

# Rendu TP02

Ce TP a été réalisé par Thomas PEUGNET.

## Sécurisation du compte AWS

Nous configurons une Alert Preference.

Nous mettons à jour la politique par défaut.

The screenshot shows the 'Edit password policy' configuration page in the AWS IAM console. The 'Custom' option is selected, indicating customized password requirements. The 'Password minimum length' is set to 14 characters. Under 'Password strength', four requirements are checked: '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', and 'Require at least one non-alphanumeric character (! @ # \$ % ^ & \* () \_ + - = [ ] { } | )'. Under 'Other requirements', 'Turn on password expiration' is unchecked. The page includes 'Cancel' and 'Save changes' buttons at the bottom.

Nous créons un budget mensuel de 5\$.

**Billing and Cost Management**

**Templates - new**  
Choose a template that best matches your use case.

- Zero spend budget  
Create a budget that notifies you once your spending exceeds \$0.01 which is above the AWS Free Tier limits.
- Monthly cost budget  
Create a monthly budget that notifies you if you exceed, or are forecasted to exceed, the budget amount.
- Daily Savings Plans coverage budget  
Create a coverage budget for your Savings Plans that notifies you when you fall below the defined target.
- Daily reservation utilization budget  
Create a utilization budget for your reservations that notifies you when you fall below the defined target.

**Monthly cost budget - Template**

**Budget name**  
Provide a descriptive name for this budget.

Names must be between 1-100 characters.

**Enter your budgeted amount (\$)**  
Last month's cost:

**Email recipients**  
Specify the email recipients you want to notify when the threshold has exceeded.

Maximum number of email recipients is 10.

**Scope**  
All AWS services are in scope in this budget.

**Notes**  
You will be notified when 1) your **actual spend** reaches 85% 2) your **actual spend** reaches 100% 3) if your **forecasted spend** is expected to reach 100%.

**Template settings**

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Nous activons l'accès des utilisateurs IAM aux informations de facturation.

**Bills**  
**Payments**  
**Credits**  
**Purchase Orders**

**Cost Analysis**  
Cost Explorer  
Cost Explorer Saved Reports  
Cost Anomaly Detection  
Free Tier  
Data Exports

**Cost Organization**  
Cost Categories  
Cost Allocation Tags  
Billing Conductor

**Budgets and Planning**  
**Budgets**  
Budgets Reports  
Pricing Calculator

**Savings and Commitments**  
Cost Optimization Hub

► **Savings Plans**  
► **Reservations**

**Preferences and Settings**  
Payment Preferences  
Billing Preferences  
Cost Management Preferences  
Tax Settings

**Introducing the new AWS account page experience**  
We've redesigned the AWS account page. Let us know what you think.

**IAM user and role access to Billing information** [Info](#)

Activate IAM Access

**Reserved instance marketplace settings**

The Reserved Instance Marketplace gives you the flexibility to sell the remaining full months on your Reserved Instances. Manage your Reserved Instance Marketplace disbursement and tax information using the following options.

**Manage seller and bank account information**  
You can update your business name and bank account information so we can disburse funds to the appropriate location.

**Manage tax settings**  
Change your tax information so that your 1099K or W-8BEN is generated appropriately. Setting this information up also allows you to sell more than 200 transactions or \$20,000 in Reserved Instances.

**Account Contract Information** [Info](#)

Service public sector customer  
 Deactivated

**Other settings**

To update your payment currency, go to [Payment preferences](#).

To manage your communication preferences, see [Communication preferences](#).

To manage your AWS Support plans, see [Support plans](#).

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Nous ajoutons un groupe **facturation** et nous le rattachons aux permissions **Billing**.

