

Rendu TP06

Rendu de TP06 effectué par Thomas PEUGNET.

Nous créons notre instance.

Nous nous connectons en SSH à la VM.

```
● ● ●  ✘ 2 ec2-user@ip-172-31-47-175:~  
e host.  
Connection to ec2-35-180-79-238.eu-west-3.compute.amazonaws.com closed.  
└─ thomas@MacBook-Pro-de-Thomas ~/Downloads  
    └─ ssh -i "thomas-key-macos.pem" ec2-user@ec2-15-188-50-217.eu-west-3.compute.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+0w0YHUrC0Ny0H3Z1HG0cLthwMCPbIaIpITI.  
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  
      ~~       \|-'>  
      ~~~        /  
      ~~_._. /  
      _/_/_/  
      _/m/'  
[ec2-user@ip-172-31-47-175 ~]$ █
```

Nous tentons de lister les s3.

```

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+0w0YHrCONyoH3Z1HG0cLthwMCPbIaIpITI.
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.

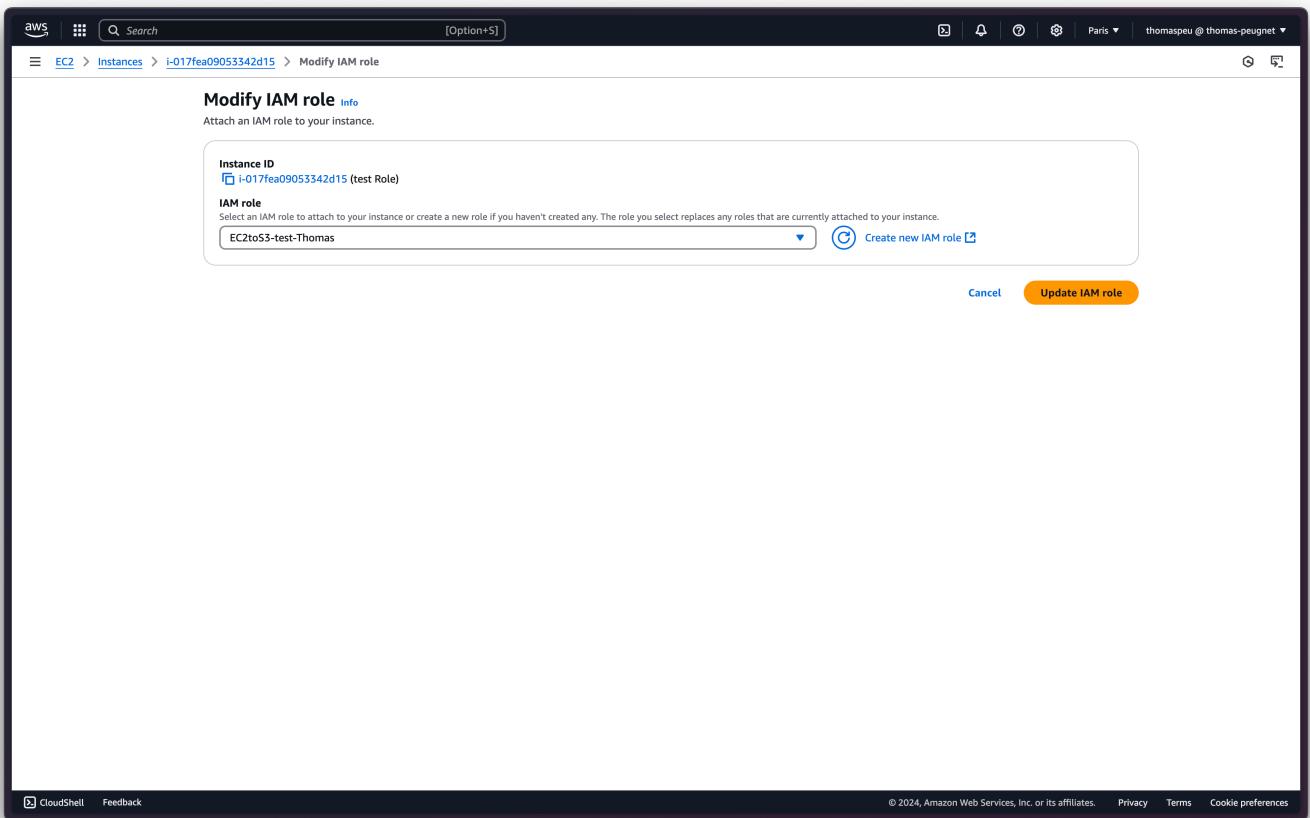
,      #
~\_ ##### Amazon Linux 2023
~~ \#####\
~~   \###|
~~     \#/ ___ https://aws.amazon.com/linux/amazon-linux-2023
~~       \~'-'>
~~         /
~~../. /_
~/ /_/
~/m/' [ec2-user@ip-172-31-47-175 ~]$ aws s3 ls
Unable to locate credentials. You can configure credentials by running "aws con
figure".
[ec2-user@ip-172-31-47-175 ~]$ 

