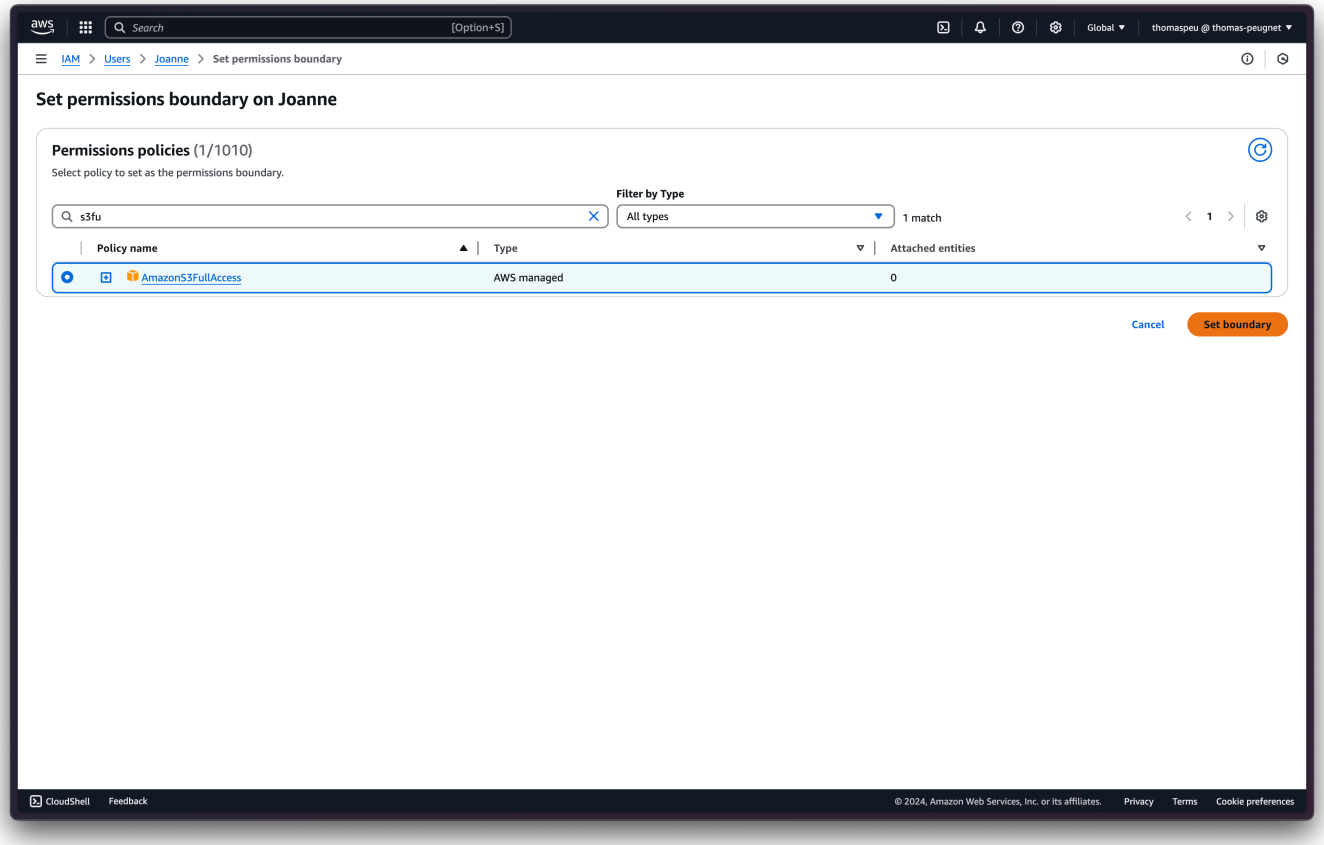
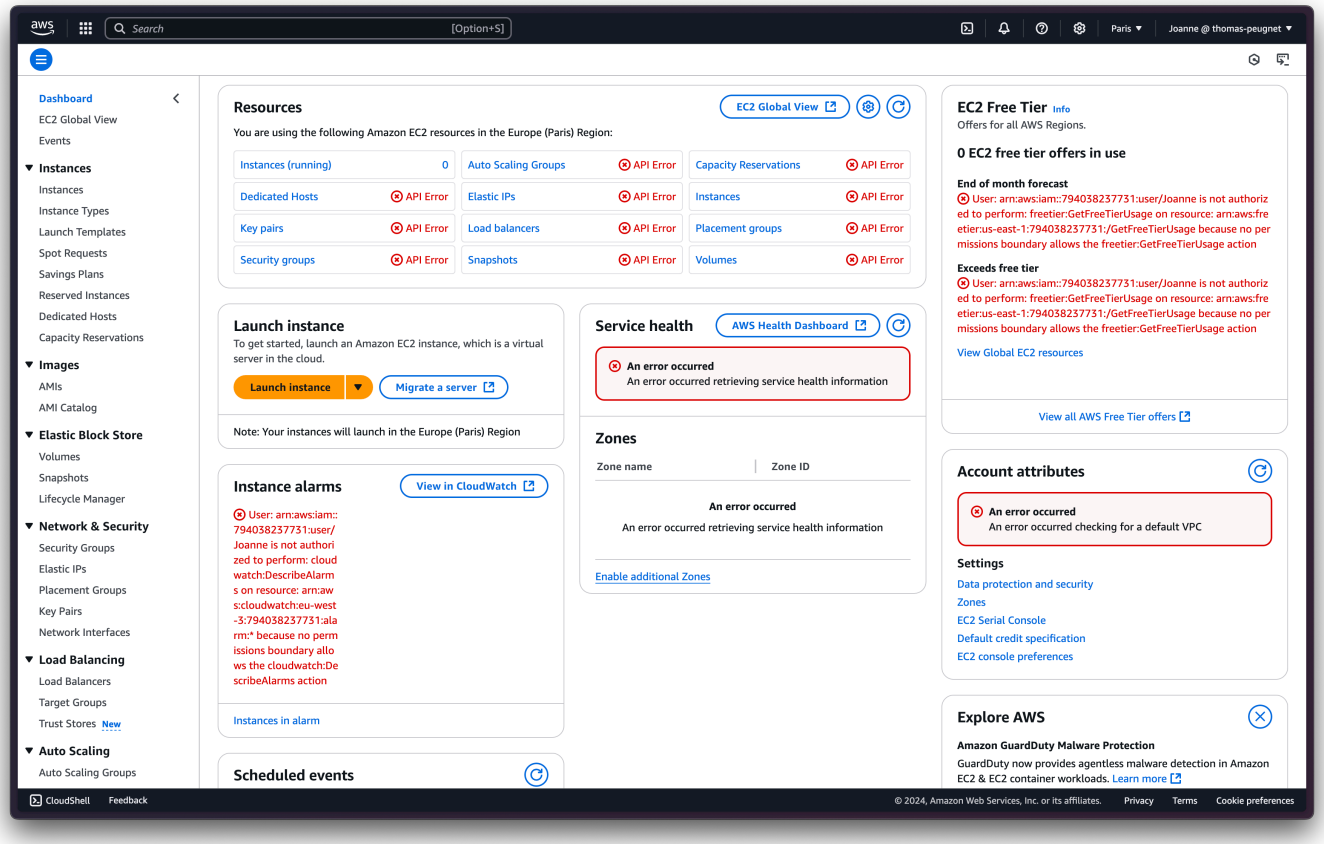
Rendu TP03

Rendu du TP03 effectué par `Thomas PEUGNET`.

