

# Rendu TP01

Ce TP a été réalisé par Thomas PEUGNET.

## Préparation

Nous commençons par installer AWS CLI avec les commandes suivantes:

```
thomas@MacBook-Pro-de-Thomas:~  
└─ thomas@MacBook-Pro-de-Thomas ~  
    └─ curl "https://awscli.amazonaws.com/AWSCLIV2.pkg" -o "AWSCLIV2.pkg"  
    └─ sudo installer -pkg AWSCLIV2.pkg -target /  
        % Total    % Received % Xferd  Average Speed   Time     Time      Time  Current  
                  Dload  Upload Total   Spent    Left Speed  
100 38.3M  100 38.3M    0      0  28.3M       0  0:00:01  0:00:01 --:--:-- 28.3M  
Password:  
installer: Package name is AWS Command Line Interface  
installer: Installing at base path /  
installer: The install was successful.  
└─ thomas@MacBook-Pro-de-Thomas ~  
    └─ which aws  
    /usr/local/bin/aws  
└─ thomas@MacBook-Pro-de-Thomas ~  
    └─  
    └─ thomas@MacBook-Pro-de-Thomas ~  
    └─ █
```

Nous poursuivons avec les étapes d'inscription à l'offre gratuite de AWS.

The screenshot shows the AWS sign-up confirmation page. At the top, there's a navigation bar with links for 'Produits', 'Solutions', 'Tarification', 'Documentation', 'Apprendre', 'Réseau de partenaires', 'AWS Marketplace', 'Déploiements clients', 'Événements', 'Découvrir davantage', and a search icon. The top right features links for 'À propos d'AWS', 'Nous contacter', 'Support', 'Français', 'Mon compte', and a button to 'Connectez-vous à la console'. Below the navigation is a large blue rocket launching from a cloud icon. The main heading is 'Félicitations !' followed by the text 'Merci de vous être inscrit à AWS.' A message below states: 'Nous procédons actuellement à l'activation de votre compte. Cela devrait prendre quelques minutes. Vous recevez un e-mail au terme de la procédure.' There are two buttons: 'Accéder à la console de gestion AWS' (orange) and 'Créer un autre compte ou contacter le service commercial' (blue). At the bottom, a dark banner contains the text 'Sélectionner vos préférences de cookies' with a detailed explanation about cookies. It includes three buttons: 'Accepter' (orange), 'Refuser' (white), and 'Personnaliser' (white).

Nous activons la MFA depuis les recommandations de la section IAM. Nous configurons notre application Google Authenticator.

Screenshot of the AWS IAM console showing the "Attribuer un dispositif MFA" (Assign MFA device) step. The user is selecting an MFA device type.

**MFA device name:** Nom du dispositif (Device name)

**MFA device:**

- Clé d'accès ou clé de sécurité (Access key or security key):** Authentifiez-vous à l'aide de votre empreinte digitale, de votre visage ou du verrouillage d'écran. Créez une clé d'accès sur cet appareil ou utilisez un autre appareil, comme une clé de sécurité FIDO2.
- Application d'authentification (Authentication app):** S'authentifier à l'aide d'un code généré par une application installée sur votre appareil mobile ou votre ordinateur.
- Jeton TOTP matériel (Hardware TOTP token):** Authentifiez-vous à l'aide d'un code généré par un jeton TOTP matériel ou d'autres appareils matériels.

Bottom navigation bar: CloudShell, Commentaires, © 2024, Amazon Web Services, Inc. ou ses affiliés, Confidentialité, Conditions, Préférences relatives aux cookies.

## Gestion des utilisateurs avec IAM

Nous créons un utilisateur `test-user-1`.

The screenshot shows the AWS IAM 'Create New User' wizard at Step 3: Verify and Create. The left sidebar lists three steps: Step 1 (Specify details), Step 2 (Set permissions), and Step 3 (Verify and create). The main content area is titled 'Vérifier et créer' and contains the following sections:

- Détails de l'utilisateur**: Shows the user name 'test-user-1' and console password type 'None'. A checkbox for requesting password reset is checked.
- Résumé des autorisations**: Shows no resources associated with the user.
- Balises - facultatif**: Shows no tags assigned to the user.