```

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

The screenshot shows the AWS IAM Roles page. The top navigation bar includes the AWS logo, a search bar, and global settings. The main content area has a green header bar stating "Role EC2toS3-test-Thomas created." Below this, there's a table titled "Roles (4) Info" listing four roles: "AWSServiceRoleForOrganizations", "AWSServiceRoleForSupport", "AWSServiceRoleForTrustedAdvisor", and "EC2toS3-test-Thomas". The "EC2toS3-test-Thomas" row shows it was created by "AWS Service: ec2". To the right of the table are three cards: "Access AWS from your non AWS workloads" (X.509 Standard), "X.509 Standard" (using existing PKI infrastructure or AWS Certificate Manager Private Certificate Authority), and "Temporary credentials" (use temporary credentials for enhanced security). The left sidebar contains sections for Identity and Access Management (IAM), Access management (User groups, Roles, Policies, Identity providers, Account settings, Root access management), Access reports (Access Analyzer, External access, Unused access, Analyzer settings, Credential report, Organization activity, Service control policies, Resource control policies), and Related consoles (IAM Identity Center, AWS Organizations).

Nous modifions le rôle IAM pour mettre celui nouvellement créé.



Nous pouvons constater que le `ls` fonctionne désormais.

```
ec2-user@ip-172-31-47-175:~  
.188.50.217)' can't be established.  
ED25519 key fingerprint is SHA256:Ayc9yKc+0w0YHUrCOnyoH3Z1HG0cLthwMCPbIaIpITI.  
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  
~~ \~' \~-->  
~~~ /  
~~~ ._. /  
~~~ /_ /  
~~~ /m/'  
[ec2-user@ip-172-31-47-175 ~]$ aws s3 ls  
Unable to locate credentials. You can configure credentials by running "aws configure".  
[ec2-user@ip-172-31-47-175 ~]$ aws s3 ls  
2024-12-02 12:26:56 bucket-thomas02-12-2024  
[ec2-user@ip-172-31-47-175 ~]$
```

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

Nous nous connectons à cette nouvelle instance.

```
ec2-user@ip-172-31-37-142:~$ host.
Connection to ec2-15-188-50-217.eu-west-3.compute.amazonaws.com closed.
└─thomas@MacBook-Pro-de-Thomas ~/Downloads
  └─ ssh -i "thomas-key-macos.pem" ec2-user@ec2-13-38-7-57.eu-west-3.compute.amazonaws.com
The authenticity of host 'ec2-13-38-7-57.eu-west-3.compute.amazonaws.com (13.38.7.57)' can't be established.
ED25519 key fingerprint is SHA256:euP0kzpsBDuK5VmUUuSih3i7aMGbkQb5pn9aYk3tPA.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ec2-13-38-7-57.eu-west-3.compute.amazonaws.com' (ED25519) to the list of known hosts.
,
#_
~\_ #####_      Amazon Linux 2023
~~ \_#####\_
~~   \###|
~~     \#/ ___ https://aws.amazon.com/linux/amazon-linux-2023
~~       \|~'-'>
~~         /
~~.._. /_
~/m/ /
[ec2-user@ip-172-31-37-142 ~]$
```

Nous créons un nouvel utilisateur Thomas1.

The screenshot shows the 'Create user' process in the AWS IAM console. The user 'Thomas1' has been created with a password type 'None' and no password reset required. They are assigned to the 'Admin' group. There are no tags associated with this user. The 'Create user' button is highlighted.

Nous créons une access key pour notre utilisateur.

The screenshot shows the 'Create access key' process. An access key has been created with the ID 'AKIA3RYC57IRTJOGJSNU'. The 'Show' link next to the secret access key is highlighted. Best practices for managing access keys are listed, including never storing them in plain text or code, disabling or deleting them when no longer needed, enabling least-privilege permissions, and rotating them regularly. The 'Done' button is highlighted.