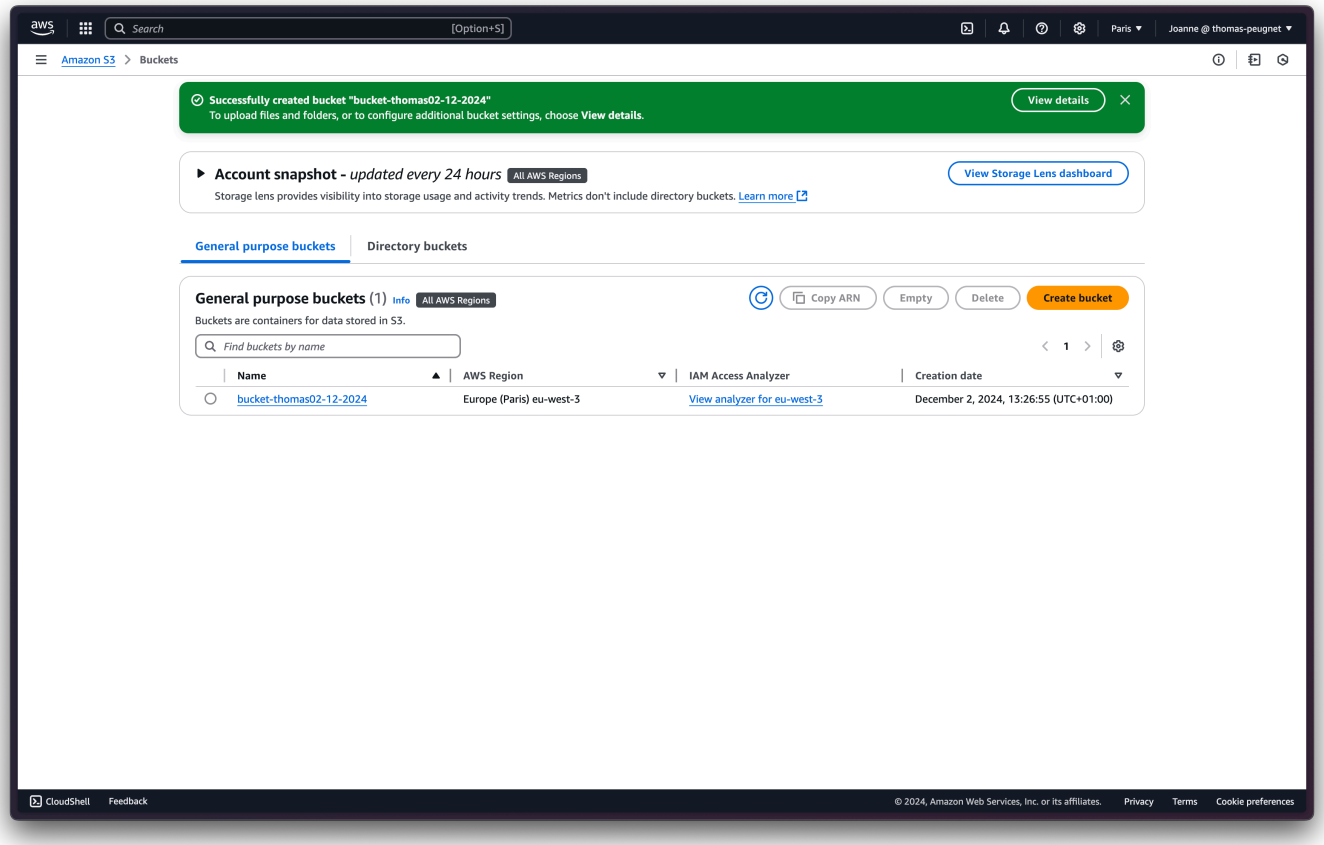
Nous créons l'utilisateur Joanne.



Nous nous reconnectons avec `Joanne` et constatons le résultat suivant:



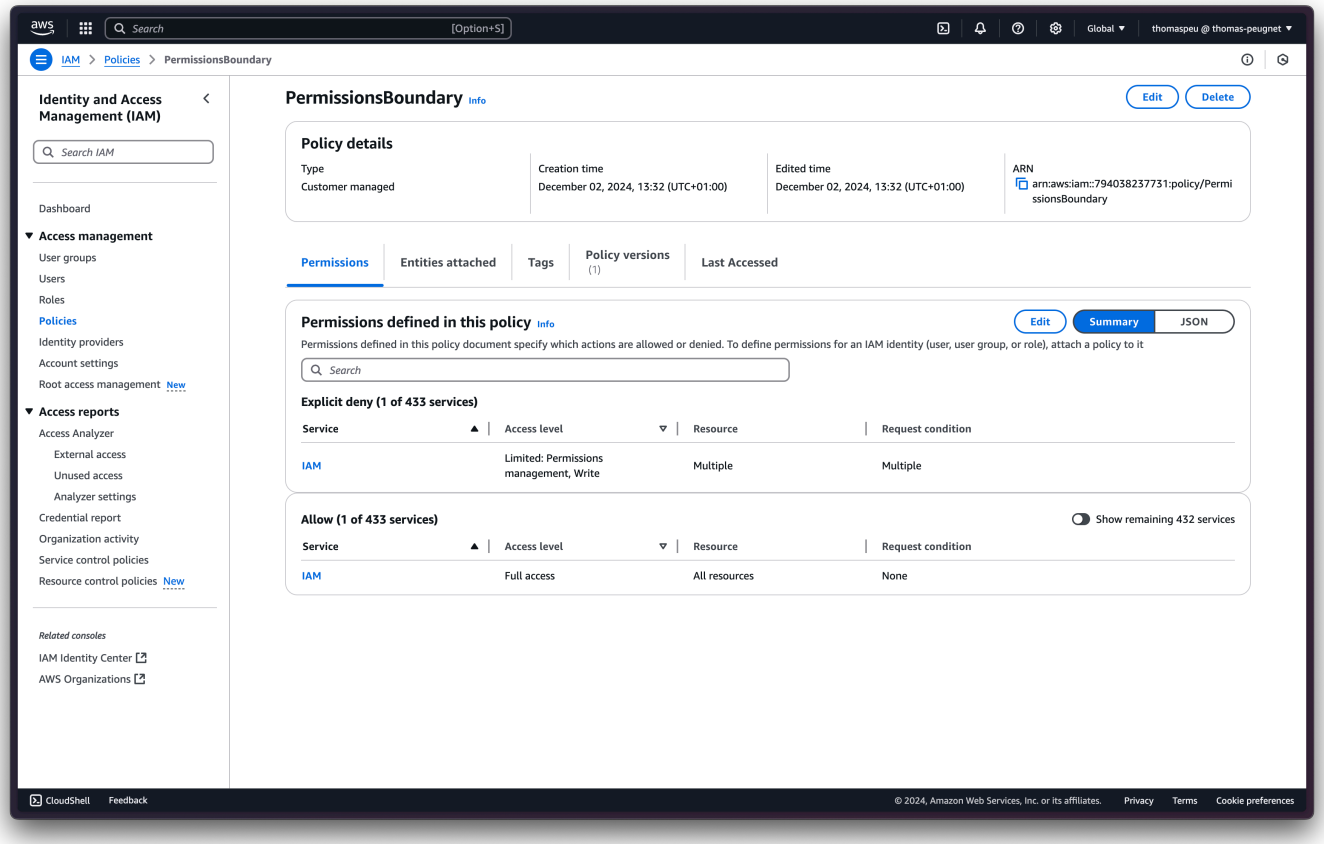
Nous créons un bucket S3.



