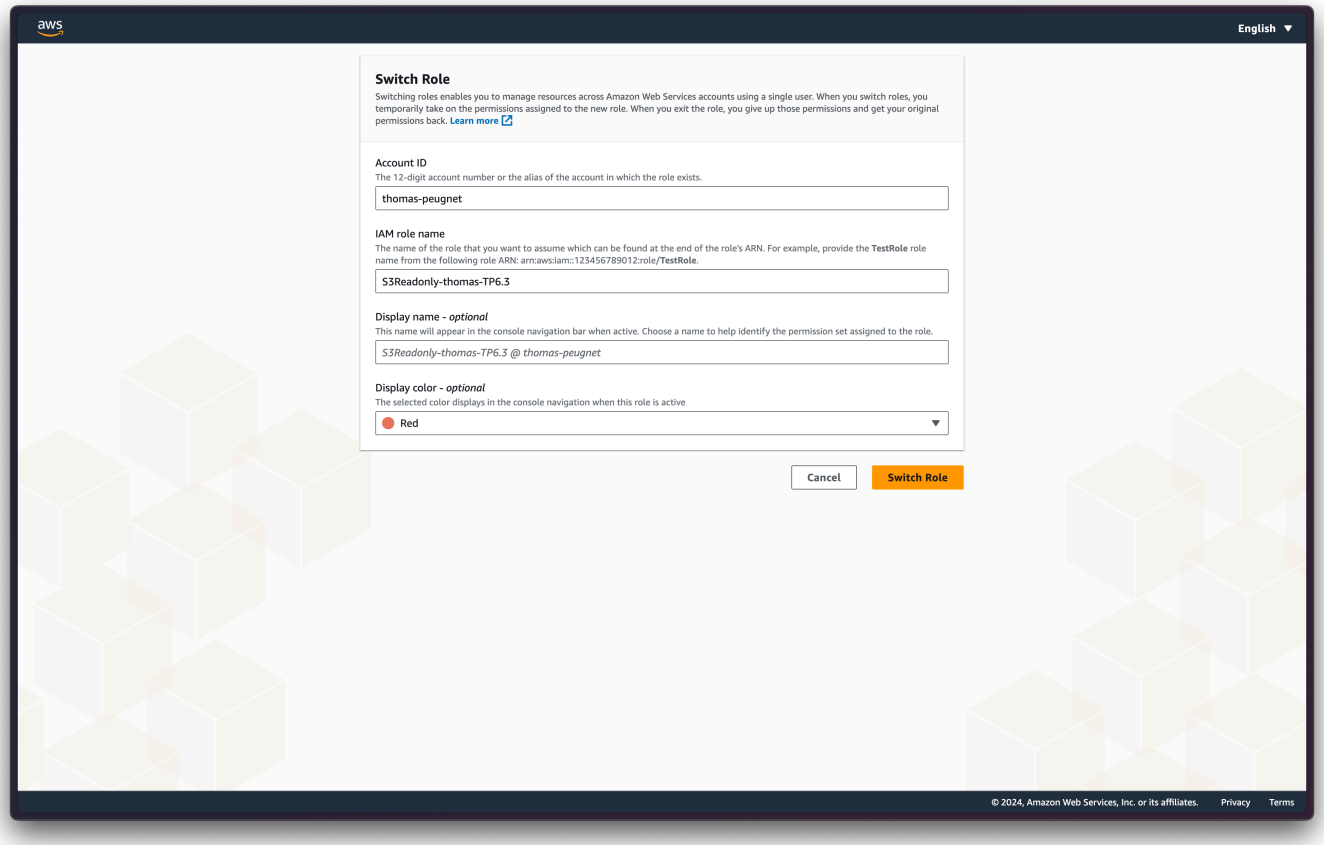
Nous nous connectons au service EC2.