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

```
● ○ ● ✎ ec2-user@ip-172-31-37-142:~  
[ec2-user@ip-172-31-37-142 ~]$ aws configure  
AWS Access Key ID [None]: AKIA3RYC57IRTJ0GJSNU  
AWS Secret Access Key [None]: 4gNIRtCcZJCsKjAcBu7fKqVESo5usyCkehmqmnTX  
Default region name [None]: eu-west-3  
Default output format [None]:  
[ec2-user@ip-172-31-37-142 ~]$ aws s3 ls  
2024-12-02 12:26:56 bucket-thomas02-12-2024  
[ec2-user@ip-172-31-37-142 ~]$
```

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

```
● ○ ● ✎ ec2-user@ip-172-31-37-142:~/aws  
[ec2-user@ip-172-31-37-142 ~]$ aws s3 ls  
2024-12-02 12:26:56 bucket-thomas02-12-2024  
[ec2-user@ip-172-31-37-142 ~]$ cd .aws  
[ec2-user@ip-172-31-37-142 .aws]$ cat credentials  
[default]  
aws_access_key_id = AKIA3RYC57IRTJ0GJSNU  
aws_secret_access_key = 4gNIRtCcZJCsKjAcBu7fKqVESo5usyCkehmqmnTX  
[ec2-user@ip-172-31-37-142 .aws]$
```

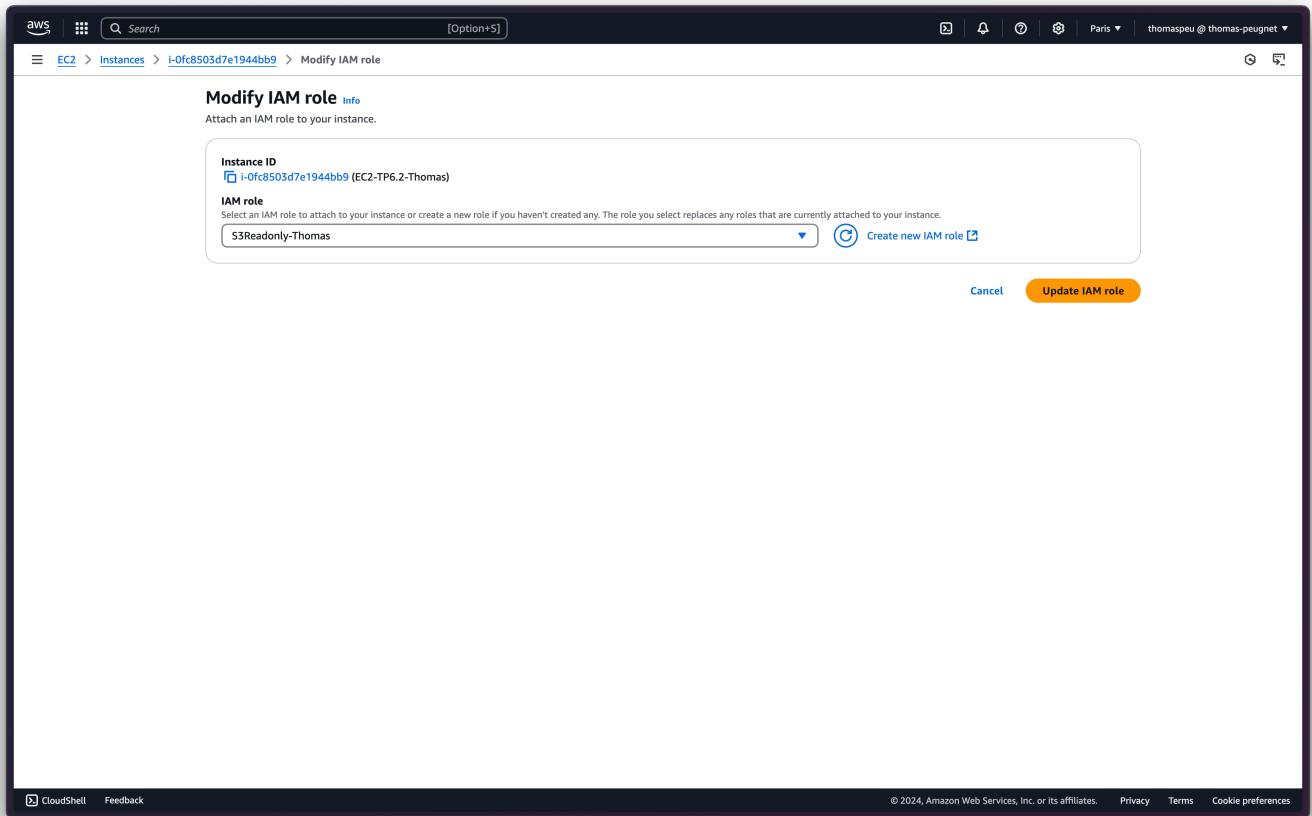
Nous supprimons ce fichier.

```
● ● ●  ~%2 ec2-user@ip-172-31-37-142:~/aws
Warning: Permanently added 'ec2-13-38-7-57.eu-west-3.compute.amazonaws.com' (ED
25519) to the list of known hosts.
      #_
~\_ #####_ Amazon Linux 2023
~~ \#####\
~~ \###|
~~ \#/ ___ https://aws.amazon.com/linux/amazon-linux-2023
~~ \~' '-'>
~~~ /
~~_. /_
/_/ _/
/_m/'