**Create user group**

**Name the group**

User group name  
Enter a meaningful name to identify this group.  
**facturation**

**Add users to the group - Optional (0) 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.

**Attach permissions policies - Optional (1/966) 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.

Policy name	Type	Used as	Description
AWSBillingConductorFullAccess	AWS managed	None	Use the AWSBillingConductorFullAccess...
AWSBillingConductorReadOnly...	AWS managed	None	Use the AWSBillingConductorReadOnl...
AWSBillingReadOnlyAccess	AWS managed	None	Allows users to view bills on the Billing...
<b>Billing</b>	AWS managed - job function	None	Grants permissions for billing and cost...

**Create user group**

Nous créons un utilisateur **Mathias** et le mettons dans le groupe **facturation**.

**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**

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.

**Create user**

Nous activons l'accès console pour notre utilisateur.

**Manage console access**

- Disable console access
- Reset password

Console password

- Autogenerated password
- Custom password

\*\*\*\*\*

User must create new password at next sign-in

Revoke active console sessions

Cancel    Reset password

Nous créons un utilisateur `thomaspeu`, l'attachons à la politique `AdminAccess` et lui activons son accès console.

**Review and create**

Step 1  
Specify user details

Step 2  
Set permissions

Step 3  
Review and create

**User details**

User name thomaspeu	Console password type None	Require password reset No
------------------------	-------------------------------	------------------------------

**Permissions summary**

Name	Type	Used as
AdministratorAccess	AWS managed - job function	Permissions policy

**Tags - optional**

No tags associated with the resource.