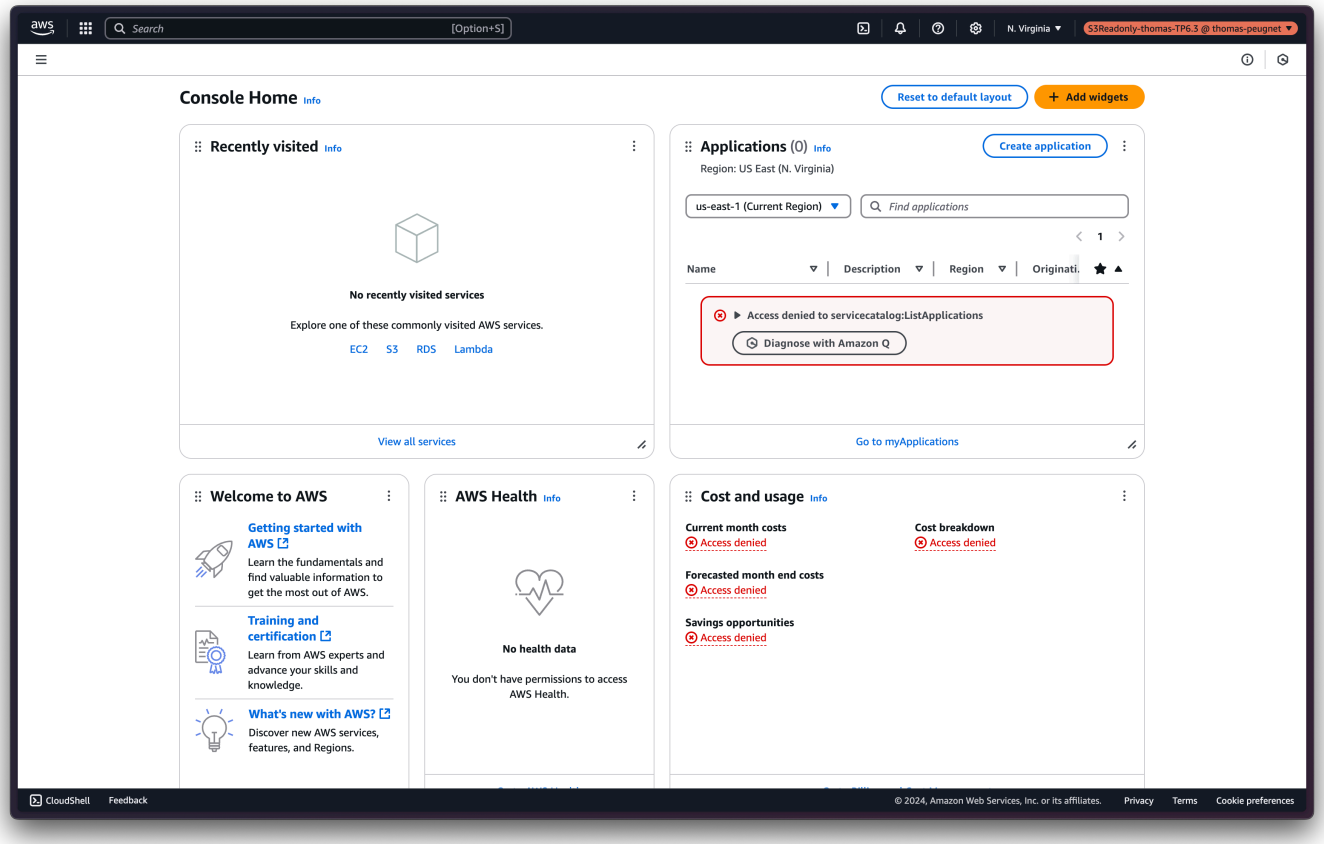
Nous créons noétre nouveau rôle.



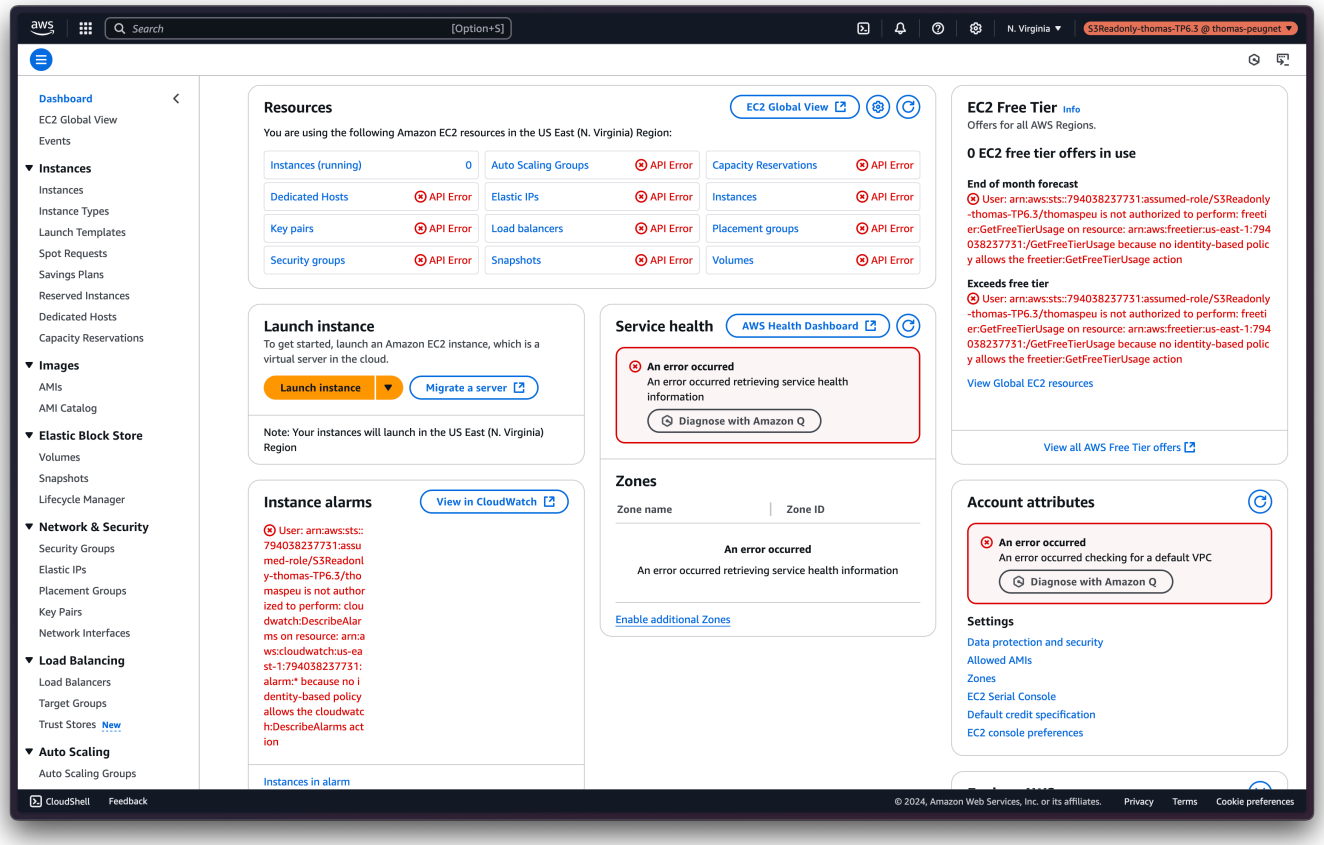
Nous faisons le switch du role.