[ec2-user@ip-172-31-37-142 ~]$ aws configure
AWS Access Key ID [None]: AKIA3RYC57IRTJ0GJSNU
AWS Secret Access Key [None]: 4gNIRtCcZJCsKjAcBu7fKqVESo5usyCkehmqmnTX
Default region name [None]: eu-west-3
Default output format [None]:
[ec2-user@ip-172-31-37-142 ~]$ aws s3 ls
2024-12-02 12:26:56 bucket-thomas02-12-2024
[ec2-user@ip-172-31-37-142 ~]$ cd .aws
[ec2-user@ip-172-31-37-142 .aws]$ cat credentials
[default]
aws_access_key_id = AKIA3RYC57IRTJ0GJSNU
aws_secret_access_key = 4gNIRtCcZJCsKjAcBu7fKqVESo5usyCkehmqmnTX
[ec2-user@ip-172-31-37-142 .aws]$ rm -rf *
[ec2-user@ip-172-31-37-142 .aws]$ aws s3 ls

Unable to locate credentials. You can configure credentials by running "aws con
figure".
[ec2-user@ip-172-31-37-142 .aws]$ █
```

Nous modifions le role IAM.



Nous pouvons voir le résultat suivant.

```
● ○ ● ✎ 2 ec2-user@ip-172-31-37-142:~/aws

      #_
~\_ #####_ Amazon Linux 2023
~~ \_#####\
~~ \###|
~~ \#/ __ https://aws.amazon.com/linux/amazon-linux-2023
~~ \~'-'>
~~~ /
~~_. /_
/_/ /_
/_m/'_

[ec2-user@ip-172-31-37-142 ~]$ aws configure
AWS Access Key ID [None]: AKIA3RYC57IRTJ0GJSNU
AWS Secret Access Key [None]: 4gNIRtCcZJCsKjAcBu7fKqVESo5usyCkehmqmnTX
Default region name [None]: eu-west-3
Default output format [None]:
[ec2-user@ip-172-31-37-142 ~]$ aws s3 ls
2024-12-02 12:26:56 bucket-thomas02-12-2024
[ec2-user@ip-172-31-37-142 ~]$ cd .aws
[ec2-user@ip-172-31-37-142 .aws]$ cat credentials
[default]
aws_access_key_id = AKIA3RYC57IRTJ0GJSNU
aws_secret_access_key = 4gNIRtCcZJCsKjAcBu7fKqVESo5usyCkehmqmnTX
[ec2-user@ip-172-31-37-142 .aws]$ rm -rf *
[ec2-user@ip-172-31-37-142 .aws]$ aws s3 ls

Unable to locate credentials. You can configure credentials by running "aws configure".
[ec2-user@ip-172-31-37-142 .aws]$ aws s3 ls
2024-12-02 12:26:56 bucket-thomas02-12-2024
[ec2-user@ip-172-31-37-142 .aws]$ █
```

Nous supprimons tous les éléments du TP.

Screenshot of the AWS IAM Users page. A modal window titled "Managing human user access account by account? There's a better way." is displayed, showing four icons: "One-time set up for workforce user access" (two people icon), "Centrally manage access to multiple AWS accounts" (laptop icon), "Provide access centrally to the cloud applications your workforce uses" (monitor icon), and "All with one-click access through a simple web portal" (monitor with cursor icon). Below the modal is a table listing 8 IAM users:

User name	Path	Group	Last activity	MFA	Password age	Console last sign-in	Access key ID
BadUSER	/	0	1 hour ago	-	1 hour	December 02, 2024, 1...	-
Joanne	/	0	1 hour ago	-	1 hour	December 02, 2024, 1...	-
Mathias	/	1	-	-	19 days	-	-
testABAC	/	0	-	-	-	-	-
testThomas1	/	0	1 hour ago	-	1 hour	December 02, 2024, 1...	-
testThomas2	/	0	1 hour ago	-	1 hour	December 02, 2024, 1...	-
Thomas1	/	1	9 minutes ago	-	-	-	Active - AKIA3RYC57IR...
thomaspeu	/	0	1 hour ago	Virtual	19 days	December 02, 2024, 1...	-

Nous nous connectons au service EC2.

Screenshot of the AWS EC2 Instances page. The left sidebar shows navigation links for Dashboard, Instances, Images, Elastic Block Store, Network & Security, Load Balancing, and Auto Scaling. The main content area includes sections for Resources (listing 0 instances, 0 auto scaling groups, 0 capacity reservations, etc.), Launch instance (with "Launch instance" and "Migrate a server" buttons), Service health (status: "This service is operating normally"), Zones (listing AZs: us-east-1a, us-east-1b, us-east-1c, us-east-1d, us-east-1e, us-east-1f), Account attributes (Default VPC: vpc-0a9b71bfd7dae8e35), and Explore AWS (sections for Get Up to 40% Better Price Performance, Amazon GuardDuty Malware Protection, and Comparable Best Price Performance with AWS Lambda).

Nous créons notre nouveau rôle.

Role S3Readonly-thomas-TP6.3 created.

Roles (1/5) Info

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

Role name	Trusted entities	Last activity
AWSServiceRoleForOrganizations	AWS Service: organizations (Service-Linker)	-
AWSServiceRoleForSupport	AWS Service: support (Service-Linker)	-
AWSServiceRoleForTrustedAdvisor	AWS Service: trustedadvisor (Service-Linker)	-
S3Readonly-Thomas	AWS Service: ec2	-
S3Readonly-thomas-TP6.3	Account: 794038237731	-

Roles Anywhere Info

Authenticate your non AWS workloads and securely provide access to AWS services.

Access AWS from your non AWS workloads

Operate your non AWS workloads using the same authentication and authorization strategy that you use within AWS.

X.509 Standard

Use your own existing PKI infrastructure or use [AWS Certificate Manager Private Certificate Authority](#) to authenticate identities.

Temporary credentials

Use temporary credentials with ease and benefit from the enhanced security they provide.

Nous faisons le switch du role.

Switch Role

Switching roles enables you to manage resources across Amazon Web Services accounts using a single user. When you switch roles, you temporarily take on the permissions assigned to the new role. When you exit the role, you give up those permissions and get your original permissions back. [Learn more](#)

Account ID
The 12-digit account number or the alias of the account in which the role exists.

IAM role name
The name of the role that you want to assume which can be found at the end of the role's ARN. For example, provide the TestRole role name from the following role ARN: arn:aws:iam::123456789012:role/TestRole.

Display name - optional
This name will appear in the console navigation bar when active. Choose a name to help identify the permission set assigned to the role.

Display color - optional
The selected color displays in the console navigation when this role is active.
 Red

Cancel **Switch Role**

Nous avons bien le résultat suivant.

The screenshot shows the AWS Console Home page. It includes sections for Recently visited services (with a placeholder for a cube icon), Applications (listing 0 applications with a note about access denied), Welcome to AWS (with links for Getting started with AWS, Training and certification, and What's new with AWS), AWS Health (showing no health data), and Cost and usage (listing current month costs, forecasted month end costs, and savings opportunities, all with access denied notes). The bottom of the page has CloudShell, Feedback, and footer links.

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

The screenshot shows the AWS EC2 Dashboard. The left sidebar lists navigation items such as Dashboard, Instances, Images, Elastic Block Store, Network & Security, Load Balancing, and Auto Scaling. The main content area shows Resources (listing 0 instances running, 0 auto scaling groups, 0 capacity reservations, 0 dedicated hosts, 0 elastic IPs, 0 key pairs, 0 load balancers, 0 security groups, 0 snapshots, 0 instances, 0 placement groups, 0 volumes), Launch instance (with Launch instance and Migrate a server buttons), Service health (with an error occurred message and a Diagnose with Amazon Q button), Zones (with an error occurred message and a Diagnose with Amazon Q button), and Account attributes (with an error occurred message and a Diagnose with Amazon Q button). The bottom of the page has CloudShell, Feedback, and footer links.

Idem pour le service IAM.

The screenshot shows the AWS IAM Dashboard. On the left, there's a sidebar with navigation links like 'Identity and Access Management (IAM)', 'Dashboard', 'Access management', 'Access reports', and 'Related consoles'. The main content area is titled 'IAM Dashboard' and contains sections for 'IAM resources' (showing an 'Access denied' error for 'iam:GetAccountSummary'), 'What's new' (listing recent changes), and 'AWS Account' (also showing an 'Access denied' error for 'iam>ListAccountAliases').

Pas de problème pour la lecture sur S3.

The screenshot shows the AWS S3 Bucket details page for 'bucket-thomas02-12-2024'. The left sidebar includes 'Amazon S3', 'Buckets', 'Storage Lens', and 'AWS Marketplace for S3'. The main content area shows the bucket's configuration with tabs for 'Objects', 'Properties', 'Permissions', 'Metrics', 'Management', and 'Access Points'. It displays 'Objects (0)' and a message stating 'No objects'. There are buttons for 'Upload' and 'Create folder'.

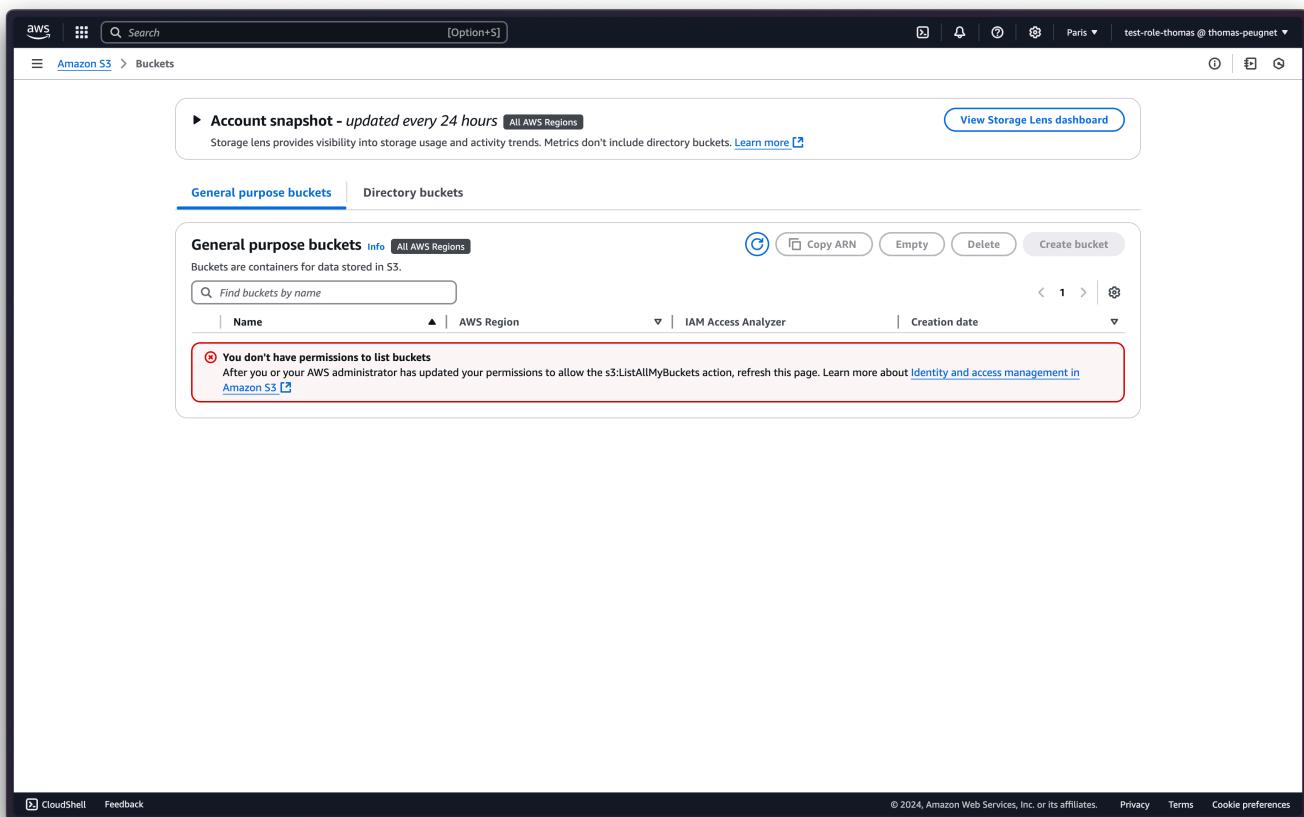
Nous ne pouvons pas créer de bucket.

The screenshot shows the 'Create bucket' wizard on the AWS S3 service. In the 'Default encryption' section, the 'Server-side encryption with Amazon S3 managed keys (SSE-S3)' option is selected. In the 'Bucket Key' section, the 'Enable' option is selected. A red box highlights the error message 'Failed to create bucket' under the heading 'Failed to create bucket'. The message states: 'To create a bucket, the s3:CreateBucket permission is required.' Below this, it says 'View your permissions in the IAM console [?] Identity and Access Management in Amazon S3 [?]' and '▶ API response'. At the bottom right, there are 'Cancel' and 'Create bucket' buttons.

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

The screenshot shows the 'Users' page in the AWS IAM service. On the left, there is a navigation menu with options like 'Identity and Access Management (IAM)', 'Access management', 'Access reports', and 'Related consoles'. The main area shows a user named 'test-role-thomas' has been created successfully. A green box displays the message: 'User created successfully. You can view and download the user's password and email instructions for signing in to the AWS Management Console.' Below this, there is a 'Summary' section with details: ARN (arn:aws:iam::794058237731:user/test-role-thomas), Console access (Disabled), Last console sign-in (December 02, 2024, 15:18 (UTC+01:00)), and an 'Access key 1' button with 'Create access key'. Below the summary, there are tabs for 'Permissions', 'Groups', 'Tags', 'Security credentials', and 'Last Accessed'. Under the 'Permissions' tab, there is a section for 'Permissions policies (0)' with a note: 'Permissions are defined by policies attached to the user directly or through groups.' A search bar and filter options are available. A red box highlights the 'Generate policy based on CloudTrail events' section, which includes a 'Generate policy' button and the note: 'You can generate a new policy based on the access activity for this user, then customize, create, and attach it to this role. AWS uses your CloudTrail events to identify the services and actions used and generate a policy. Learn more [?]'.

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.

Screenshot of the AWS IAM User Details page for 'test-role-thomas'. The page shows basic user information like ARN, console access status, and a single inline policy named 'test-assume-role'. The 'Permissions' tab is selected, showing the attached policy.

Nous switchons de rôle.

Screenshot of the 'Switch Role' dialog box. It shows fields for Account ID (thomas-peugnet), IAM role name (\$3ReadOnly-thomas-TP6.3), Display name (S3ReadOnly-thomas-TP6.3 @ thomas-peugnet), and Display color (Red). The 'Switch Role' button is highlighted.

Nous avons bien un accès en lecture seule.

The screenshot shows the AWS S3 console interface. On the left, there's a sidebar with navigation links like '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' (which is expanded), 'Dashboards', 'Storage Lens groups', 'AWS Organizations settings', 'Feature spotlight', and 'AWS Marketplace for S3'. The main content area has a header 'Account snapshot - updated every 24 hours [All AWS Regions]' with a note about storage usage trends. Below it, there are tabs for 'General purpose buckets' (which is selected) and 'Directory buckets'. A table lists one bucket: 'bucket-thomas02-12-2024' (Name), 'Europe (Paris) eu-west-3' (AWS Region), and 'December 2, 2024, 13:26:55 (UTC+01:00)' (Creation date). Action buttons include 'Copy ARN', 'Empty', 'Delete', and 'Create bucket'. At the bottom, there are links for 'CloudShell', 'Feedback', and copyright information: '© 2024, Amazon Web Services, Inc. or its affiliates.' followed by 'Privacy', 'Terms', and 'Cookie preferences'.