At the bottom right are buttons for 'Annuler' (Cancel), 'Précédent' (Previous), and a prominent orange 'Créer un utilisateur' (Create User) button.

Nous activons l'accès à la console.

The screenshot shows the AWS Identity and Access Management (IAM) service interface. On the left, the navigation menu includes options like 'Tableau de bord', 'Gestion des accès', 'Utilisateurs', 'Rôles', 'Politiques', 'Fournisseurs d'identité', 'Paramètres du compte', 'Rapports d'accès', 'Analyseur d'accès', 'Activités de l'organisation', and 'Politiques de contrôle des services'. The main content area displays the 'test-user-1' user profile. A modal window titled 'Activer l'accès à la console' is centered, asking the user to choose a password type. The 'Mot de passe généré automatiquement' option is selected. Below the modal, a note states: 'L'utilisateur doit créer un nouveau mot de passe lors de la prochaine connexion. Les utilisateurs obtiennent automatiquement la politique IAMUserChangePassword [?] les autorisant à modifier leur propre mot de passe.' At the bottom of the modal, there are 'Annuler' and 'Activer l'accès à la console' buttons, with the latter being orange. Below the modal, there's a section for MFA devices with a large 'Attribuer un dispositif MFA' button.

On effectue une connexion sur le lien de connexion fourni lors de l'activation de l'accès console.

The screenshot shows the AWS Management Console homepage. At the top, there's a search bar and a 'Réinitialiser la mise en page par défaut' (Reset layout) button. A 'Créer une application' (Create application) button is also visible. The main content area includes:

- Récemment visité**: Shows a single entry: IAM.
- Applications**: Shows 0 applications. It includes a 'Créer une application' button and a search bar for 'Rechercher des applications'. A red box highlights the 'Accès refusé' (Access denied) status for a specific application entry.
- Bienvenue sur AWS**: Includes links for 'Démarrage avec AWS', 'Formation et certification', and 'Quelles sont les nouveautés d'AWS?'.
- AWS Health**: Shows 'Aucune donnée d'état' (No data available) and a message stating 'Vous n'êtes pas autorisé à accéder à AWS Health.'
- Coût et utilisation**: Shows cost information for the month and savings opportunities, both of which are marked as 'Accès refusé'.

At the bottom, there are links for CloudShell, Commentaires, and other AWS services like Confidentialité, Conditions, and Préférences relatives aux cookies.

On se deconnecte du compte `test-user-1`, on se reconnecte avec le compte `root` et on ajoute une politique d'autorisation pour l'utilisateur `test-user-1`.

The screenshot shows the AWS IAM User Details page for a user named 'test-user-1'. The left sidebar contains navigation links for Identity and Access Management (IAM), including 'Utilisateurs' (selected), 'Rôles', 'Politiques', 'Fournisseurs d'identité', and 'Paramètres du compte'. The main content area displays the user's ARN (arn:aws:iam::794038237731:user/test-user-1), creation date (November 13, 2024, 09:30 (UTC+01:00)), and last connection (Aujourd'hui). It also shows that access is via the console without MFA (Activé sans l'authentification MFA). The 'Autorisations' tab is selected, showing no attached policies (0). A 'Créer une politique en ligne' button is visible. The bottom of the page includes a link to generate a CloudTrail policy and a note about generating a policy based on activity.