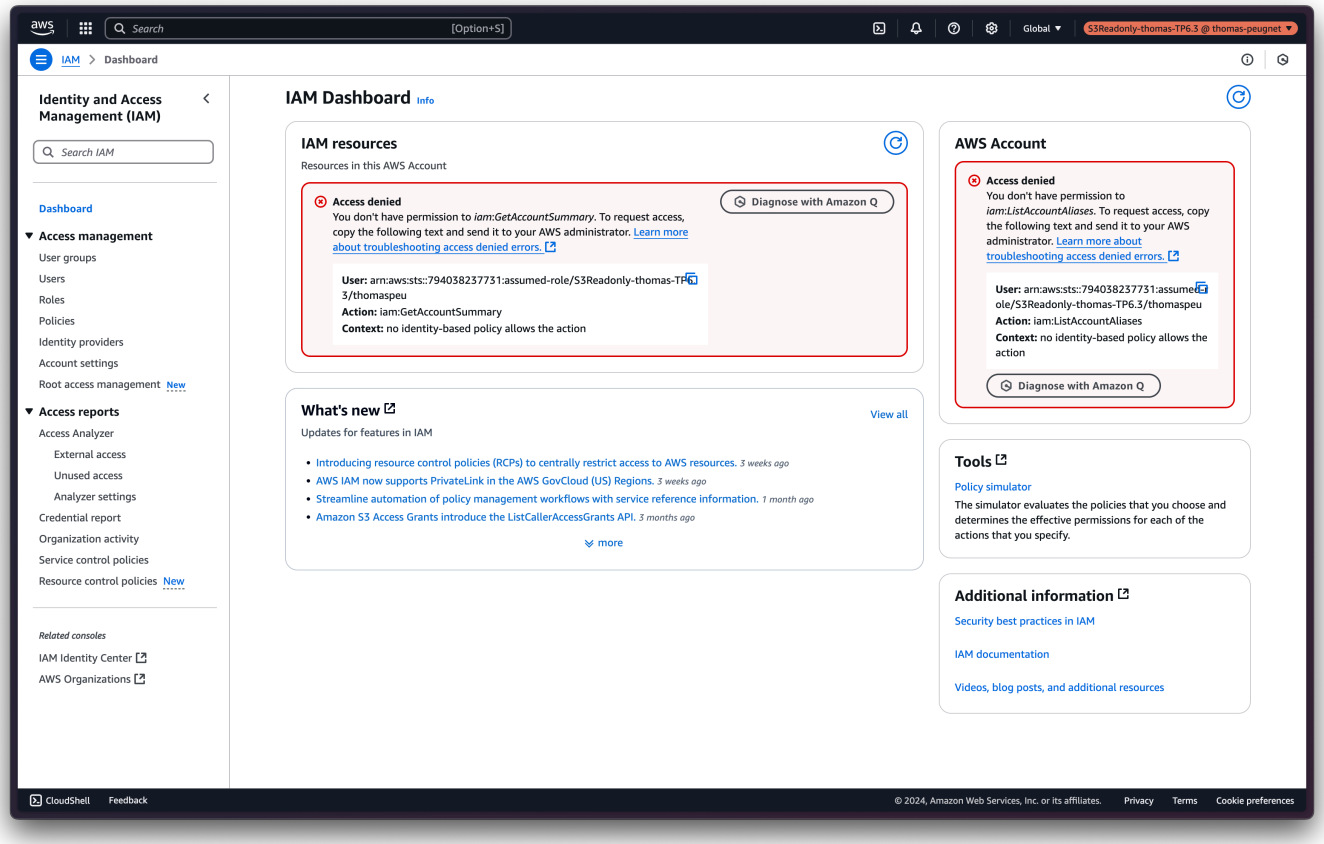
Nous avons bien le résultat suivant.