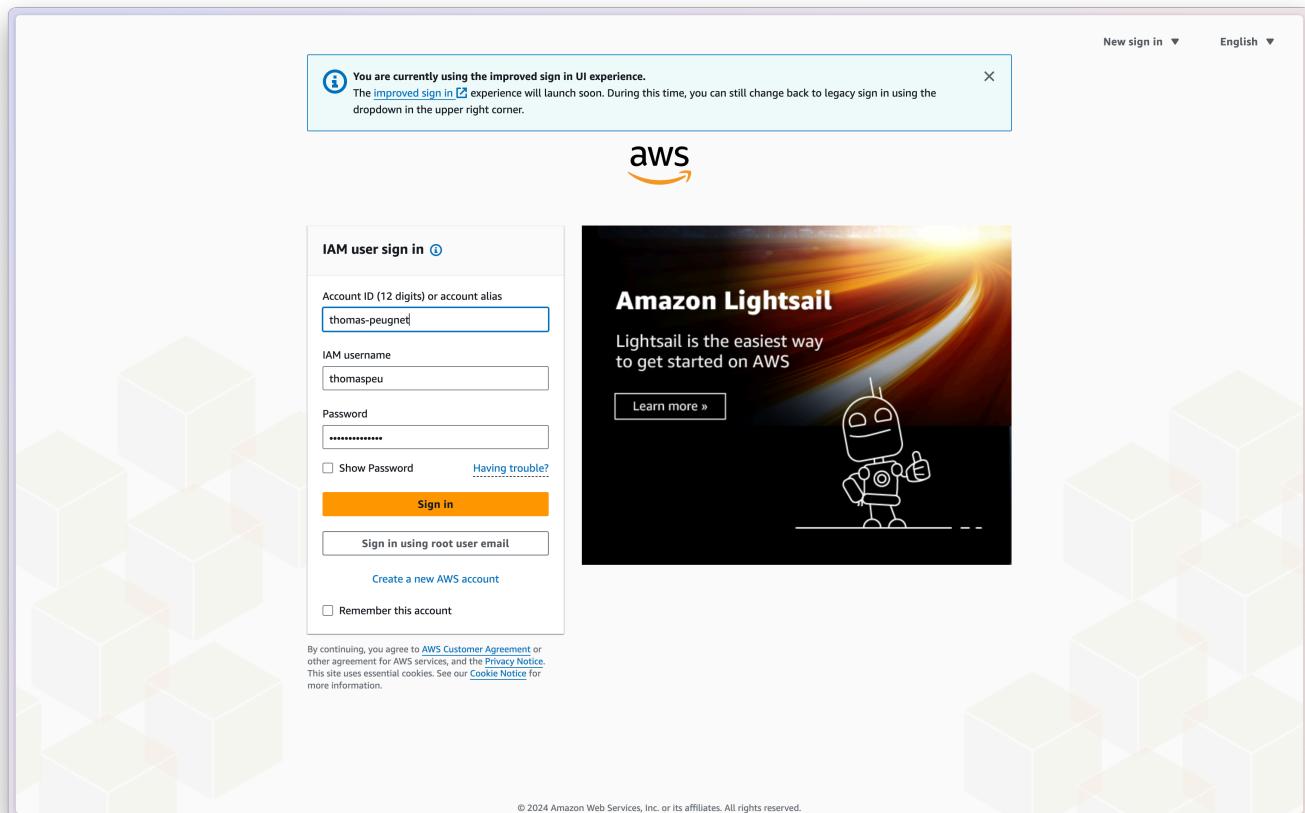
Add new tag

Cancel    Previous    Create user

Nous activons l'utilisation de la MFA pour cet utilisateur et nous reconnectons avec ce dernier.

Nous pouvons constater que nous avons bien toutes les permissions nécessaires.

Nous créons un alias `thomas-peugnet` pour notre compte AWS et nous reconnectons.



Nous créons le groupe `Admin` et y ajoutons notre utilisateur.

A screenshot of the AWS IAM User Groups page. The left sidebar shows navigation options like Dashboard, Access management (User groups selected), Roles, Policies, Identity providers, Account settings, Access reports, and Related consoles. The main content area shows a summary for the "Admin" group, which has one user added: "thomaspeu". The "Users" tab is selected, showing the user's ARN: "arn:aws:iam::794038237751:group/Admin". Below this is a table titled "Users in this group (1)". The table has columns for "User name" (thomaspeu), "Groups" (Admin), "Last activity" (5 minutes ago), and "Creation time" (10 minutes ago). There are buttons for "Search", "Remove", and "Add users".

Nous créons maintenant une politique pour rester dans le Free Tier qui aura le JSON suivant. Son objectif est d'interdire le lancement des VM si elles ne sont pas dans la région de Paris.

```
{  
    "Version": "2012-10-17",  
    "Statement": [  
        {  
            "Effect": "Deny",  
            "Action": "ec2:RunInstances",  
            "Resource": "*",  
            "Condition": {  
                "StringNotEquals": {  
                    "aws:RequestedRegion": "eu-west-3"  
                }  
            }  
        }  
    ]  
}
```

The screenshot shows the 'Review and create' step of an IAM policy creation process. The policy name is 'allow-only-paris-region'. The 'Permissions defined in this policy' section shows one explicit deny statement for the EC2 service, limiting write access to all resources in regions other than 'eu-west-3'. The 'Add tags - optional' section indicates no tags are associated with the resource.

Nous attachons cette nouvelle politique `allow-only-paris-region` à notre groupe `Admin`.

**Identity and Access Management (IAM)**

**Admin**

**Summary**

User group name: Admin | Creation time: November 13, 2024, 11:45 (UTC+01:00) | ARN: arn:aws:iam::794038237731:group/Admin