On ajoute le code indiqué dans le sujet du TP, donnant donc le JSON complet suivant:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "s3fullaccess",
      "Effect": "Allow",
      "Action": "s3:*",
      "Resource": "*"
    }
  ]
}
```

Nous créons notre politique `S3FullAccess`.

The screenshot shows the AWS Identity and Access Management (IAM) service interface. A user named 'test-user-1' has been created. The 'Récapitulatif' section displays the ARN (arn:aws:iam::794038237731:user/test-user-1), access method (Accès par console - Activé sans l'authentification MFA), creation date (November 13, 2024, 09:30 (UTC+01:00)), and last connection (Aujourd'hui). The 'Autorisations' tab is selected, showing one policy attached: 'S3FullAccess'. Other tabs include 'Groupes', 'Balises', 'Informations d'identification de sécurité', and 'Last Accessed'. The bottom section provides options to generate a CloudTrail-based policy or to generate a new one.

Nous nous connectons ensuite au service IAM Policy Simulator grâce à l'URL <https://policysim.aws.amazon.com/home/index.jsp>.

IAM Policy Simulator

Mode : Existing Policies thomaspeugnet Run Simulation

Users, Groups, and Roles

Users Filter test-user-1

Policy Simulator

Select service Select actions Select All Deselect All Reset Contexts Clear Results Run Simulation

Global Settings

Action Settings and Results [0 actions selected. 0 actions not simulated. 0 actions allowed. 0 actions denied.]

Service	Action	Resource Type	Simulation Resource	Permission
---------	--------	---------------	---------------------	------------

The IAM policy simulator is a testing environment that may not model all of the factors present in your production environment, so we cannot guarantee the accuracy of the results. Authorization results in your production environment may differ from what's shown in the IAM policy simulator therefore we recommend testing your policies with production IAM users and AWS requests.

© 2013, Amazon Web Services, Inc. or its affiliates. All rights reserved.  
An [amazon.com](#) company

This screenshot shows the IAM Policy Simulator interface. On the left, there's a sidebar titled 'Users, Groups, and Roles' with a dropdown set to 'Users' and a 'Filter' input field containing 'test-user-1'. The main area is titled 'Policy Simulator' and contains several buttons: 'Select service', 'Select actions', 'Select All', 'Deselect All', 'Reset Contexts', 'Clear Results', and a prominent blue 'Run Simulation' button. Below these buttons is a link to 'Global Settings'. Underneath is a section titled 'Action Settings and Results' with the message '[0 actions selected. 0 actions not simulated. 0 actions allowed. 0 actions denied.]'. A large table is present, with its header row showing columns for Service, Action, Resource Type, Simulation Resource, and Permission. At the bottom of the page, there's a note about the simulator being a testing environment and a copyright notice for Amazon Web Services.

Après avoir sélectionné notre utilisateur et les 160 actions possibles sur AmazonS3 , nous avons bien le résultat suivant:

**IAM Policy Simulator**

Policies
Back
Create New Policy

Selected user: test-user-1

**IAM Policies**

  
 S3FullAccess

**Custom IAM Policies**

There are no policies to display!

**Permissions Boundary Policy**

You can simulate a maximum of one permissions boundary policy per user or role.  
There are no policies to display!

**Custom IAM Permissions Boundary Policy**

There are no policies to display!

**Resource Policies**

**Policy Simulator**

Amazon S3    160 Action(s) selected    Select All    Deselect All    Reset Contexts    Clear Results    Run Simulation

▶ Global Settings ⓘ

Action Settings and Results [160 actions selected, 0 actions not simulated, 160 actions allowed, 0 actions denied.]

Service	Action	Resource Type	Simulation Resource	Permission
▶ Amazon S3	AbortMultipartUpload	object	▪	● allowed 1 matching statements.
▶ Amazon S3	AssociateAccessGrantsIdentity...	accessgrantsinstance	▪	● allowed 1 matching statements.
▶ Amazon S3	BypassGovernanceRetention	object	▪	● allowed 1 matching statements.
▶ Amazon S3	CreateAccessGrant	accessgrantslocation	▪	● allowed 1 matching statements.