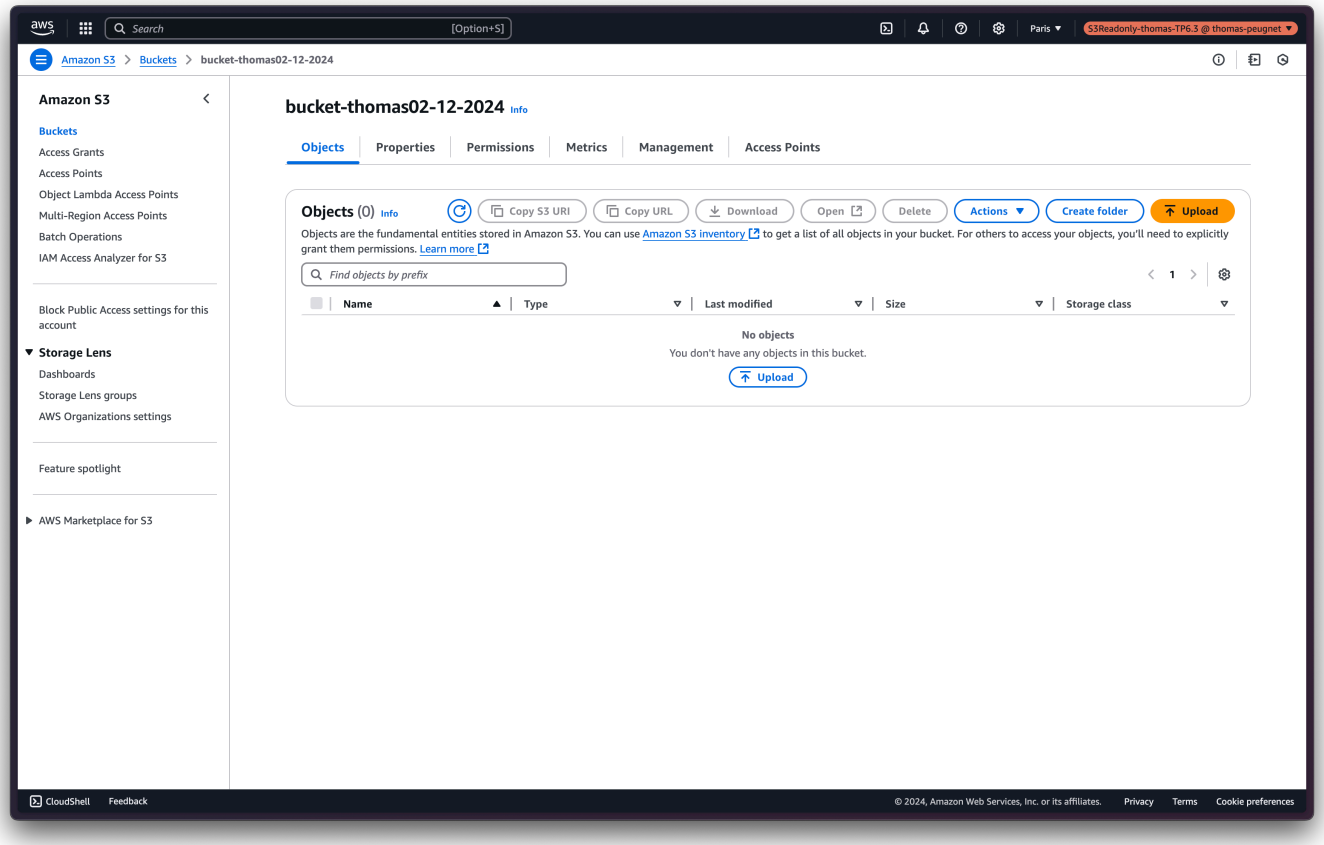
Nous n'avons pas d'accès au service EC2.



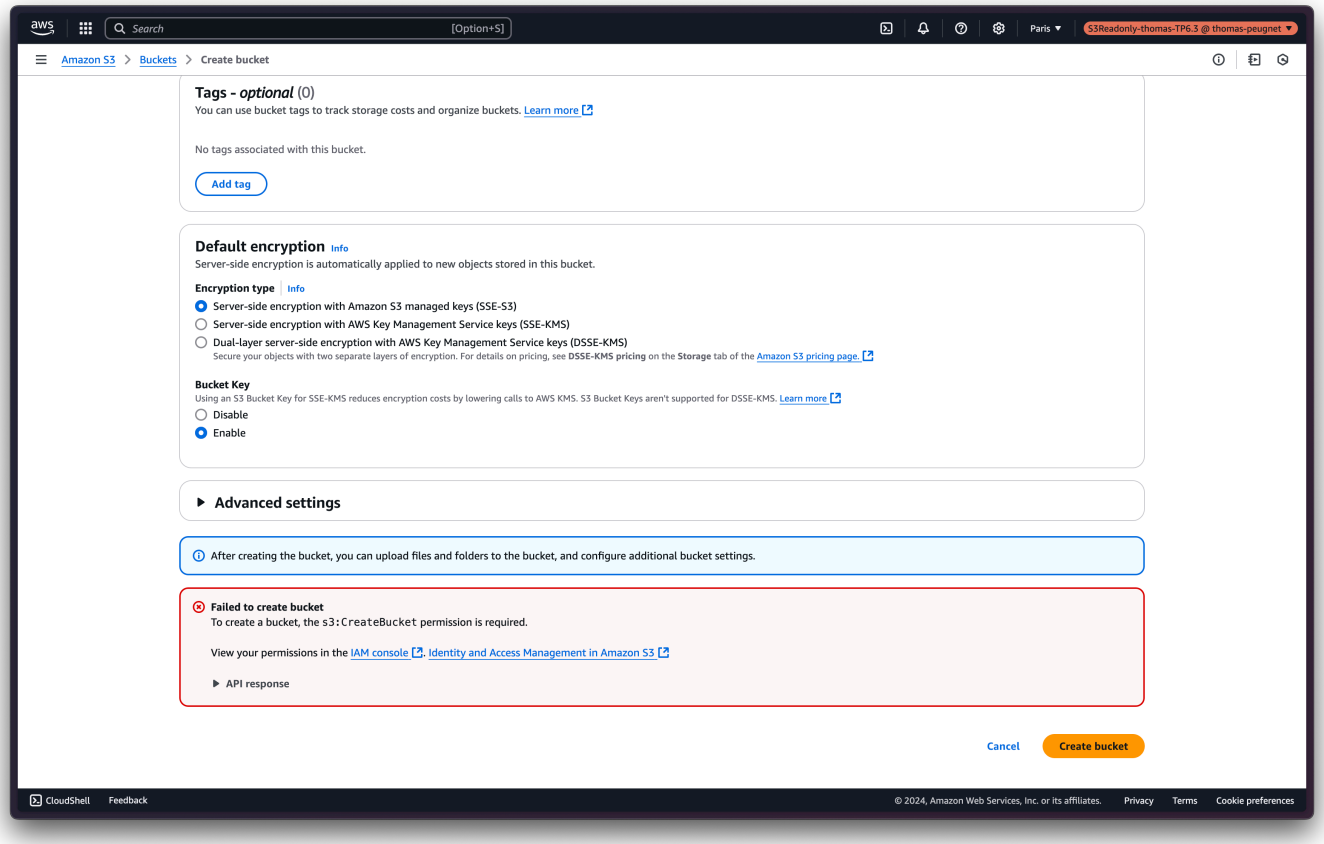
Idem pour le service IAM.