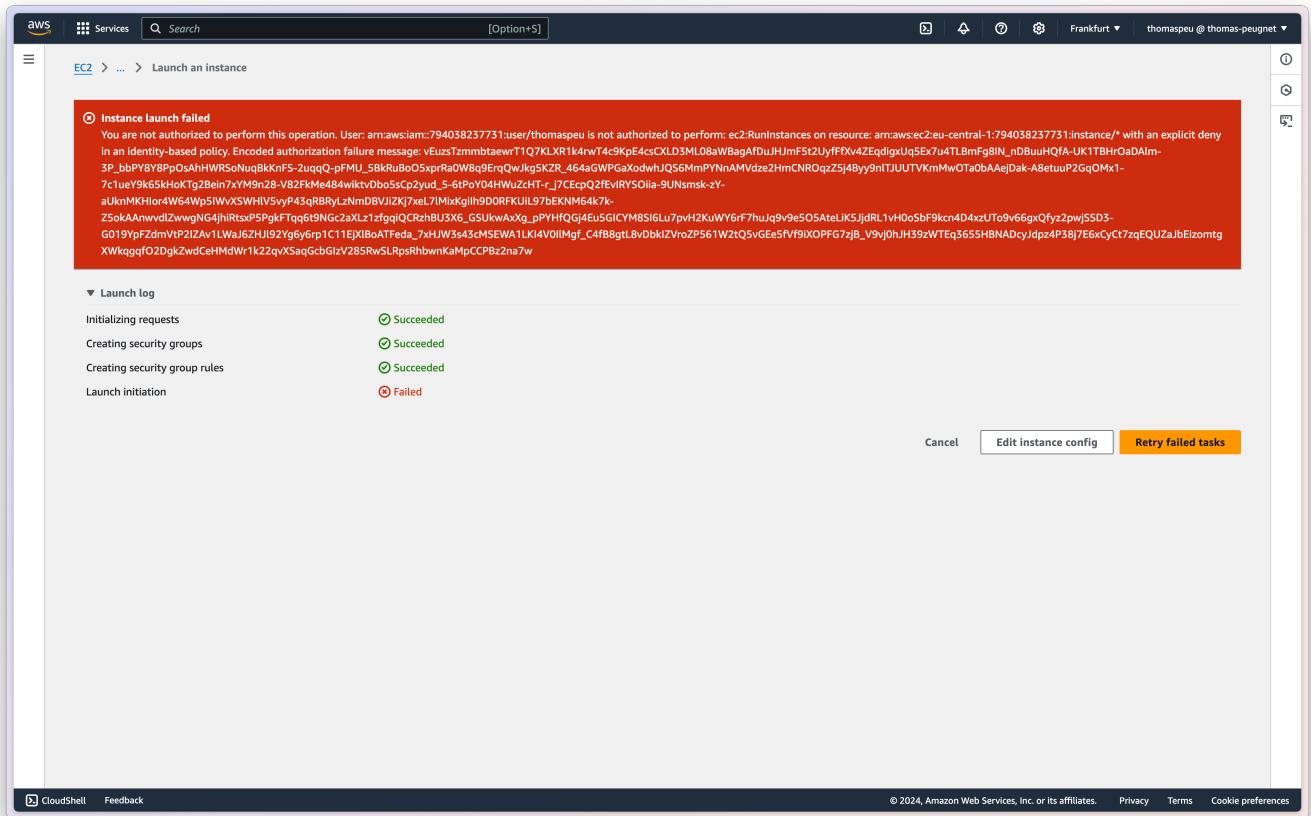
**Permissions**

AdministratorAccess (AWS managed - job function) | allow-only-paris-region (Customer managed)

Nous testons de lancer une instance `t2.micro` hors de France (Frankfurt).

```
function helloWorld(event, context) {
    console.log("Hello from Lambda");
}
```

Comme prévu, nous avons un message d'erreur.



Nous créons ensuite la politique `allow-only-t2-micro` ayant pour objectif d'interdire le lancement de VM différentes du type `t2.micro`. Cette politique aura le JSON suivant:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "ec2:RunInstances",
      "Resource": "*",
      "Condition": {
        "StringNotEquals": {
          "ec2:InstanceType": "t2.micro"
        }
      }
    }
  ]
}
```

Nous associons cette nouvelle politique à notre groupe `Admin`.

Policies attached to this user group.

**Admin** Info

**Summary** Edit

User group name: Admin | Creation time: November 13, 2024, 11:45 (UTC+01:00) | ARN: arn:aws:iam::794038237731:group/Admin

**Permissions** Users (1) Last Accessed

**Permissions policies (3) Info**

You can attach up to 10 managed policies.

Policy name	Type	Attached entities
AdministratorAccess	AWS managed - job function	2
allow-only-paris-region	Customer managed	1
allow-only-t2-micro	Customer managed	1

Nous testons notre politique avec le lancement d'une instance t2.micro en se situant dans la région Paris.

Key pair name - required

Select Create new key pair

**Summary**

Number of instances: 1

Software Image (AMI): Amazon Linux 2023 AMI 2023.6.2... read more

Virtual server type (instance type): t2.micro

**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.

Create new key pair  Proceed without key pair

**Launch Instance**

100 GB of bandwidth to the internet.

**Configure storage**

1x 8 GiB gp3 Root volume (Not encrypted)

Nous obtenons, comme prévu, un message d'erreur.

**Instance launch failed**

You are not authorized to perform this operation. User: arn:aws:iam::794038237731:user/thomaspeu is not authorized to perform: ec2:RunInstances on resource: arn:aws:ec2:eu-west-3:794038237731:network-interface/\* with an explicit deny in an identity-based policy. Encoded authorization failure message: laoswb7ZWD-Geb\_A5bVdCgMzZW3Nir944WBQkpACdmMQdBRQpzDJO1yQY\_oZ38mrmSkfFG9Xqlpk23pWIOqO8JnVKRzmlaJzAyyHvM0o\_7ZDFueloVCJT9aoT4HfDM57M3MG2o4JmbxOzaBAHTSAr3VrjqyPv3y7X\_Sl030-ZxPtCARc1GLBQ6wVtommEcgHusJRYuetylNWEe27rzRZpbCae0n4h1GvJ7m57asdlQU2KX4TQQz5dOaxU2lILO-CfRmSqe8ou-XP1vHQJ3-cNOKdxSillMo9FNKVifZsh975VJLbzkh\_IkkTBfuhL5XsnkpaGjr59DsSPeTNHOrYjyNM0jKBT4X5cqHw7po3CILskdU0F1mB4hlpozig75hTAwwDxYn3\_uZyhTlyz10UJ\_52mrvpJiYPYqViW5wObLYWT5WD3wm59YHZP230LgXk3lyUIHCgH6XY4GWaQpzip5MKQUXLaxiSEFsAx07\_VcbijQZyhxz\_x0AchmTW\_OPvZ-Uj-8mu4E2XqmWCgUr1YANNNHHRo6GKZGSwvnyO\_-h8CtEhoyO2d4Mj7WSR\_pt2n2ZrpISQhCYxvv5CNhDW\_re4NdEYXwci09T6dqy8pDWeKL2PLmsk9ckZarObu4adP2wUnsZim3a-kCH2VswxQQszsKYltAxmBOCXfWxYnERZhzwIZVGQoeMs6cTF6NP82vYuDs8v52SdgvR6OmOuDJF20375Akw73HfGuX1DgjUfcD9KnMeFBqZoq7iytzAHO0MYG3C4

▼ Launch log

Initializing requests	✔ Succeeded
Creating security groups	✔ Succeeded
Creating security group rules	✔ Succeeded
Launch initiation	✖ Failed

Cancel Edit instance config Retry failed tasks

Nous allons maintenant gérer les autorisations AWS en nous basant sur les attributs.

Nous créons une Politique `EC2limitedAccess` avec le JSON suivant:

```
{
  "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:RequesterPrincipal": "arn:aws:iam::794038237731:user/thomaspeu"
        }
      }
    }
  ]
}
```

```

        "aws:PrincipalTag/Department":"EC2Admins",
        "ec2:ResourceTag/Environment":"Production"
    }
}
]
}

```

**Review and create** Info

Review the permissions, specify details, and tags.

**Policy details**

**Policy name**  
Enter a meaningful name to identify this policy.  
**EC2limitedAccess**

**Description - optional**  
Add a short explanation for this policy.

**Permissions defined in this policy** Info

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.

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**

Nous créons ensuite un utilisateur nommé `testABAC` auquel nous assignons la politique `EC2limitedAccess`. Nous assignons également les tags suivant:

- `key` = Department
- `value` = EC2Admins

Screenshot of the AWS IAM 'Create user' wizard - 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	Console password type	Require password reset
testABAC	None	No

**Permissions summary**

Name	Type	Used as
EC2limitedAccess	Customer managed	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.

Key	Value - optional
Department	EC2Admins

**Create user**

Nous lançons ensuite nos 2 instances EC2 avec les tags `Environment:Production` et `Environment:Development`.

**Instances (2) Info**

Last updated less than a minute ago

Find Instance by attribute or tag (case-sensitive)

All states ▾

Instance state = running

Clear filters

	Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4
<input type="checkbox"/>	EC2 test ABAC	i-02649fc0e57a54d5d	<span>Running</span>	t2.micro	<span>2/2 checks passed</span>	<span>View alarms +</span>	eu-west-3c	ec2-51-44-
<input type="checkbox"/>	EC2 test	i-0c85bd07e3e546de0	<span>Running</span>	t2.micro	<span>Initializing</span>	<span>View alarms +</span>	eu-west-3c	ec2-35-180

Nous nous reconnectons avec l'utilisateur `testABAC` et constatons que nous pouvons bien redémarrer l'instance de Production mais pas celle de Développement.

**Failed to reboot the instance i-0c85bd07e3e546de0**

You are not authorized to perform this operation. User: arn:aws:iam::405894864588:user/testABAC is not authorized to perform: ec2:RebootInstances on resource: arn:aws:ec2:eu-west-3:405894864588:instance/i-0c85bd07e3e546de0 because no identity-based policy allows the ec2:RebootInstances action. Encoded authorization failure message: eAgvw4t4J5loNwr\_LMQuERoJAxavJ4Tz4Z0OfyNmfpdvfQgMUX\_iyY14hgfg414Nc35j4ryyMt0fjJM89FnJw4N\_gEPqbqBYZ54TnKpuGlals02x\_f6fZzID27pyL4TQGM-uuF9kwE15kbkjqgYU3eXQ56nh4Bsh26IEGBpmQ3FfmV3YUVGKSzQvulb5Ca7FUW0hHdjPIxuHgvzEq52QumFRr6eaLv7T8k6mjekHSi3z8BSPASkLG9-5DYDCe6BAH7Fs0CUdLAOGNE\_gCgaLCZFrnZKM6telghlW0SKrTGBDXPvKURg8uth608e4cpDo9iowTrFa47cg1wFAEQ9zjTLrhRzzBFdEPxKbPXeQJ\_NmfCTTaRBR9QqvdeHkIBJFTbh9E95fDyfrfrW73AnFx-05CSW9-40XL7HFp8ealegfo2o1aU\_rv7NtomyU2KgFkxFisP6p7wyS1OwsyiMpQyQLIr8cEljuFzTaZOXMmpIjtKB8qbbRVd\_x7X1t7ySSimGXa6\_FOaGwg3d3f4vJsRpJSc88kX9fEbC8RYEIwASHTU2CDj-cMJpfdoobSRZp4M6a8qjwMG\_gzoVBzDEBjQyBxTDGMtfspKXbuVU9\_1nnkTYull85NbOf0CjyPOxVlyoS8vfc346Umy6xEunkdwCAknWdGn0HSZ67W9A4IQShx5dwfRSAMJZjUQr8tRi-U9mWVwza3pK8fTawM\_7FSDCXWxX6jzwHQeceCztQroke3BVgi9ANo0P4xHO6cq68bLfdvas7skO8Seq1ac4scP0baHzaQDRhRiMxN1Sx-Qc8cZGbaZhnY4qVimrodJA9a7\_kAyBDJsdVBOVP16NrNjsvPNW9XX9vYW-1dIB0UoHnanrR2FbHWdfVg

Notifications 0 2 0 1 0 0 0 0

**Instances (1/2) Info**

Last updated 16 minutes ago

Connect

Actions ▾

Launch instances ▾

i-0c85bd07e3e546de0 (EC2 test)