▶ Amazon S3	CreateAccessGrantsInstance	accessgrantsinstance	▪	● allowed 1 matching statements.
▶ Amazon S3	CreateAccessGrantsLocation	accessgrantsinstance	▪	● allowed 1 matching statements.
▶ Amazon S3	CreateAccessPoint	accesspoint	▪	● allowed 1 matching statements.
▶ Amazon S3	CreateAccessPointForObjectL...	objectlambdaaccesssp...	▪	● allowed 1 matching statements.
▶ Amazon S3	CreateBucket	bucket	▪	● allowed 1 matching statements.
▶ Amazon S3	CreateJob	not required	▪	● allowed 1 matching statements.
▶ Amazon S3	CreateMultiRegionAccessPoint	multiregionaccesspoint	▪	● allowed 1 matching statements.
▶ Amazon S3	CreateStorageLensGroup	not required	▪	● allowed 1 matching statements.
▶ Amazon S3	DeleteAccessGrant	accessgrant	▪	● allowed 1 matching statements.
▶ Amazon S3	DeleteAccessGrantsInstance	accessgrantsinstance	▪	● allowed 1 matching statements.
▶ Amazon S3	DeleteAccessGrantsInstanceR...	accessgrantsinstance	▪	● allowed 1 matching statements.
▶ Amazon S3	DeleteAccessGrantsLocation	accessgrantslocation	▪	● allowed 1 matching statements.

The IAM policy simulator is a testing environment that may not model all of the factors present in your production environment, so we cannot guarantee the accuracy of the results. Authorization results in your production environment may differ from what's shown in the IAM policy simulator therefore we recommend testing your policies with production IAM users and AWS requests.

© 2013, Amazon Web Services, Inc. or its affiliates. All rights reserved.

An [amazon.com](#) company

Nous ajoutons ensuite la politique d'autorisation `AmazonEC2ReadOnlyAccess` à l'utilisateur `test-user-1`.

**Ajouter des autorisations**

Ajouter un utilisateur à un groupe existant ou en créer un nouveau. L'utilisation de groupes est une bonne pratique pour gérer les autorisations des utilisateurs par fonctions de tâche. [En savoir plus](#)

**Options d'autorisations**

Ajouter un utilisateur à un groupe  
Ajouter un utilisateur à un groupe existant ou créer un nouveau groupe. Nous vous recommandons d'utiliser des groupes pour gérer les autorisations utilisateur par fonction de tâche.

Copier les autorisations  
Copier toutes les appartenances à un groupe, les politiques gérées attachées, les politiques en ligne et toutes les limites d'autorisations existantes à partir d'un utilisateur existant.

Attacher directement des politiques  
Attacher une politique gérée directement à un utilisateur. La bonne pratique consiste à attacher des politiques à un groupe à la place. Ensuite, ajouter l'utilisateur au groupe approprié.

**Politiques des autorisations (1/1253)**

Filtrer par Type	Type	Entités attachées
<input type="text" value="ec2re"/> X Tous les types	1 correspondance	< 1 > ⚙
<input checked="" type="checkbox"/> Nom de la politique <a href="#">?</a>	▲ Type	▼ Entités attachées
<input checked="" type="checkbox"/> <a href="#">AmazonEC2ReadOnlyAccess</a>	Gérées par AWS	0

Annuler **Suivant**

Nous pouvons constater que notre utilisateur a bien une nouvelle politique d'autorisation.

The screenshot shows the AWS Identity and Access Management (IAM) console. On the left, there's a sidebar with navigation links like 'Tableau de bord', 'Gestion des accès', 'Utilisateurs', and 'Rapports d'accès'. The main area displays a summary for a user named 'test-user-1'. Key details include:

- ARN:** arn:aws:iam::794038237731:user/test-user-1
- Accès par console:** Activé sans l'authentification MFA
- Dernière connexion à la console:** Aujourd'hui
- Clé d'accès 1:** Créer une clé d'accès

Below this, the 'Autorisations' tab is selected, showing two attached policies:

Nom de la politique	Type	Attaché via
AmazonEC2ReadOnlyAccess	Gérées par AWS	Directement
S3FullAccess	Client en ligne	En ligne

There are sections for 'Limites d'autorisations' (not defined), 'Générer une politique basée sur les événements CloudTrail' (with a note about CloudTrail events), and a message stating no policies have been generated in the last 7 days.

Nous retournons ensuite sur le IAM Policy Simulator et testons les politiques avec notre utilisateur `test-user-1` et `Amazon EC2`.

**IAM Policy Simulator**

Policies
Back
Create New Policy

Selected user: test-user-1

**IAM Policies**


- S3FullAccess
- AmazonEC2ReadOnlyAccess