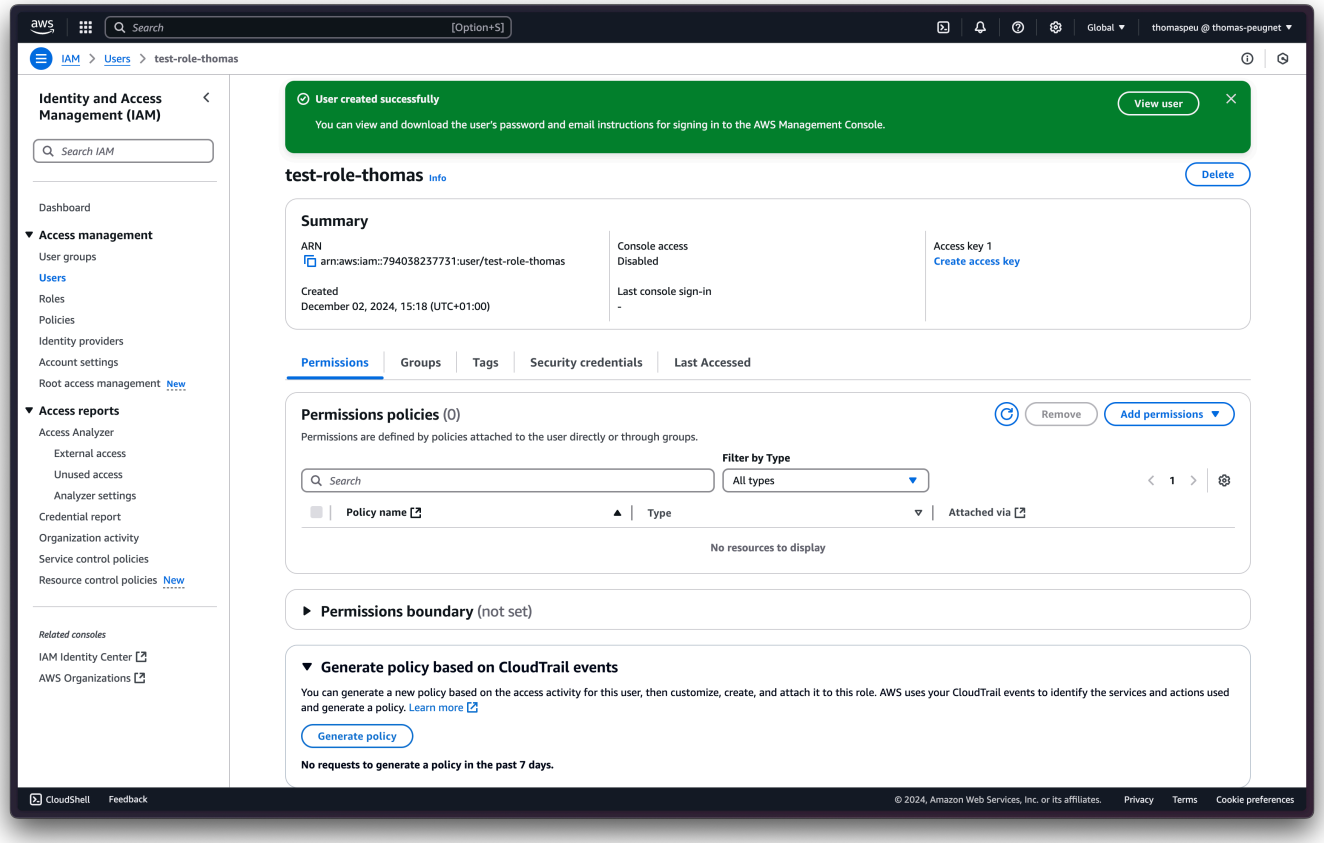
Pas de problème pour la lecture sur S3.