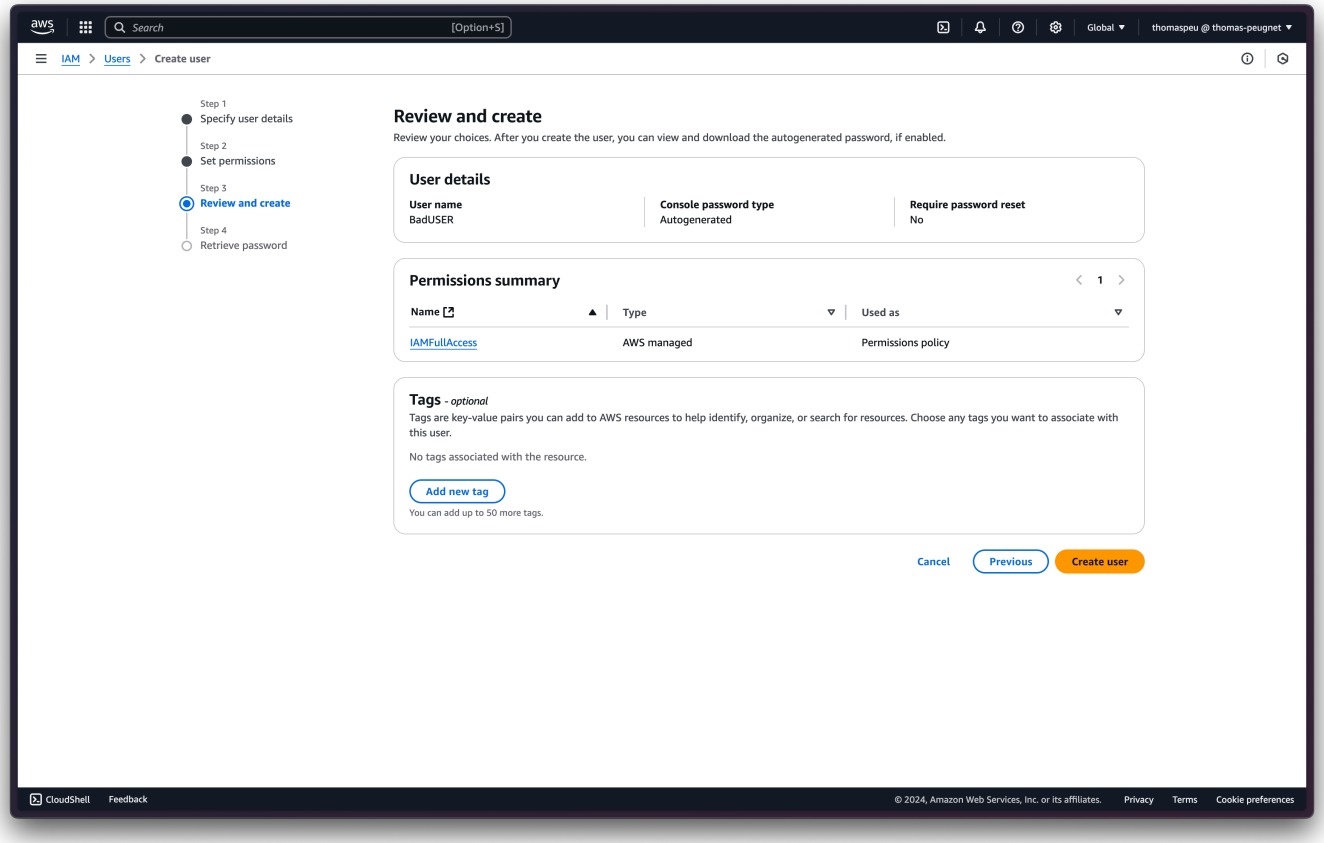
Nous créons la policy avec le contenu suivant.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "IAMAccess",
            "Effect": "Allow",
            "Action": "iam:*",
            "Resource": "*"
        },
        {
            "Sid": "DenyPermBoundaryIAMPolicyAlteration",
            "Effect": "Deny",
            "Action": [
                "iam:DeletePolicy",
                "iam:DeletePolicyVersion",
                "iam:CreatePolicyVersion",
                "iam:SetDefaultPolicyVersion"
            ],
            "Resource": [
                "arn:aws:iam::794038237731:policy/PermissionsBoundary"
            ]
        },
        {
            "Sid": "DenyRemovalOfPermBoundaryFromAnyUserOrRole",
            "Effect": "Deny",
            "Action": [
                "iam:DeleteUserPermissionsBoundary",
                "iam:DeleteRolePermissionsBoundary"
            ],
            "Resource": [
                "arn:aws:iam::794038237731:user/*",
                "arn:aws:iam::794038237731:role/*"
            ],
            "Condition": {
                "StringEquals": {
                    "iam:PermissionsBoundary":
"arn:aws:iam::794038237731:policy/PermissionsBoundary"
                }
            }
        },
        {
            "Sid": "DenyAccessIfRequiredPermBoundaryIsNotBeingApplied",
            "Effect": "Deny",
            "Action": [
                "iam:PutUserPermissionsBoundary",
                "iam:PutRolePermissionsBoundary"
            ],
            "Resource": [
                "arn:aws:iam::794038237731:user/*",
```

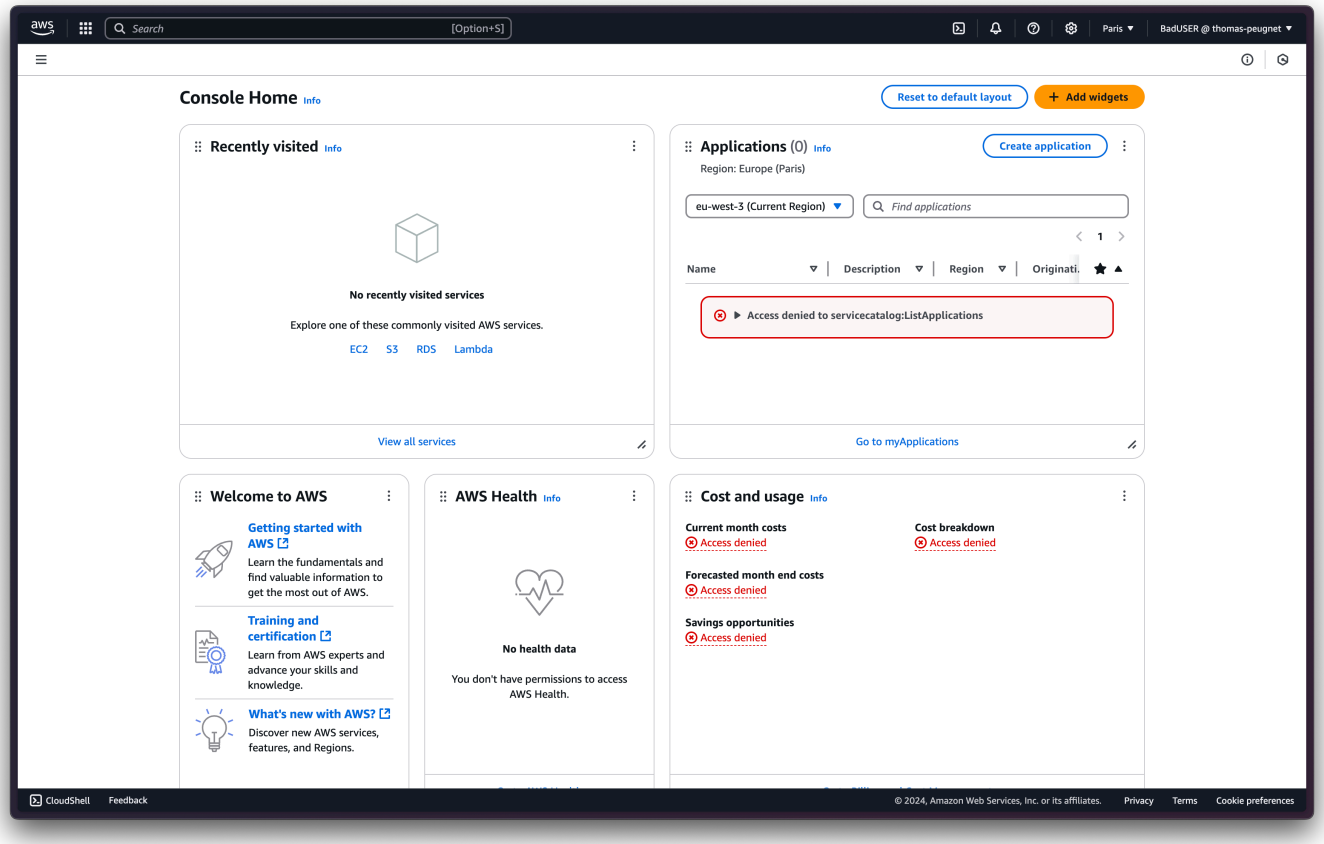
```
                "arn:aws:iam::794038237731:role/*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "iam:PermissionsBoundary":
"arn:aws:iam::794038237731:policy/PermissionsBoundary"
                }
            }
        },
        {
            "Sid": "DenyUserAndRoleCreationWithOutPermBoundary",
            "Effect": "Deny",
            "Action": [
                "iam:CreateUser",
                "iam:CreateRole"
            ],
            "Resource": [
                "arn:aws:iam::794038237731:user/*",
                "arn:aws:iam::794038237731:role/*"
            ],
            "Condition": {
                "StringNotEquals": {
                    "iam:PermissionsBoundary":
"arn:aws:iam::794038237731:policy/PermissionsBoundary"
                }
            }
        }
    ]
}
```

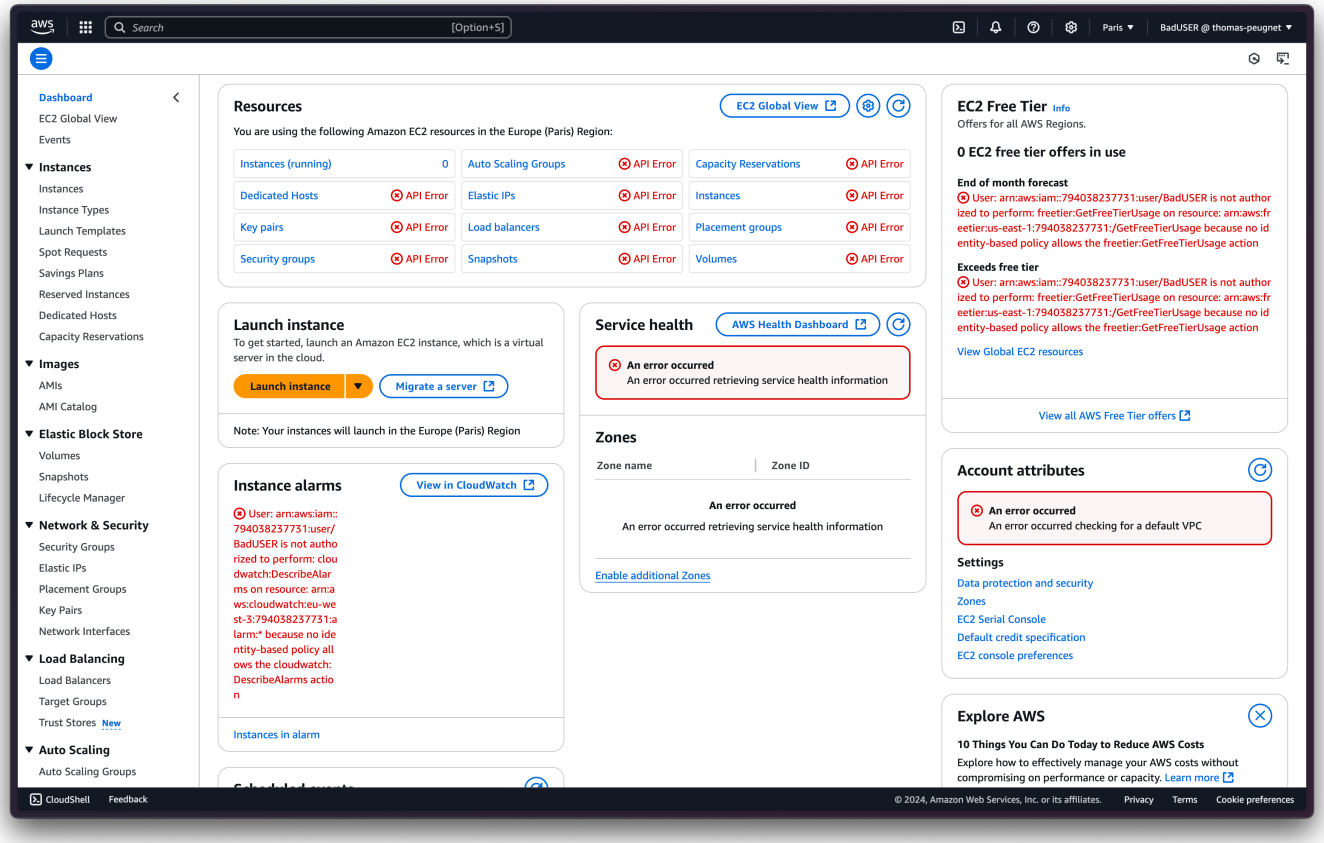


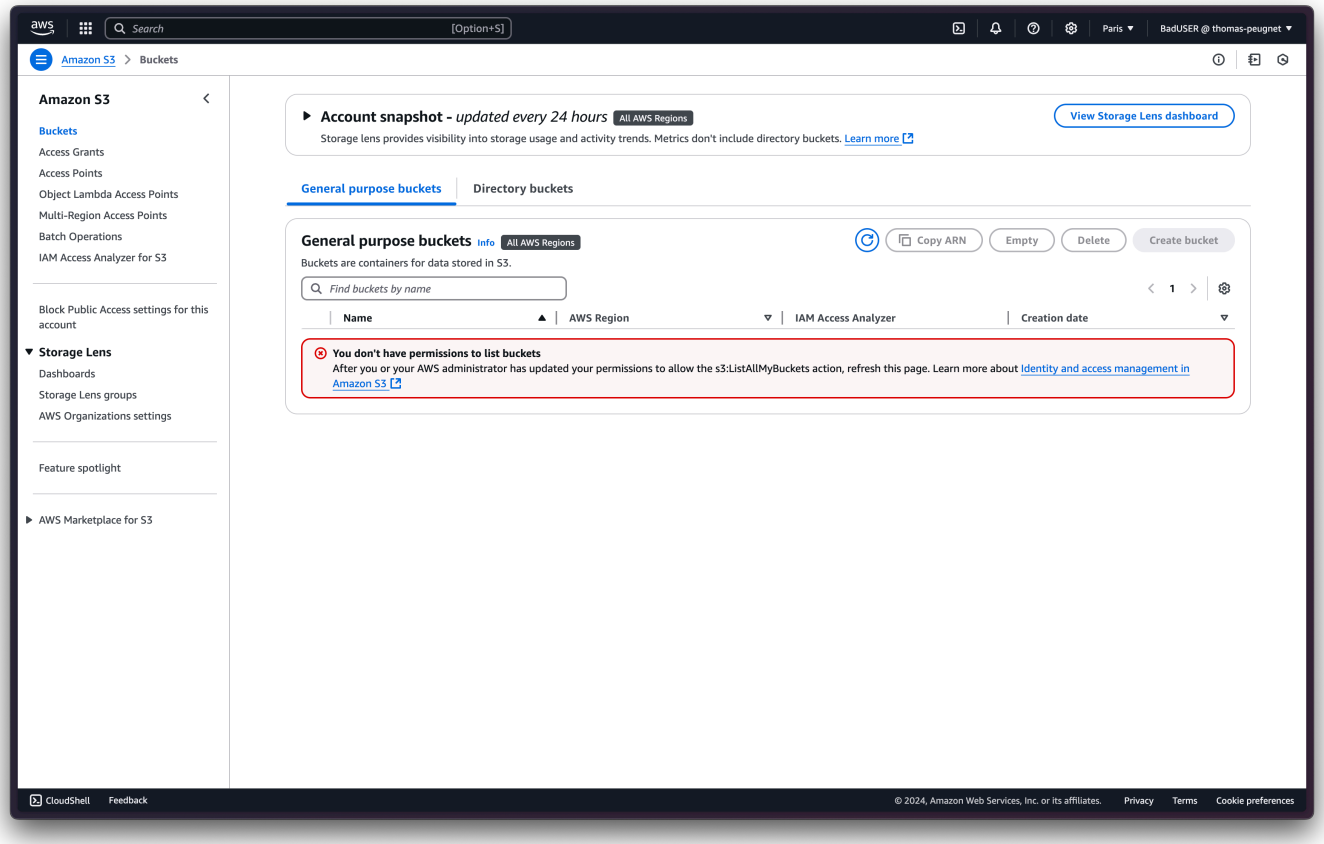
Nous créons un utilisateur `BadUSER`.



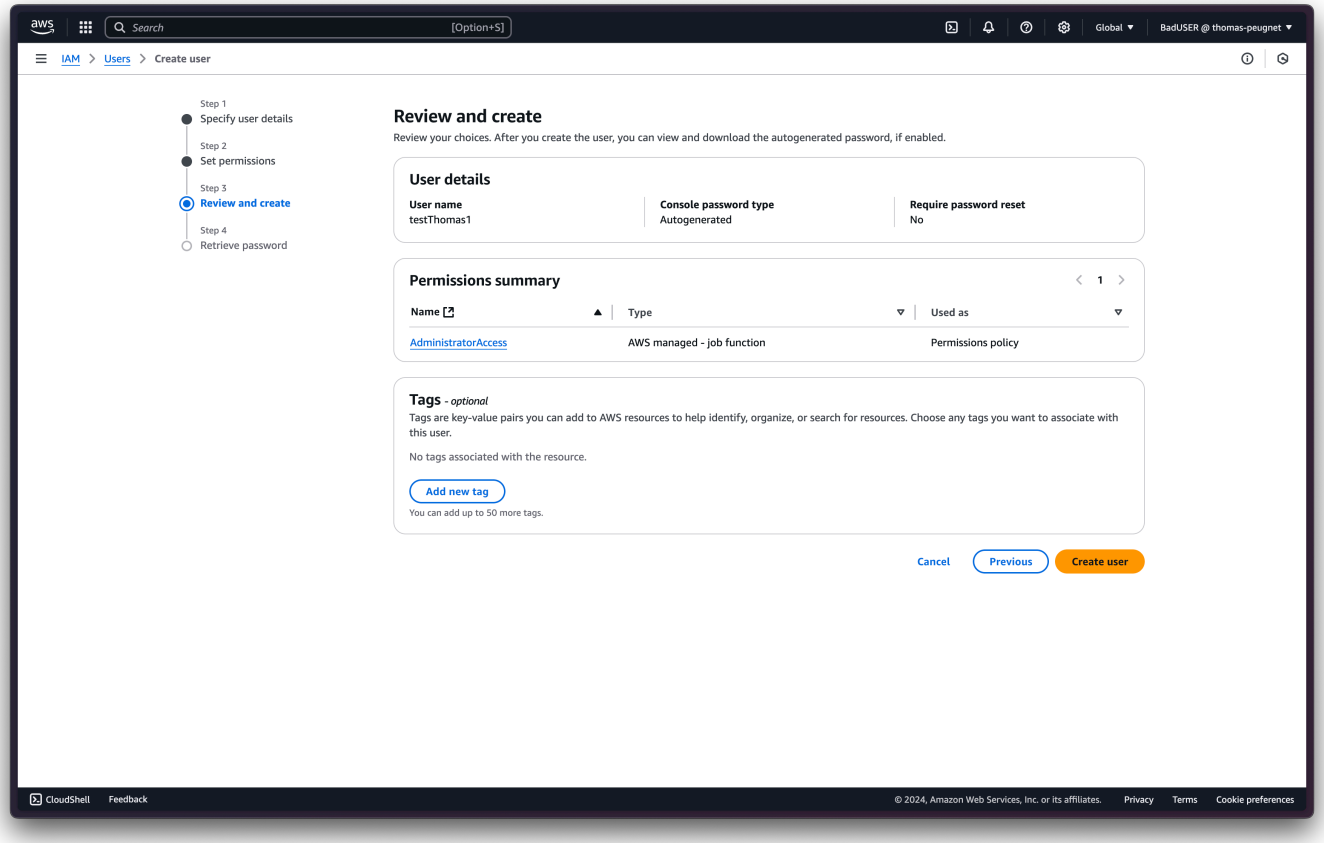
Nous nous connectons avec et constatons le résultat suivant.


Search [Option+S]
Paris
BadUSER @ thomas-peugnet
Console Home Info
Reset to default layout
+ Add widgets
Recently visited Info
No recently visited services
Explore one of these commonly visited AWS services.
EC2 S3 RDS Lambda
View all services
Applications (0) Info
Create application
Region: Europe (Paris)
eu-west-3 (Current Region)
Find applications
Name
Description
Region
Originati.
Access denied to servicecatalog:ListApplications
Go to myApplications
Welcome to AWS
Getting started with AWS
Learn the fundamentals and find valuable information to get the most out of AWS.
Training and certification
Learn from AWS experts and advance your skills and knowledge.
What's new with AWS?
Discover new AWS services, features, and Regions.
AWS Health Info
No health data
You don't have permissions to access AWS Health.
Cost and usage Info
Current month costs
Access denied
Cost breakdown
Access denied
Forecasted month end costs
Access denied
Savings opportunities
Access denied
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

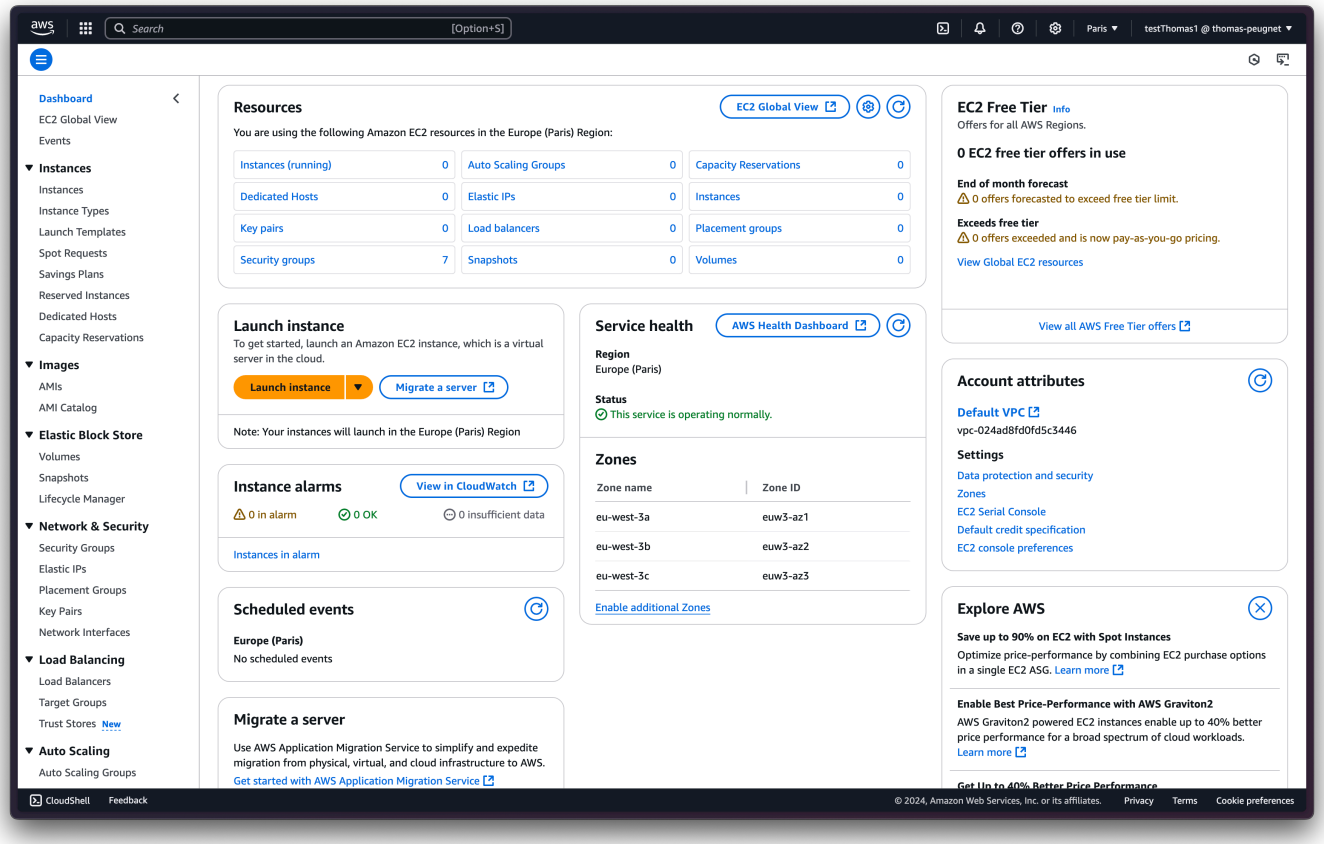

Search [Option+S]
Paris
BadUSER @ thomas-peugnet
Dashboard
EC2 Global View
Events
Instances
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Capacity Reservations
Images
AMIs
AMI Catalog
Elastic Block Store
Volumes
Snapshots
Lifecycle Manager
Network & Security
Security Groups
Elastic IPs
Placement Groups
Key Pairs
Network Interfaces
Load Balancing
Load Balancers
Target Groups
Trust Stores New
Auto Scaling
Auto Scaling Groups
Resources
EC2 Global View
You are using the following Amazon EC2 resources in the Europe (Paris) Region:
Instances (running) 0
Auto Scaling Groups API Error
Capacity Reservations API Error
Dedicated Hosts API Error
Elastic IPs API Error
Instances API Error
Key pairs API Error
Load balancers API Error
Placement groups API Error
Security groups API Error
Snapshots API Error
Volumes API Error
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
Instance alarms
View in CloudWatch
User: arn:aws:iam::794038237731:user/BadUSER is not authorized to perform: cloudwatch:DescribeAlarms on resource: arn:aws:cloudwatch:eu-west-3:794038237731:alarm:* because no identity-based policy allows the cloudwatch:DescribeAlarms action
Instances in alarm
Service health
AWS Health Dashboard
An error occurred
An error occurred retrieving service health information
Zones
Zone name
Zone ID
An error occurred
An error occurred retrieving service health information
Enable additional Zones
EC2 Free Tier Info
Offers for all AWS Regions.
0 EC2 free tier offers in use
End of month forecast
User: arn:aws:iam::794038237731:user/BadUSER is not authorized to perform: freetier:GetFreeTierUsage on resource: arn:aws:freetier:us-east-1:794038237731:/GetFreeTierUsage because no identity-based policy allows the freetier:GetFreeTierUsage action
Exceeds free tier
User: arn:aws:iam::794038237731:user/BadUSER is not authorized to perform: freetier:GetFreeTierUsage on resource: arn:aws:freetier:us-east-1:794038237731:/GetFreeTierUsage because no identity-based policy allows the freetier:GetFreeTierUsage action
View Global EC2 resources
View all AWS Free Tier offers
Account attributes
An error occurred
An error occurred checking for a default VPC
Settings
Data protection and security
Zones
EC2 Serial Console
Default credit specification
EC2 console preferences
Explore AWS
10 Things You Can Do Today to Reduce AWS Costs
Explore how to effectively manage your AWS costs without compromising on performance or capacity. Learn more
CloudShell
Feedback
© 2024, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences



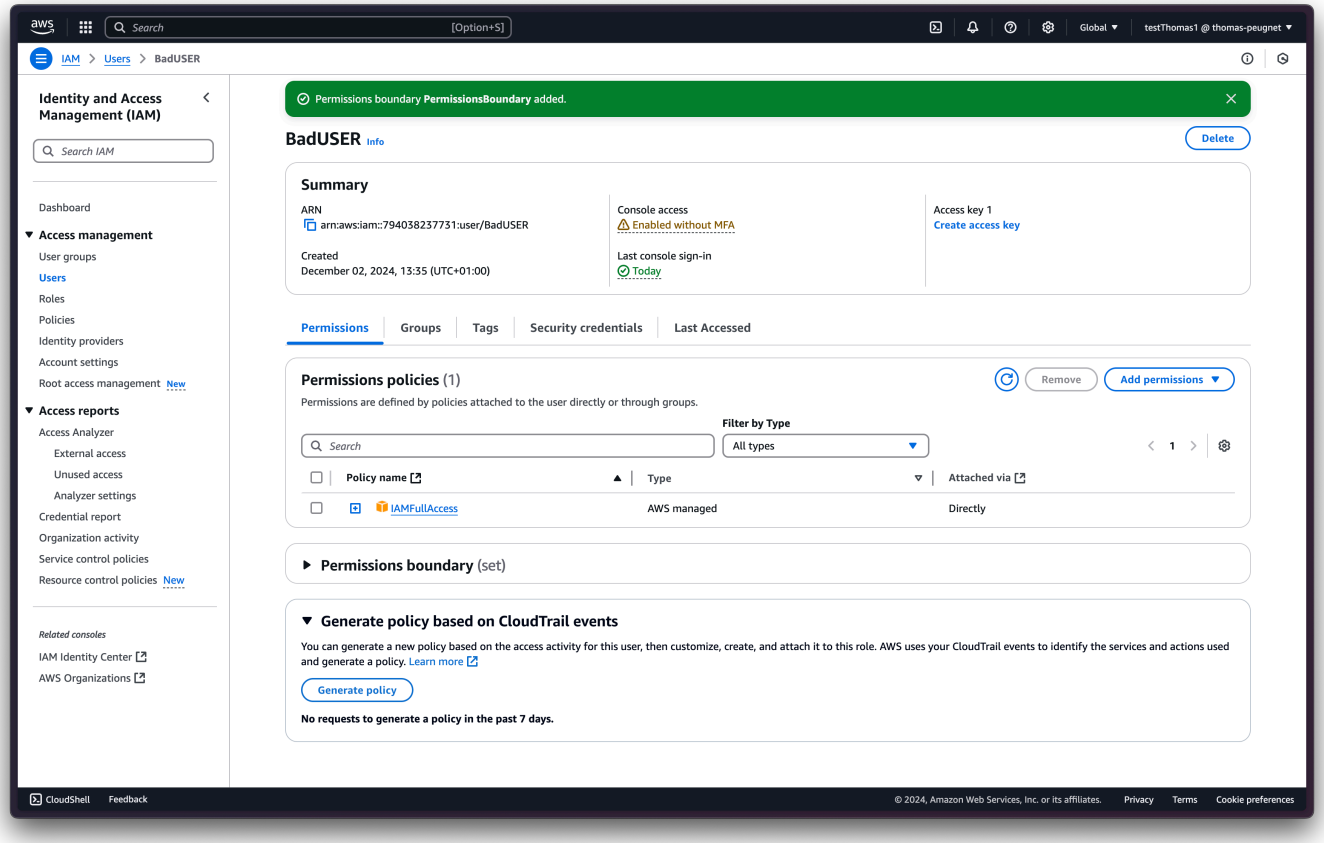
Nous allons effectuer une escalade de privilèges avec un nouvel utilisateur `testThomas1`.



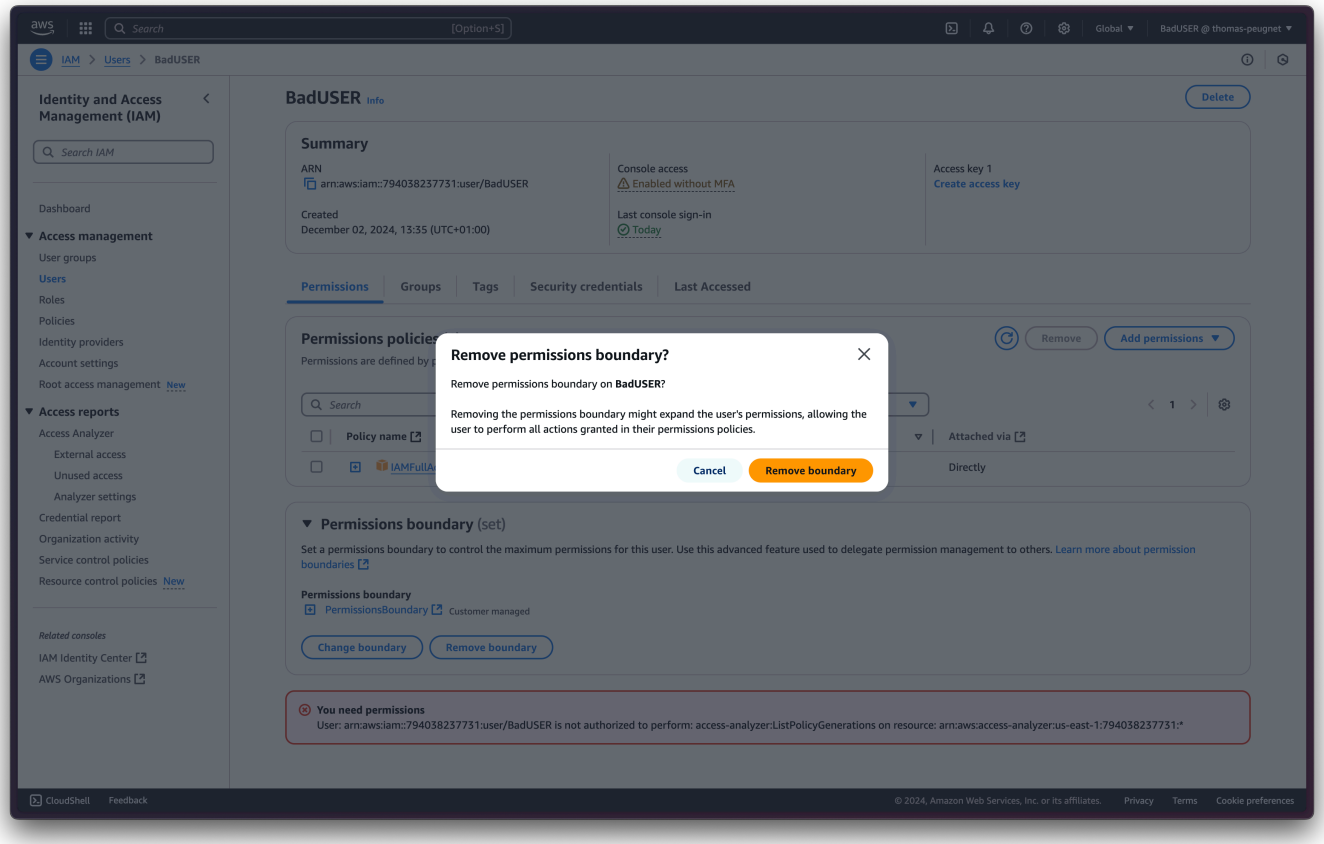
Nous nous reconnectons avec ce nouvel utilisateur et constatons que nous avons maintenant accès.



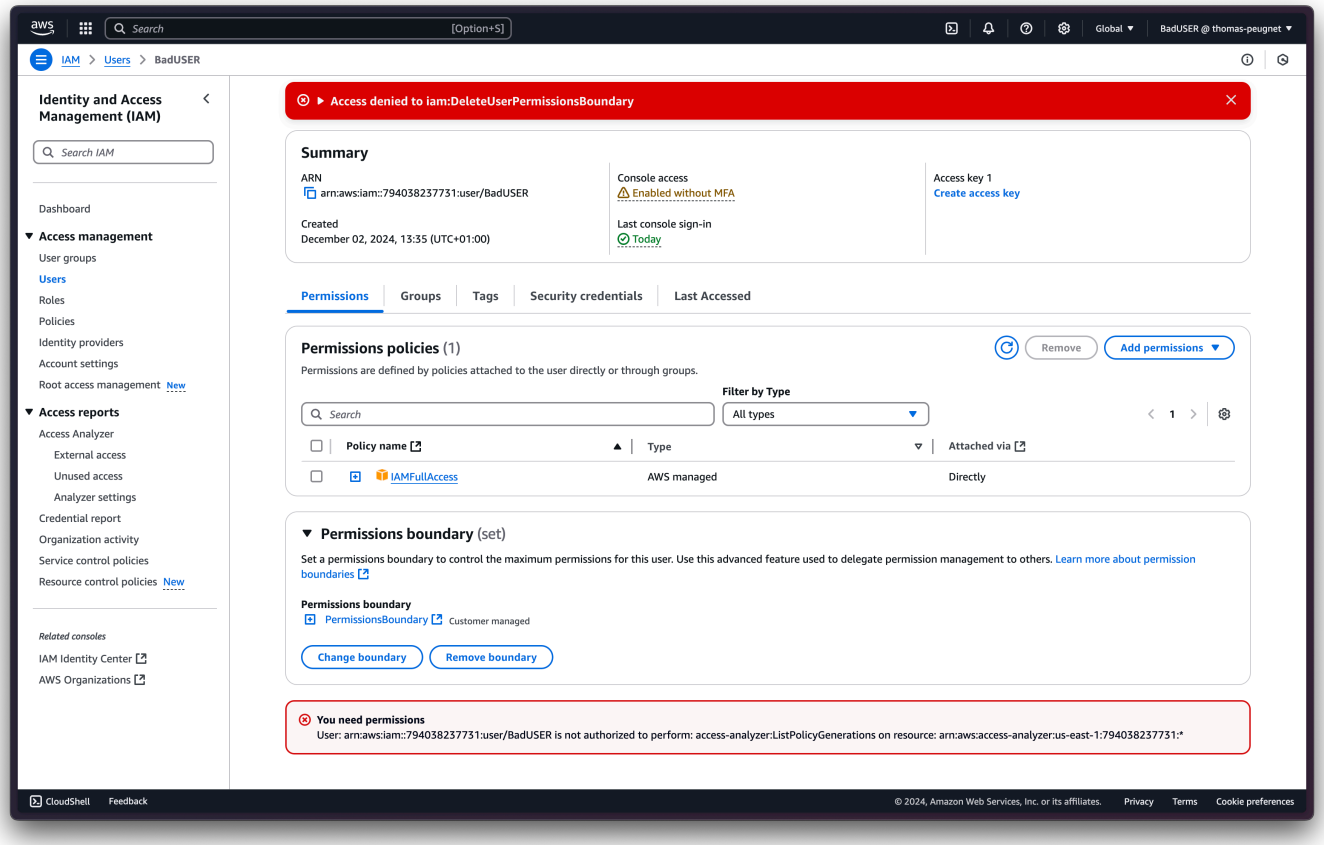
Nous appliquons `PermissionsBoundary` à notre utilisateur `BadUSER`.



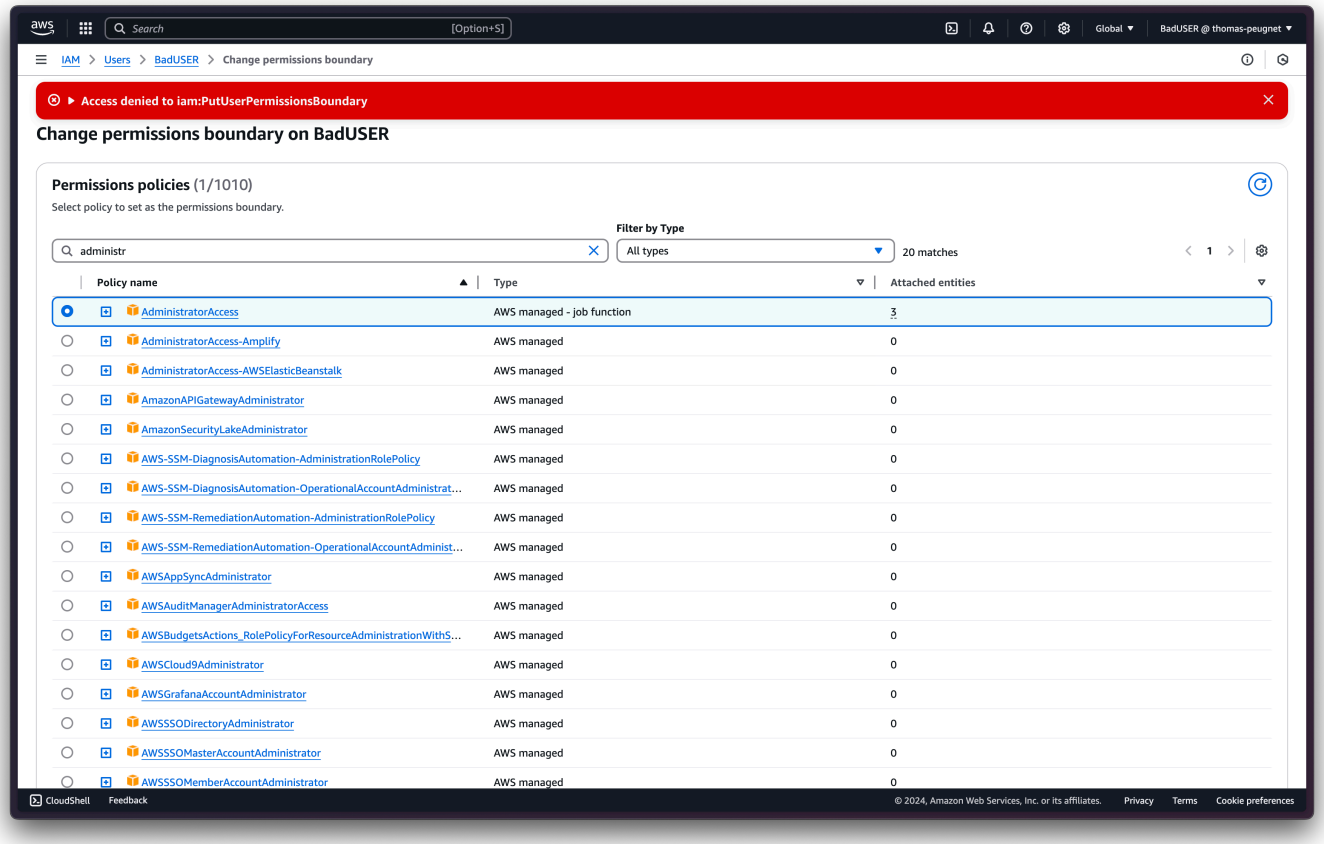
Nous nous reconnectons avec l'utilisateur `BadUSER` et tentons de supprimer permissions boundary.



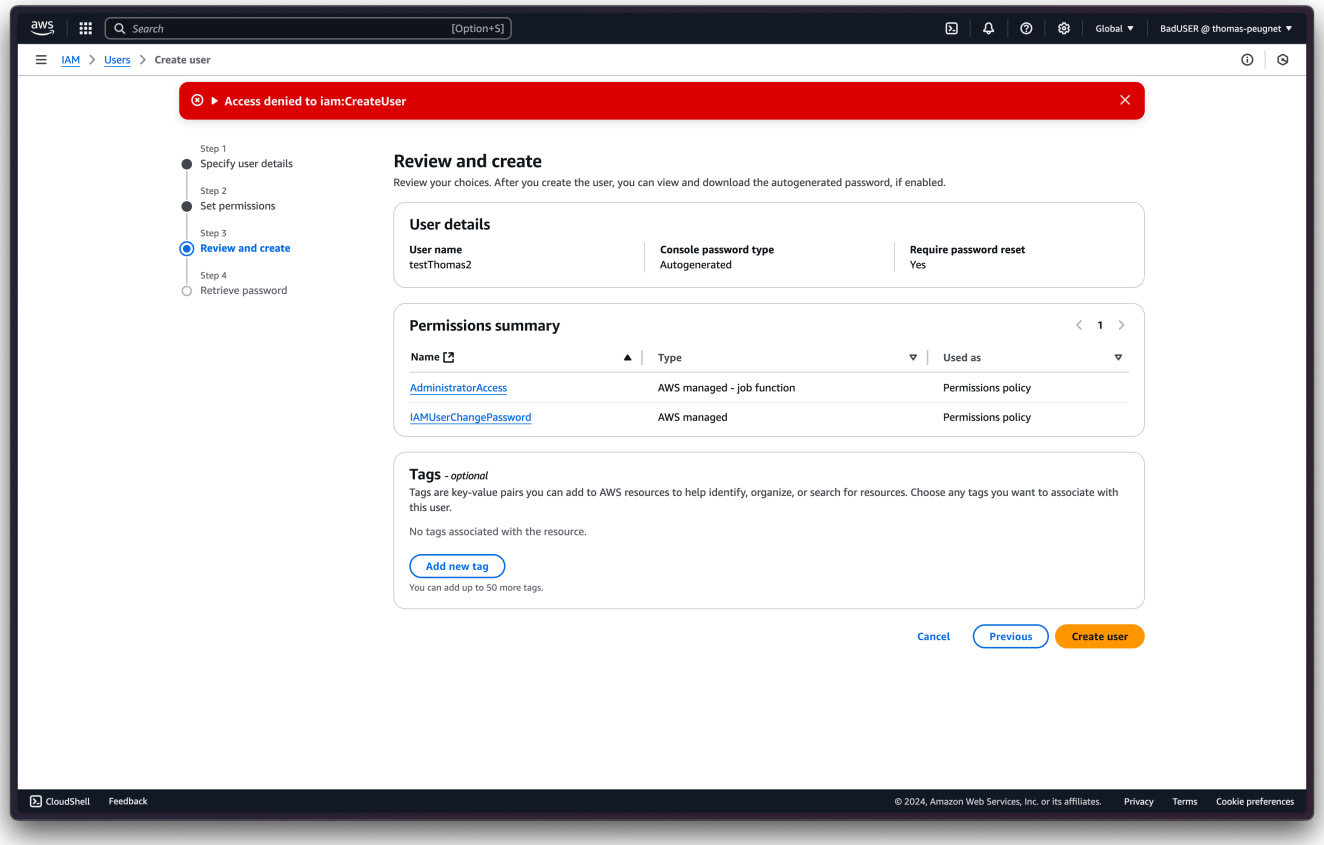
Nous obtenons le retour suivant.



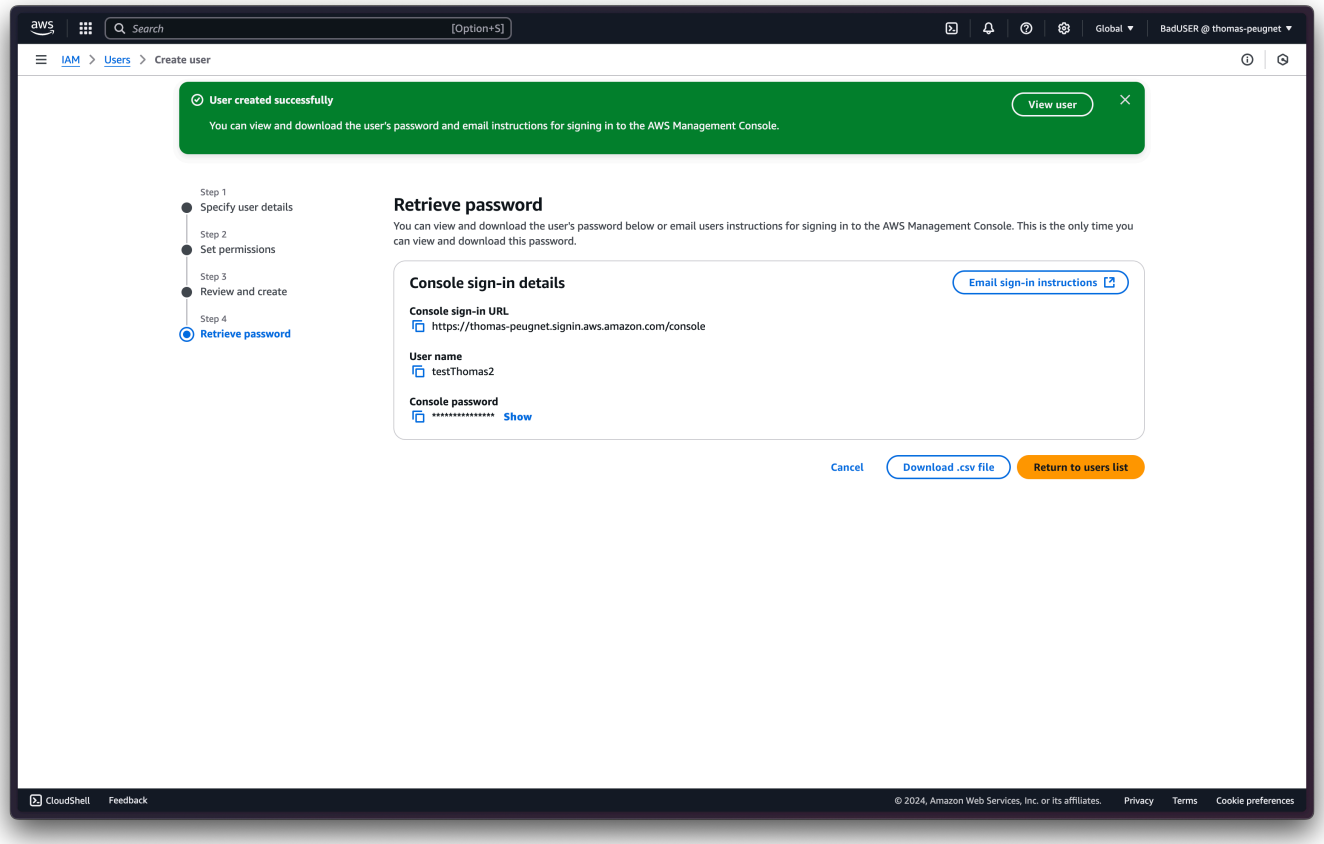
Nous tentons de modifier la politique pour obtenir `AdministratorAccess`.



Nous tentons de recréer un nouvel utilisateur et obtenons le résultat suivant.



Nous assignons notre `PermissionBoundary` à cet utilisateur et pouvons en effet le créer.



Nous pouvons confirmer que l'utilisateur `testThomas2` ne peut pas accéder aux EC2.