**Custom IAM Policies**

There are no policies to display!

**Permissions Boundary Policy**

You can simulate a maximum of one permissions boundary policy per user or role.  
There are no policies to display!

**Custom IAM Permissions Boundary Policy**

There are no policies to display!

**Resource Policies**

**Policy Simulator**

Amazon EC2    653 Action(s) se...    Select All    Deselect All    Reset Contexts    Clear Results    Run Simulation

▶ Global Settings ⓘ

Action Settings and Results [653 actions selected, 0 actions not simulated, 157 actions allowed, 496 actions denied.]

Service	Action	Resource Type	Simulation Resource	Permission
Amazon EC2	DeregisterImage	image	*	denied Implicitly denied (no matching st...)
Amazon EC2	DeregisterInstanceEventNotific...	not required	*	denied Implicitly denied (no matching st...)
Amazon EC2	DeregisterTransitGatewayMulti...	not required	*	denied Implicitly denied (no matching st...)
Amazon EC2	DeregisterTransitGatewayMulti...	not required	*	denied Implicitly denied (no matching st...)
Amazon EC2	DescribeAccountAttributes	not required	*	allowed 1 matching statements.
Amazon EC2	DescribeAddressTransfers	not required	*	allowed 1 matching statements.
Amazon EC2	DescribeAddresses	not required	*	allowed 1 matching statements.
Amazon EC2	DescribeAddressesAttribute	not required	*	allowed 1 matching statements.
Amazon EC2	DescribeAggregateIdFormat	not required	*	allowed 1 matching statements.
Amazon EC2	DescribeAvailabilityZones	not required	*	allowed 1 matching statements.
Amazon EC2	DescribeAwsNetworkPerforma...	not required	*	allowed 1 matching statements.
Amazon EC2	DescribeBundleTasks	not required	*	allowed 1 matching statements.
Amazon EC2	DescribeByIpCidrs	not required	*	allowed 1 matching statements.
Amazon EC2	DescribeCapacityBlockOfferings	not required	*	allowed 1 matching statements.
Amazon EC2	DescribeCapacityReservationB...	not required	*	allowed 1 matching statements.

The IAM policy simulator is a testing environment that may not model all of the factors present in your production environment, so we cannot guarantee the accuracy of the results. Authorization results in your production environment may differ from what's shown in the IAM policy simulator therefore we recommend testing your policies with production IAM users and AWS requests.

© 2013, Amazon Web Services, Inc. or its affiliates. All rights reserved.

An [amazon.com](#) company

Nous finissons ce TP en supprimant notre utilisateur `test-user-1`.

The screenshot shows the AWS IAM console interface. On the left, there's a sidebar with navigation links like 'Tableau de bord', 'Gestion des accès', 'Utilisateurs', 'Rôles', 'Politiques', 'Fournisseurs d'identité', and 'Paramètres du compte'. The main area shows a list of users under 'Utilisateurs (1/1)'. A modal window titled 'Supprimer test-user-1 ?' is open, asking if the user wants to permanently delete the user. It displays the user's name and last activity ('Il y a 16 minutes'). A note at the bottom says: 'Remarque : les activités récentes apparaissent généralement sous quatre heures. Les données sont stockées pendant 365 jours maximum, en fonction du moment où votre région a commencé à prendre en charge cette fonctionnalité.' Below the note is a text input field containing 'test-user-1'. At the bottom of the modal are two buttons: 'Annuler' and 'Supprimer l'utilisateur'.

Nous constatons que notre politique `S3FullAccess` a bien été supprimée.

The screenshot shows the AWS Identity and Access Management (IAM) service interface. On the left, there's a navigation sidebar with sections like 'Tableau de bord', 'Gestion des accès', 'Rapports d'accès', and 'Consoles connexes'. The main content area is titled 'Politiques (1251) Infos' and shows a single result for 'AmazonS3FullAccess'. The result table includes columns for 'Nom de la politique', 'Type', 'Utilisé comme', and 'Description'. A search bar at the top has 's3f' entered. The bottom of the screen features a footer with links for CloudShell, Commentaires, and various AWS terms like Confidentialité, Conditions, and Préférences relatives aux cookies.

Nom de la politique	Type	Utilisé comme	Description
AmazonS3FullAccess	Gérées par AWS	Aucun	Provides full access to all buckets via t...