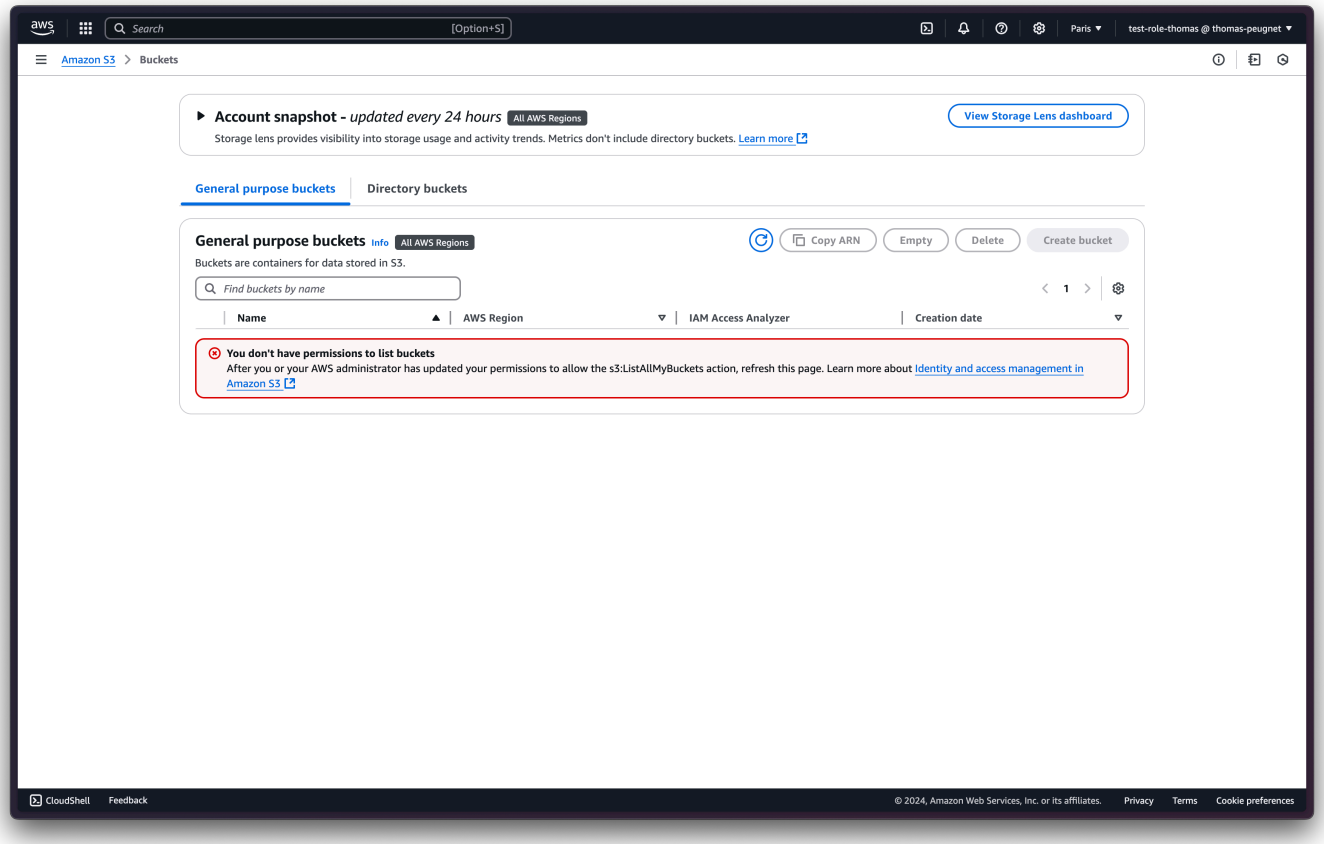
Nous ne pouvons pas créer de bucket.



Nous créons éun nouvel utilisateur `test-role-thomas`.



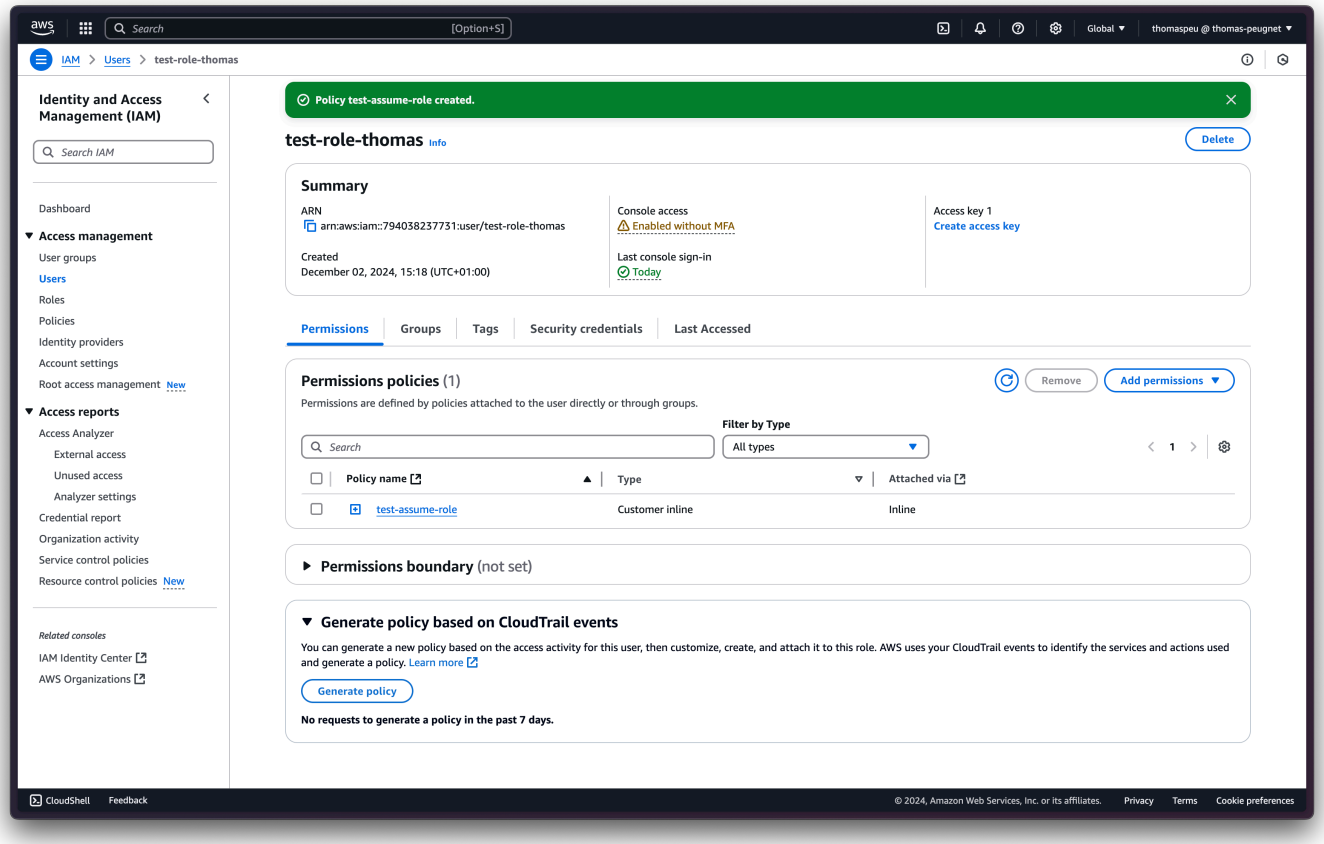
Nous n'avons pas accès au service S3.



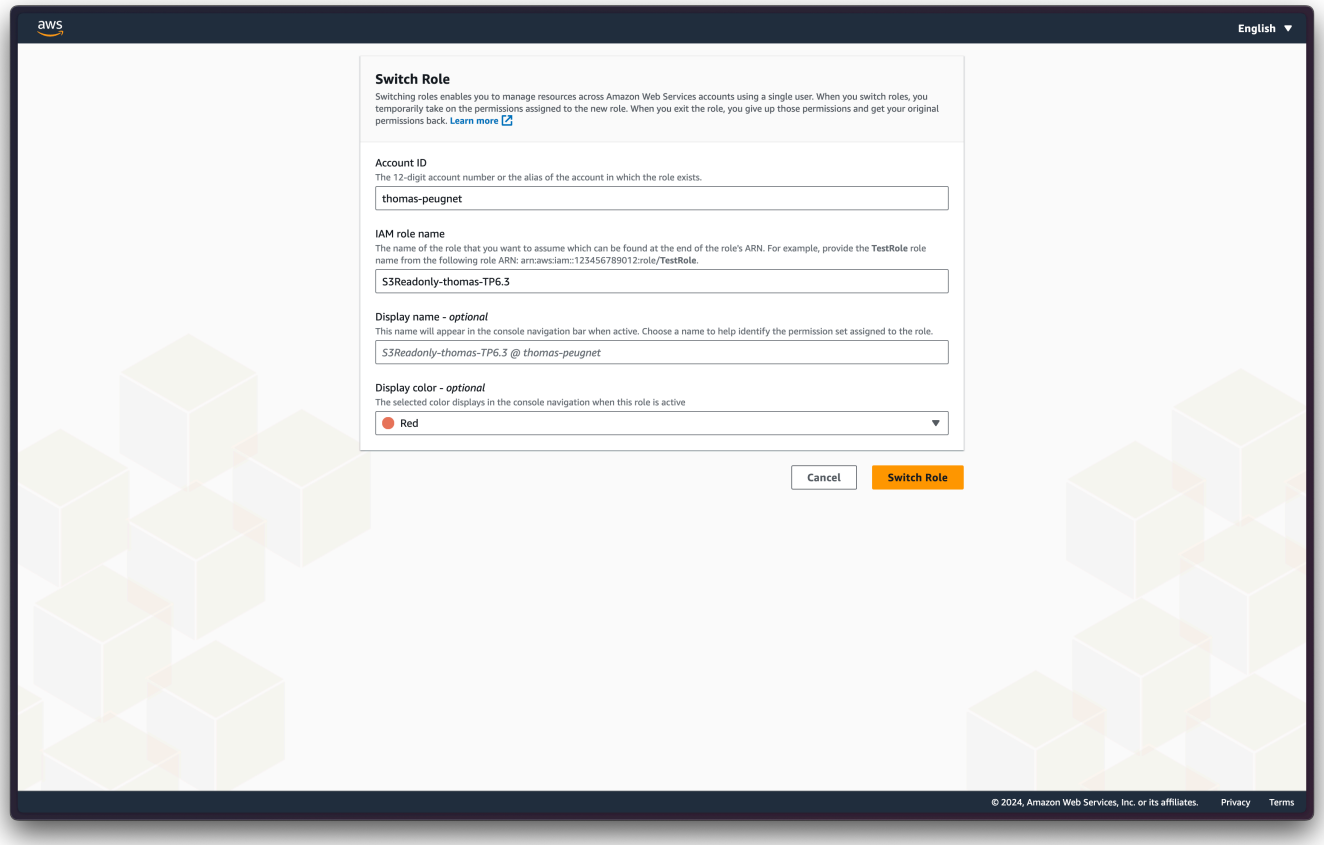
Nous créons la policy suivante.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "Statement1",
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": : "arn:aws:iam::794038237731:role/S3Readonly-thomas-TP6.3"
    }
  ]
}
```

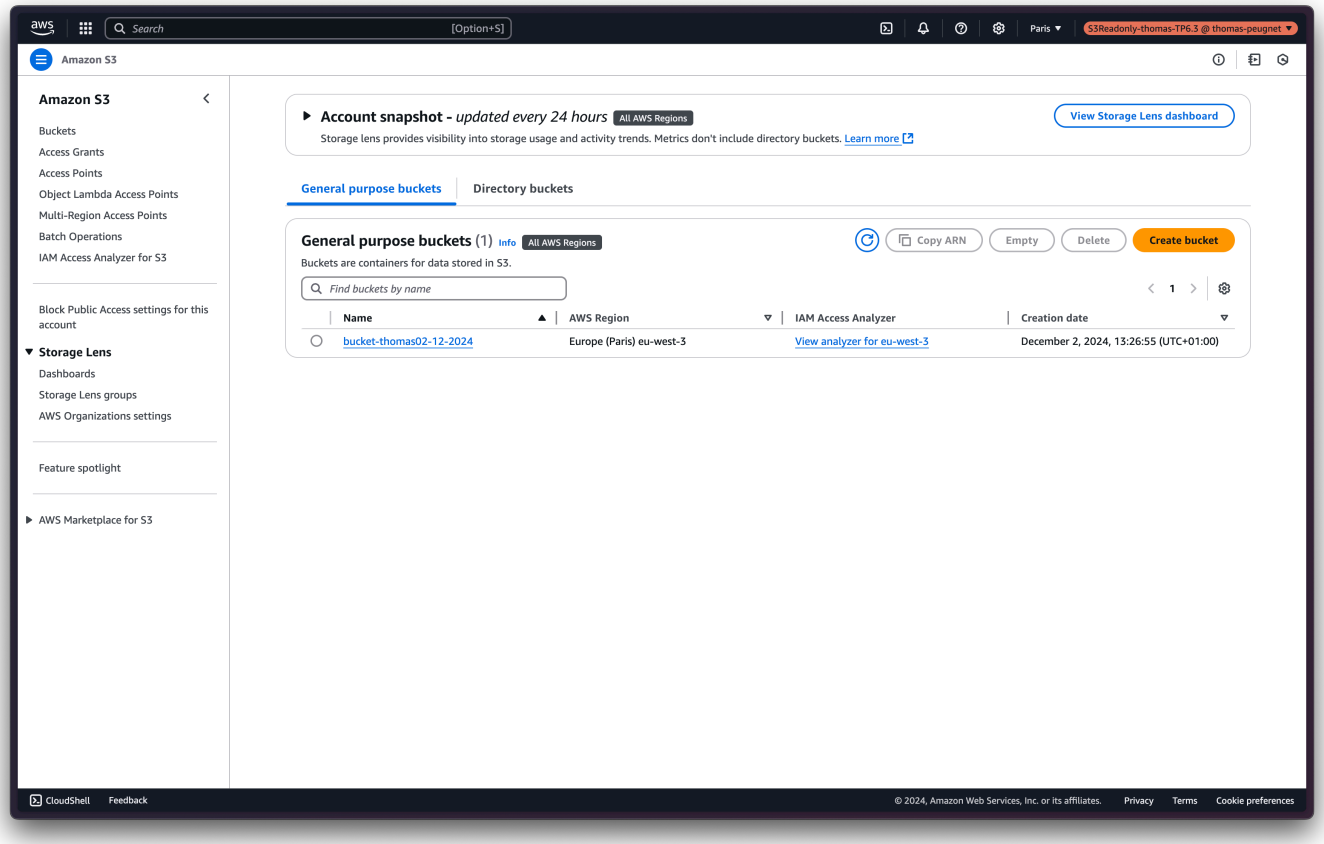
Nous créons la nouvelle policy.



Nous switchons de rôle.



Nous avons bien un accès en lecture seule.


Search
[Option+S]
Paris
S3Readonly-thomas-TP6.3 @ thomas-peugnet
Amazon S3
Amazon S3
Buckets
Access Grants
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
IAM Access Analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
Storage Lens groups
AWS Organizations settings
Feature spotlight
AWS Marketplace for S3
Account snapshot - updated every 24 hours
All AWS Regions
Storage lens provides visibility into storage usage and activity trends. Metrics don't include directory buckets. Learn more
View Storage Lens dashboard
General purpose buckets
Directory buckets
General purpose buckets (1) Info
All AWS Regions
Buckets are containers for data stored in S3.
Copy ARN
Empty
Delete
Create bucket
Find buckets by name
1
Name
AWS Region
IAM Access Analyzer
Creation date
bucket-thomas02-12-2024
Europe (Paris) eu-west-3
View analyzer for eu-west-3
December 2, 2024, 13:26:55 (UTC+01:00)
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences