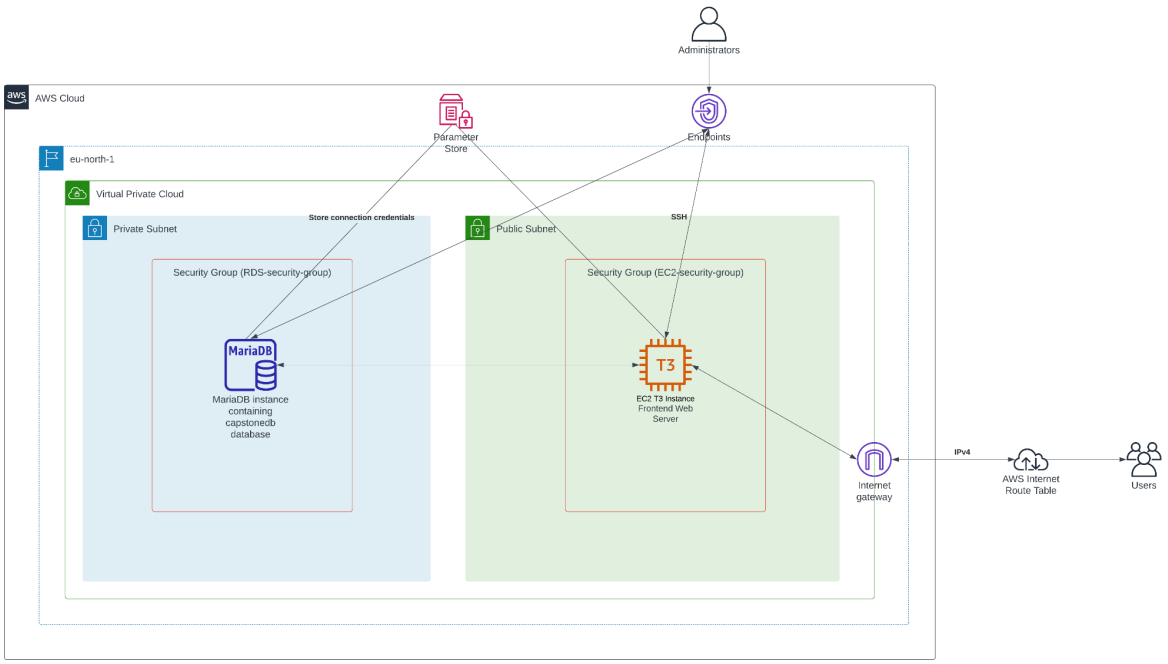
AWS Cloud & Big Data Architectures - Project

https://github.com/pascalito007/efrei-cloud-bigdata/tree/master/capstone-project

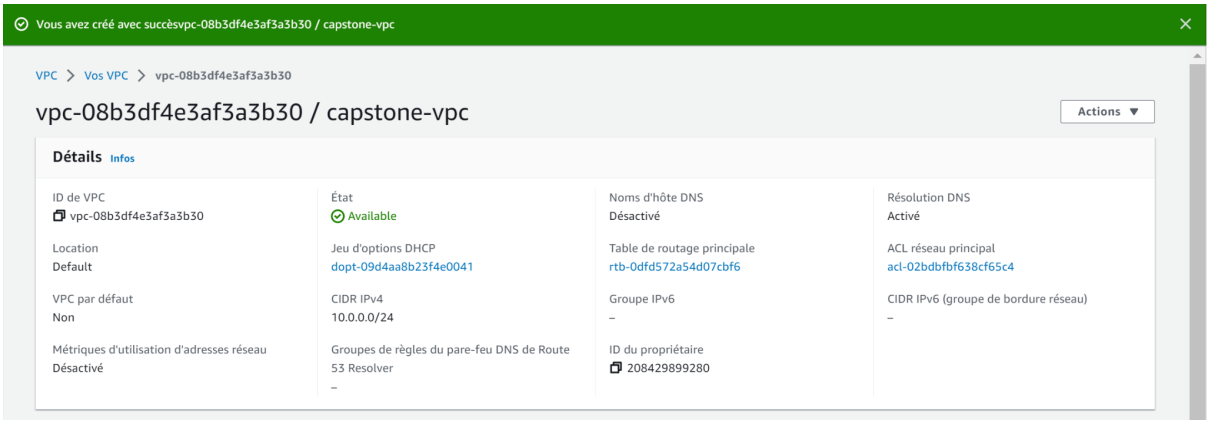
1. Design an Architecture diagram



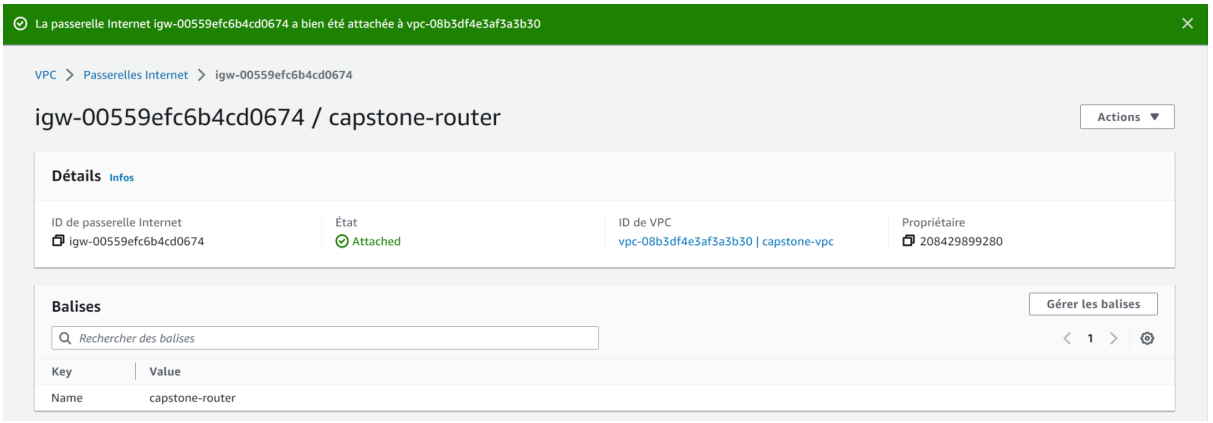
2. App Deployment

Step 1: Create VPC

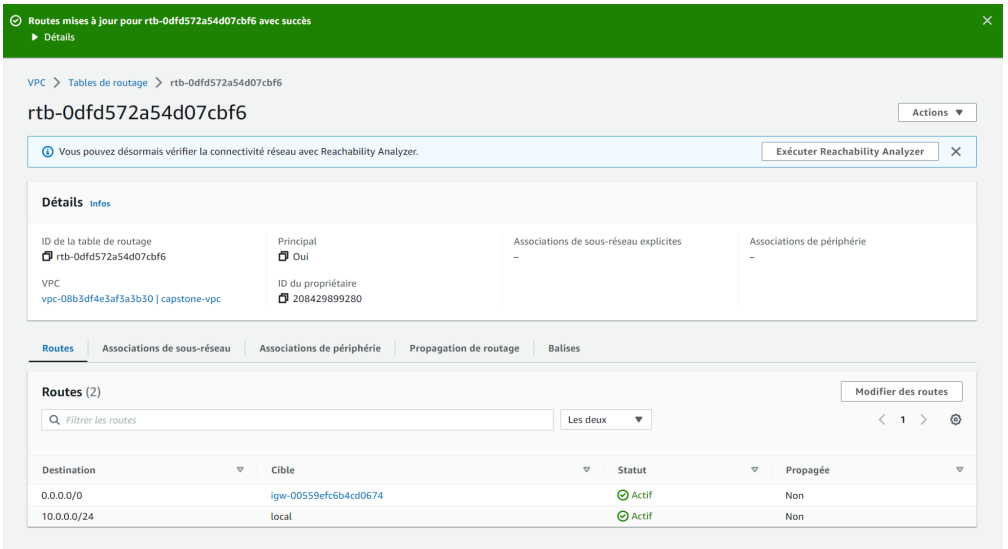
The first step of the app deployment on AWS is to create a Virtual Private Cloud (VPC).



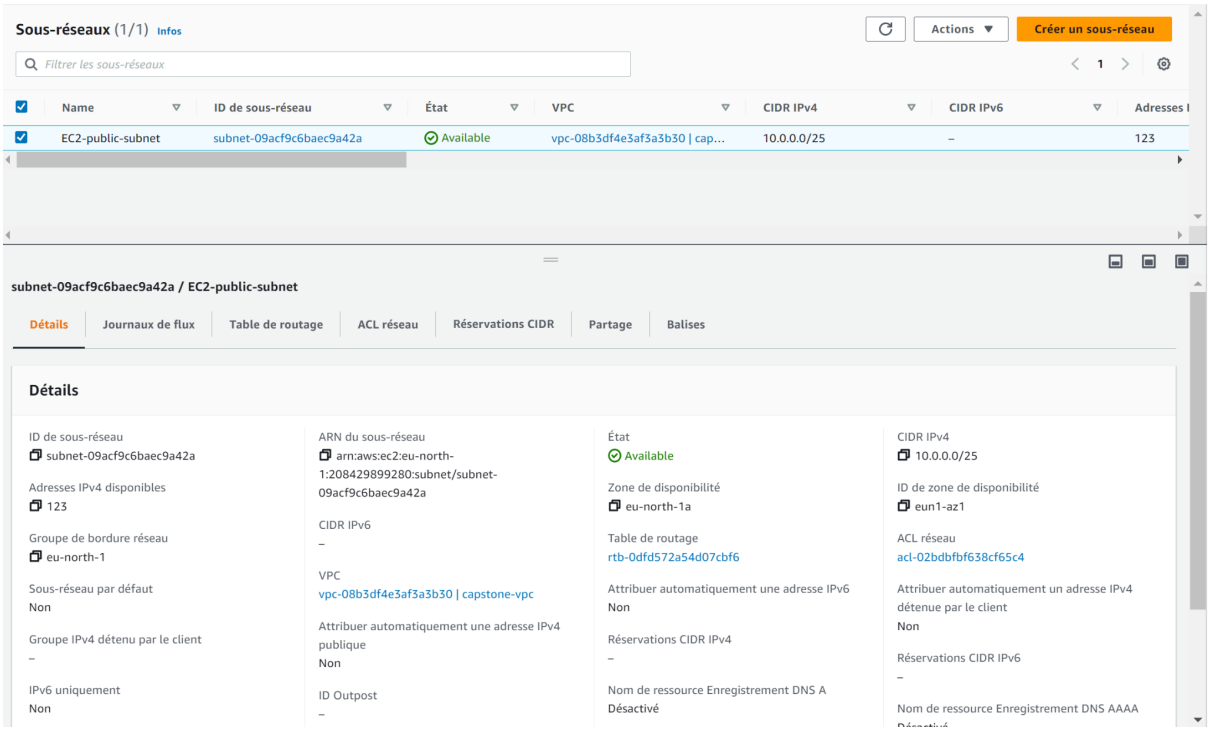
Then, we should connect the VPC to the internet through an internet gateway and attach it to the VPC. The goal is to permit the EC2 instance to connect to the internet.

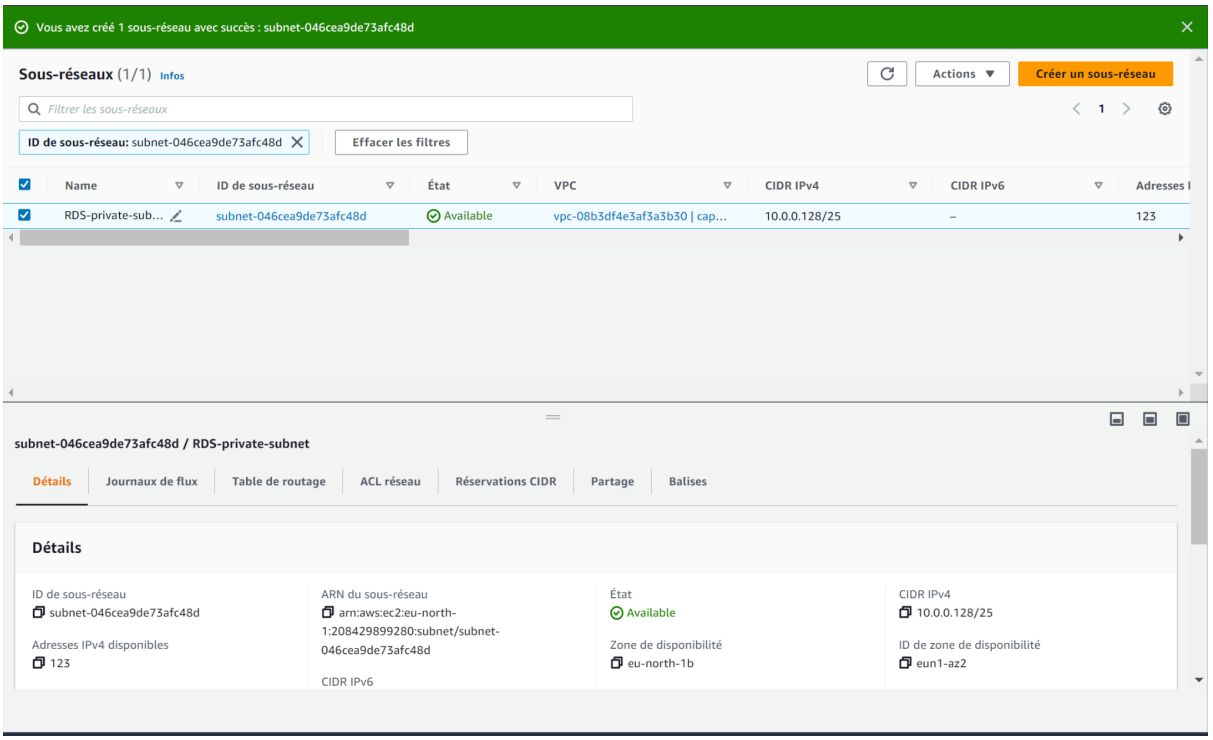


Finally we edit the VPC route table to add a new route toward the new internet gateway:



Step 2: Create 2 subsets, 1 public for EC2 instance and 1 private for RDS DB

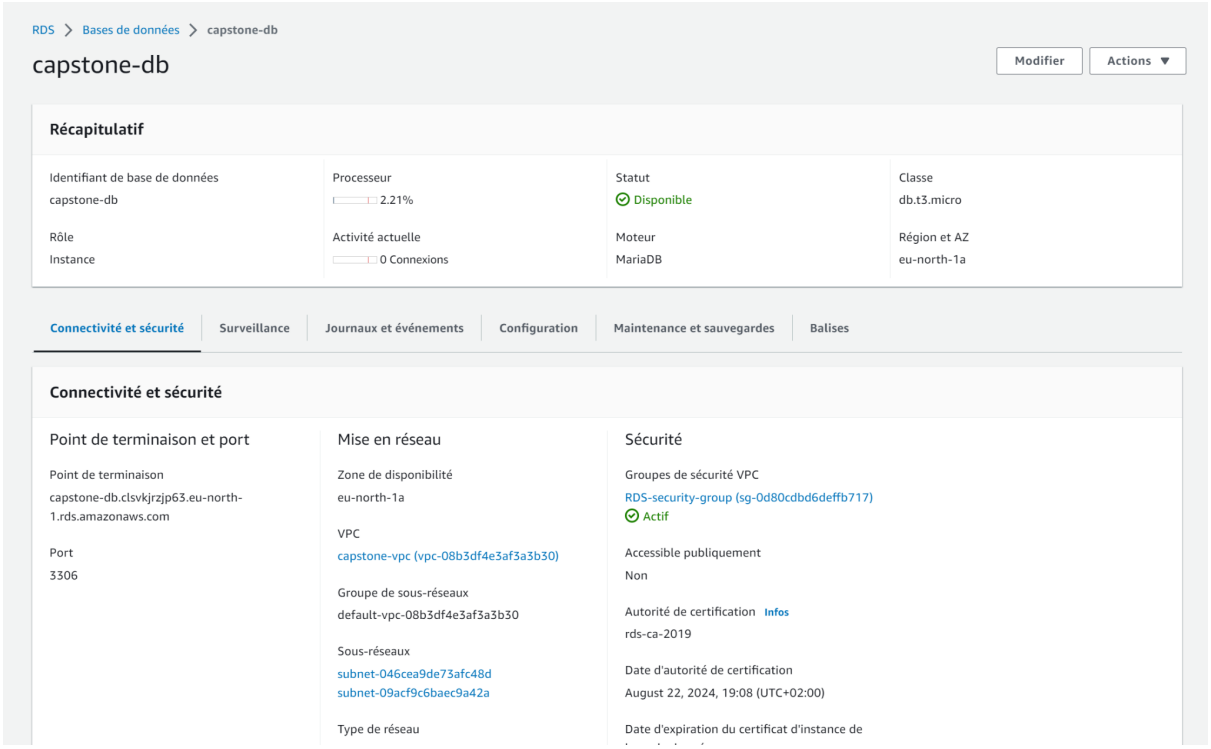




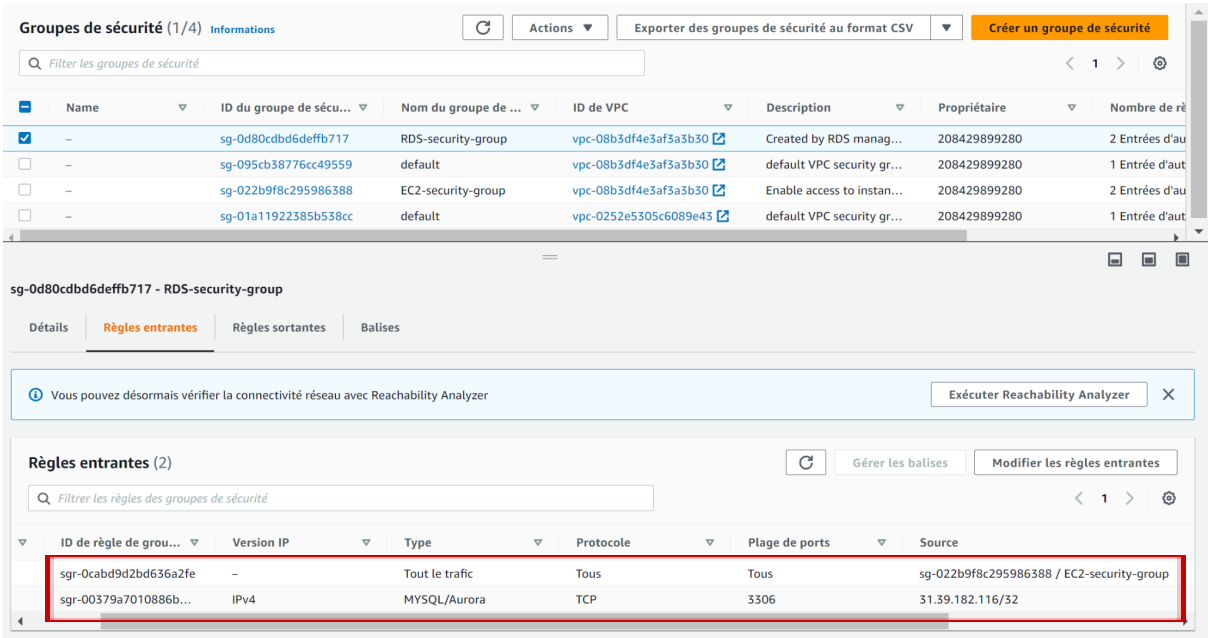
Note: we do not need a NAT gateway because the database does not need to access the internet.

Step 3: Create a private database with RDS

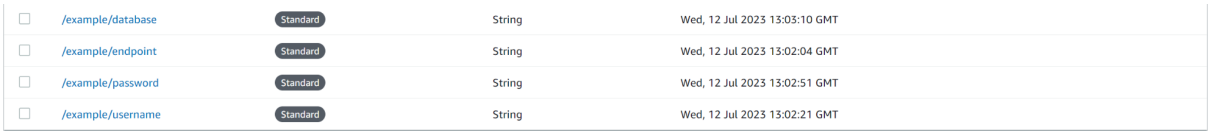
For this step, we chose the MariaDB database.



This database is linked to the capstone VPC, with a specific security group. For this security group, we should add an inbound rule to permit the EC2 instance security group to connect to the RDS database. Thus this rule accepts all traffic if it comes from the EC2 security group.



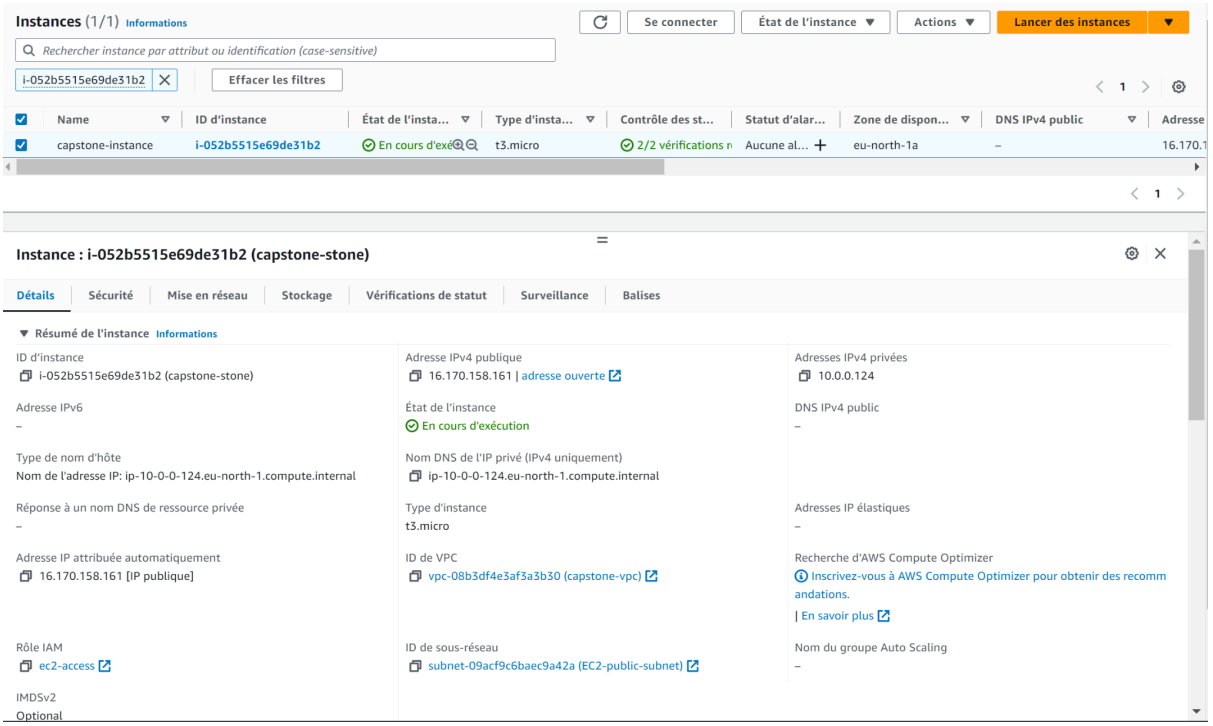
Finally, we store database connection information in the AWS Systems Manager Parameter Store:



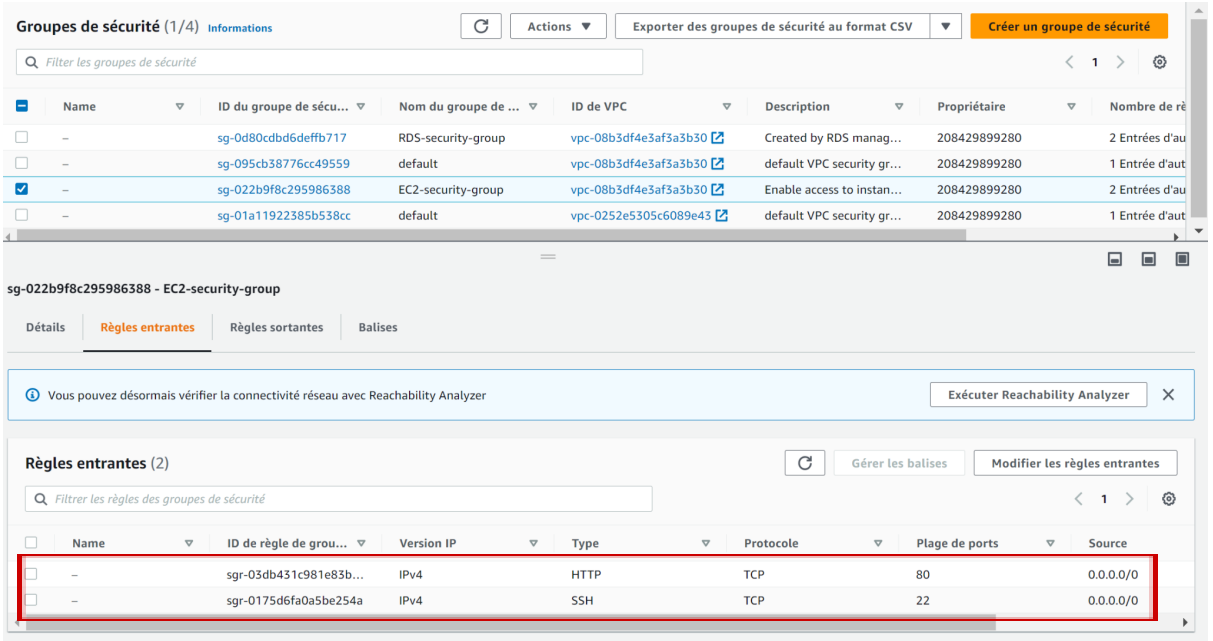
/example/database	Standard	String	Wed, 12 Jul 2023 13:03:10 GMT
/example/endpoint	Standard	String	Wed, 12 Jul 2023 13:02:04 GMT
/example/password	Standard	String	Wed, 12 Jul 2023 13:02:51 GMT
/example/username	Standard	String	Wed, 12 Jul 2023 13:02:21 GMT

Step 4: Create EC2 instance within previous public subnet

This instance is of type t3.micro because t2.micro is not available in the eu-north region. The image used is the one provided in the guidelines: AMI Cloud9AmazonLinux2-2023-06-22T17-21. Finally, it is linked to the created VPC and is attached to the EC2 security group.



The security group used for the EC2 instance is the following. It accepts SSH and HTTP inbound connections from anywhere.



Step 5: Test connections and fill the database

Now that everything is created and configured, the next step is to **test the connection to the public EC2 instance from Git Bash locally**, connect to the database from this instance and fill the database.

When creating the ec2 instance, we have generated a key-value pair (RSA) that we are going to use to ssh into our instance from our local machine. From our terminal we ssh into the instance.

```
justi@DESKTOP-5BE17F3 MINGW64 /c/M1_S8_AWS
$ ssh -i C:/M1_S8_AWS/efrei-capstone.pem ec2-user@16.170.158.161
The authenticity of host '16.170.158.161 (16.170.158.161)' can't be established.
ED25519 key fingerprint is SHA256:ydIkwgmo6LHiVHgUjCkeT3uhLNb2DGbo41Whpi/e8c4.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '16.170.158.161' (ED25519) to the list of known hosts.

       __|  __|_  )
       _|  (     /   Amazon Linux 2 AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-2/
17 package(s) needed for security, out of 19 available
Run "sudo yum update" to apply all updates.
:~ $ sudo -i
[root@ip-10-0-0-124 ~]# yum -y update
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
amzn2-core
244 packages excluded due to repository priority protections
Resolving Dependencies
--> Running transaction check
---> Package glib2.x86_64 0:2.56.1-9.amzn2.0.5 will be updated
---> Package glib2.x86_64 0:2.56.1-9.amzn2.0.6 will be an update
---> Package iputils.x86_64 0:20160308-10.amzn2.0.2 will be updated
---> Package iputils.x86_64 0:20180629-11.amzn2.1.20160308 will be an update
---> Package kernel.x86_64 0:4.14.318-241.531.amzn2 will be installed
---> Package kernel-devel.x86_64 0:4.14.318-241.531.amzn2 will be installed
```

We are well connected, now we can run line by line the script given in the guidelines to install MariaDB features, download files and stock them in the instance.

```
Complete!
[root@ip-10-0-0-124 ~]# amazon-linux-extras install -y lamp-mariadb10.2-php7.2 php7.2
Topic php7.2 has end-of-support date of 2020-11-30
Installing php-pdo, php-mysqlnd, php-fpm, php-cli, php-json, mariadb
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
Cleaning repos: amzn2-core amzn2extra-docker amzn2extra-epel amzn2extra-lamp-mariadb10.2-php7.2 amzn2extra-php7.2 epel hashicorp
33 metadata files removed
11 sqlite files removed
0 metadata files removed
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
amzn2-core                                                                                                                                                | 3.7 kB  00:00:00
amzn2extra-docker                                                                                                                                         | 3.0 kB  00:00:00
amzn2extra-epel                                                                                                                                           | 3.0 kB  00:00:00
amzn2extra-lamp-mariadb10.2-php7.2                                                                                                                        | 3.0 kB  00:00:00
amzn2extra-php7.2                                                                                                                                         | 3.0 kB  00:00:00
epel/x86_64/metalink                                                                                                                                      |  26 kB  00:00:00
epel                                                                                                                                                      | 4.7 kB  00:00:00
hashicorp                                                                                                                                                 | 1.4 kB  00:00:00
(1/15): amzn2-core/2/x86_64/group_gz                                                                                                                      | 2.5 kB  00:00:00
(2/15): amzn2-core/2/x86_64/updateinfo                                                                                                                    | 637 kB  00:00:00
(3/15): amzn2extra-epel/2/x86_64/primary_db                                                                                                               | 1.8 kB  00:00:00
```

```
[root@ip-10-0-0-124 ~]# yum install -y httpd mariadb-server
Loaded plugins: extras_suggestions, langpacks, priorities, update-motd
Existing lock /var/run/yum.pid: another copy is running as pid 29540.
Another app is currently holding the yum lock; waiting for it to exit...
  The other application is: yum
    Memory : 345 M RSS (562 MB VSZ)
    Started: Wed Jul 12 12:09:21 2023 - 00:08 ago
    State  : Running, pid: 29540
Another app is currently holding the yum lock; waiting for it to exit...
  The other application is: yum
    Memory : 345 M RSS (562 MB VSZ)
    Started: Wed Jul 12 12:09:21 2023 - 00:10 ago
    State  : Running, pid: 29540
245 packages excluded due to repository priority protections
Package httpd-2.4.57-1.amzn2.x86_64 already installed and latest version
Resolving Dependencies
--> Running transaction check
---> Package mariadb-server.x86_64 3:10.2.38-1.amzn2.0.1 will be installed
--> Processing Dependency: mariadb-tokudb-engine(x86-64) = 3:10.2.38-1.amzn2.0.1 for package: 3:mariadb-server-10.2.38-1.amzn2.0.1.x86_64
--> Processing Dependency: mariadb-server-utils(x86-64) = 3:10.2.38-1.amzn2.0.1 for package: 3:mariadb-server-10.2.38-1.amzn2.0.1.x86_64
```

```
Complete!
[root@ip-10-0-0-124 ~]# chkconfig httpd on
Note: Forwarding request to 'systemctl enable httpd.service'.
Created symlink from /etc/systemd/system/multi-user.target.wants/httpd.service to /usr/lib/systemd/system/httpd.service.
[root@ip-10-0-0-124 ~]# service httpd start
Redirecting to /bin/systemctl start httpd.service
[root@ip-10-0-0-124 ~]#
[root@ip-10-0-0-124 ~]# cd /home/ec2-user
[root@ip-10-0-0-124 ec2-user]# wget https://aws-tc-largeobjects.s3.us-west-2.amazonaws.com/CUR-TF-200-ACACAD-2/21-course-project/s3/Countrydatadump.sql
--2023-07-12 12:11:04--  https://aws-tc-largeobjects.s3.us-west-2.amazonaws.com/CUR-TF-200-ACACAD-2/21-course-project/s3/Countrydatadump.sql
Resolving aws-tc-largeobjects.s3.us-west-2.amazonaws.com (aws-tc-largeobjects.s3.us-west-2.amazonaws.com)... 52.92.243.2, 3.5.84.169, 52.218.176.169, ...
Connecting to aws-tc-largeobjects.s3.us-west-2.amazonaws.com (aws-tc-largeobjects.s3.us-west-2.amazonaws.com)|52.92.243.2|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 15508 (15K) [application/x-sql]
Saving to: 'Countrydatadump.sql'

100%[=============================================================================================================================================>] 15,508      --.-K/s   in 0s

2023-07-12 12:11:05 (176 MB/s) - 'Countrydatadump.sql' saved [15508/15508]

[root@ip-10-0-0-124 ec2-user]# chown ec2-user:ec2-user Countrydatadump.sql
[root@ip-10-0-0-124 ec2-user]# cd /var/www/html
[root@ip-10-0-0-124 html]# wget https://aws-tc-largeobjects.s3.us-west-2.amazonaws.com/CUR-TF-200-ACACAD-2/21-course-project/s3/Example.zip
--2023-07-12 12:11:42--  https://aws-tc-largeobjects.s3.us-west-2.amazonaws.com/CUR-TF-200-ACACAD-2/21-course-project/s3/Example.zip
Resolving aws-tc-largeobjects.s3.us-west-2.amazonaws.com (aws-tc-largeobjects.s3.us-west-2.amazonaws.com)... 52.218.236.49, 52.92.176.42, 52.92.177.234, ...
Connecting to aws-tc-largeobjects.s3.us-west-2.amazonaws.com (aws-tc-largeobjects.s3.us-west-2.amazonaws.com)|52.218.236.49|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 6359580 (6.1M) [application/zip]
Saving to: 'Example.zip'

100%[=============================================================================================================================================>] 6,359,580   4.81MB/s   in 1.3s

2023-07-12 12:11:44 (4.81 MB/s) - 'Example.zip' saved [6359580/6359580]
```

```
[root@ip-10-0-0-124 html]# unzip Example.zip -d /var/www/html/
Archive:  Example.zip
  inflating: /var/www/html/index.php
  inflating: /var/www/html/gdp.php
  inflating: /var/www/html/Shirley.jpeg
  inflating: /var/www/html/query2.php
  inflating: /var/www/html/query3.php
  inflating: /var/www/html/population.php
  inflating: /var/www/html/lifeexpectancy.php
  inflating: /var/www/html/get-parameters.php
  inflating: /var/www/html/aws.phar
  inflating: /var/www/html/mortality.php
  inflating: /var/www/html/menu.php
  inflating: /var/www/html/Logo.png
 extracting: /var/www/html/style.css
  inflating: /var/www/html/mobile.php
  inflating: /var/www/html/query.php
[root@ip-10-0-0-124 html]# chown -R ec2-user:ec2-user /var/www/html
```

Now that the sql script is saved and that the example files are unzipped in the instance, we connect to the MariaDB database instance and create the database *capstonedb*:

```
[root@ip-10-0-0-124 ec2-user]# mysql -u admin -h capstone-db.clsvkjrzjp63.eu-north-1.rds.amazonaws.com -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 86
Server version: 10.6.10-MariaDB-log managed by https://aws.amazon.com/rds/

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> CREATE DATABASE capstonedb;
Query OK, 1 row affected (0.01 sec)

MariaDB [(none)]> use capstonedb source Countrydatadump.sql
Database changed
```

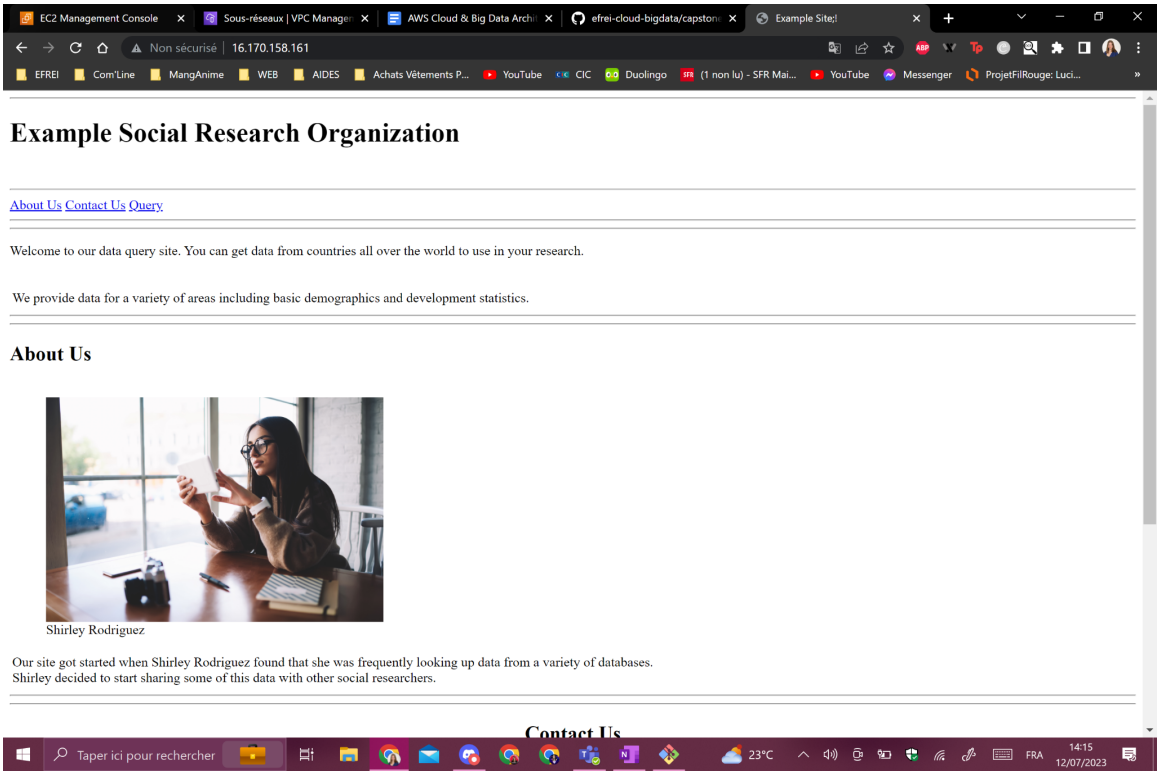
Finally, we execute the sql script file using the previous created database:

```
MariaDB [capstonedb]> source Countrydatadump.sql
Query OK, 0 rows affected (0.00 sec)

Query OK, 0 rows affected (0.00 sec)

Query OK, 0 rows affected (0.00 sec)

Query OK, 0 rows affected (0.00 sec)

Query OK, 0 rows affected (0.00 sec)

Query OK, 0 rows affected (0.00 sec)

Query OK, 0 rows affected (0.00 sec)

Query OK, 0 rows affected (0.00 sec)

Query OK, 0 rows affected (0.00 sec)

Query OK, 0 rows affected (0.00 sec)

Query OK, 0 rows affected (0.01 sec)

Query OK, 0 rows affected (0.00 sec)

Query OK, 0 rows affected (0.00 sec)

Query OK, 0 rows affected (0.01 sec)

Query OK, 0 rows affected (0.00 sec)

Query OK, 0 rows affected (0.00 sec)

Query OK, 0 rows affected (0.00 sec)

Query OK, 214 rows affected (0.01 sec)
Records: 214  Duplicates: 0  Warnings: 0

Query OK, 0 rows affected (0.00 sec)

Query OK, 0 rows affected (0.00 sec)

Query OK, 0 rows affected (0.01 sec)

Query OK, 0 rows affected (0.00 sec)

Query OK, 0 rows affected (0.00 sec)

Query OK, 0 rows affected (0.00 sec)

Query OK, 0 rows affected (0.00 sec)

Query OK, 0 rows affected (0.00 sec)

Query OK, 0 rows affected (0.00 sec)
```

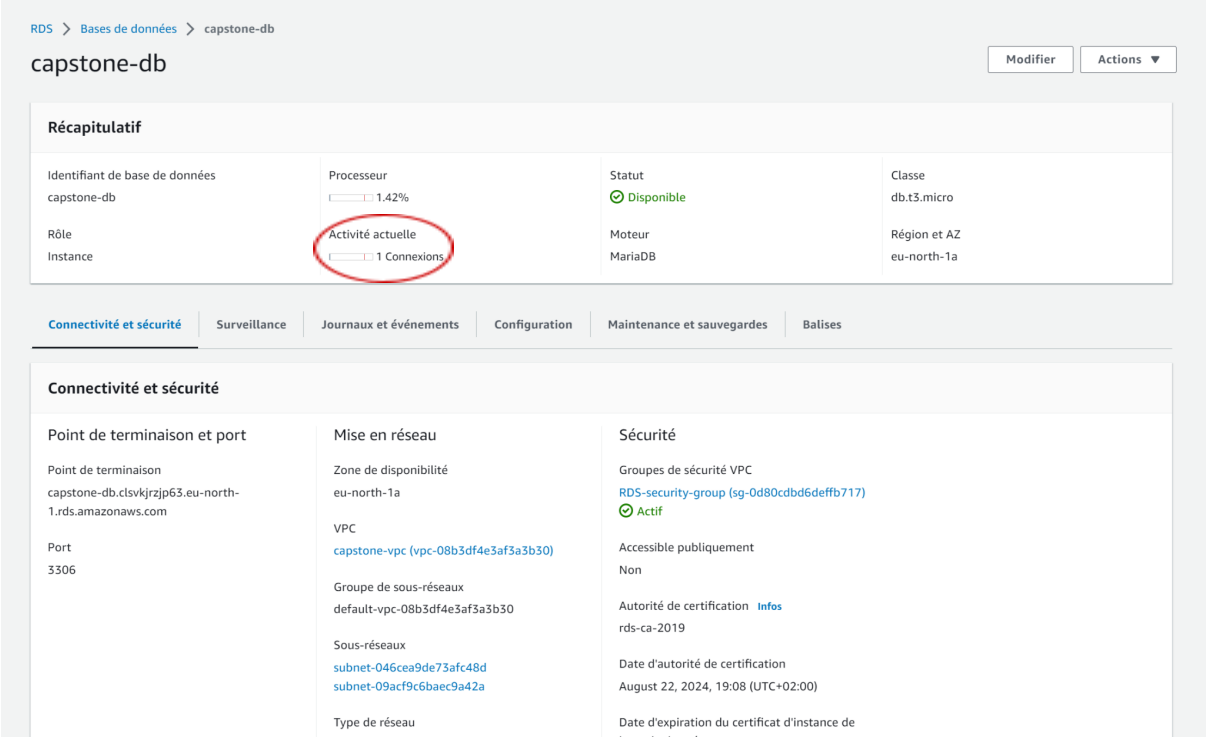
```
MariaDB [capstonedb]> SHOW TABLES;
+----------------------+
| Tables_in_capstonedb |
+----------------------+
| countrydata_final    |
+----------------------+
1 row in set (0.00 sec)
```

The SHOW TABLES query shows that the database is well filled and that the table countrydata_final has been created.

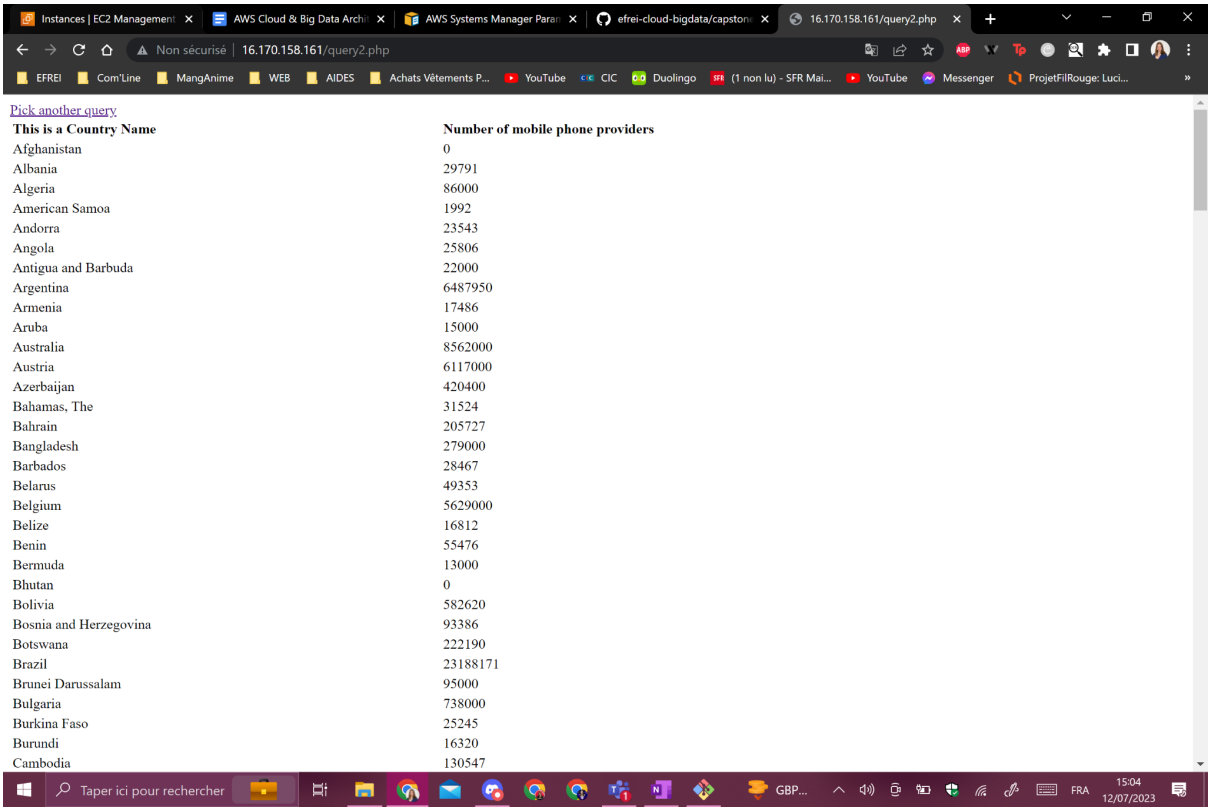
Step 6: Results



We well have access to the website and we can see that the database has a current connection opened:



When we choose and execute a query, we have well the result meaning that the website can connect well to the database and use data:



3. QUIZ

A. IAM QUIZZ

Which statement describes AWS Identity and Access Management (IAM) users?

- IAM users are used to control access to a specific AWS resource.
- IAM user names can represent a collection of individuals.
- Every IAM user for an account must have a unique name.
- Every IAM user name is unique across all AWS accounts.

How can you grant the same level of permissions to multiple users within an account?

- Apply an AWS Identity and Access Management (IAM) policy to an IAM group.
- Apply an AWS Identity and Access Management (IAM) policy to an IAM role.
- Create a resource-based policy.
- Create an organization in AWS Organizations.

Which statements describe AWS Identity and Access Management (IAM) roles? (Select TWO.)

- [ ] They are uniquely associated to an individual.
- [ ] They can only be used by accounts associated to the person who creates the role.
- [x] They can be assumed by individuals, applications, and services.
- [x] They provide temporary security credentials.
- [ ] They provide permanent security credentials.

Which statement describes a resource-based policy?

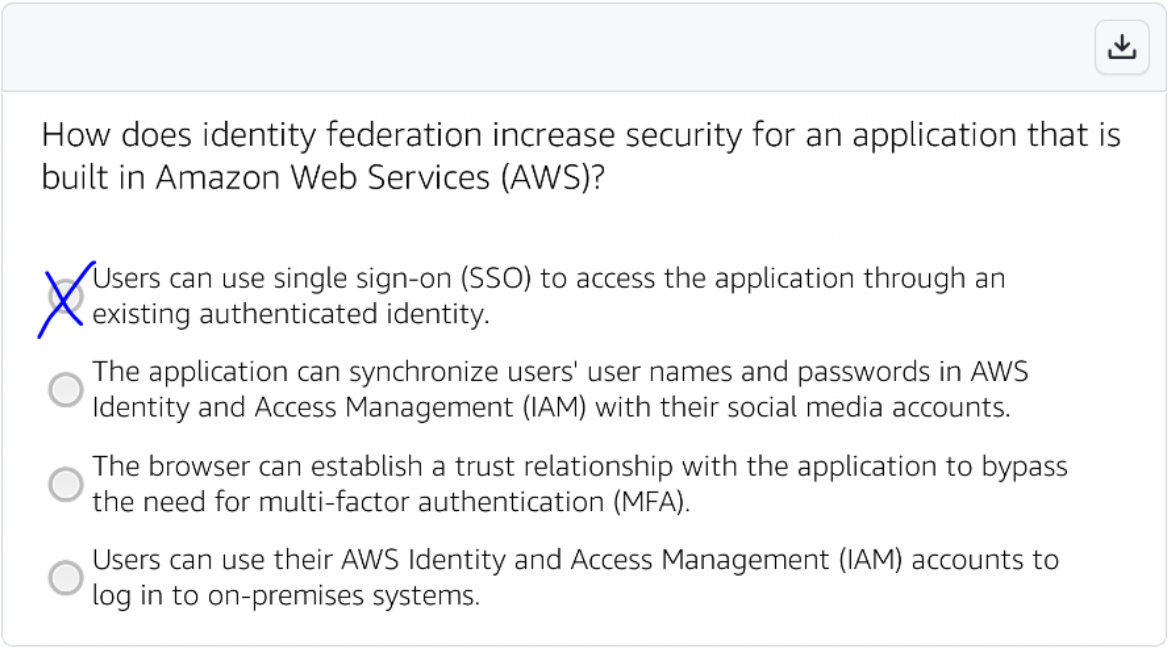
- (x) It can be applied to any AWS resource.
- ( ) It can be an AWS managed policy.
- ( ) It is attached to a user or group.
- ( ) It is always an inline policy.

How does AWS Identity and Access Management (IAM) evaluate a policy?

- It checks for explicit allow statements before it checks for explicit deny statements.
- It checks for explicit deny statements before it checks for explicit allow statements.
- If there is no explicit deny statement or explicit allow statement, users will have access by default.
- An explicit deny statement does not override an explicit allow statement.

A team of developers needs access to several services and resources in a virtual private cloud (VPC) for 9 months. How can you use AWS Identity and Access Management (IAM) to enable access for them?

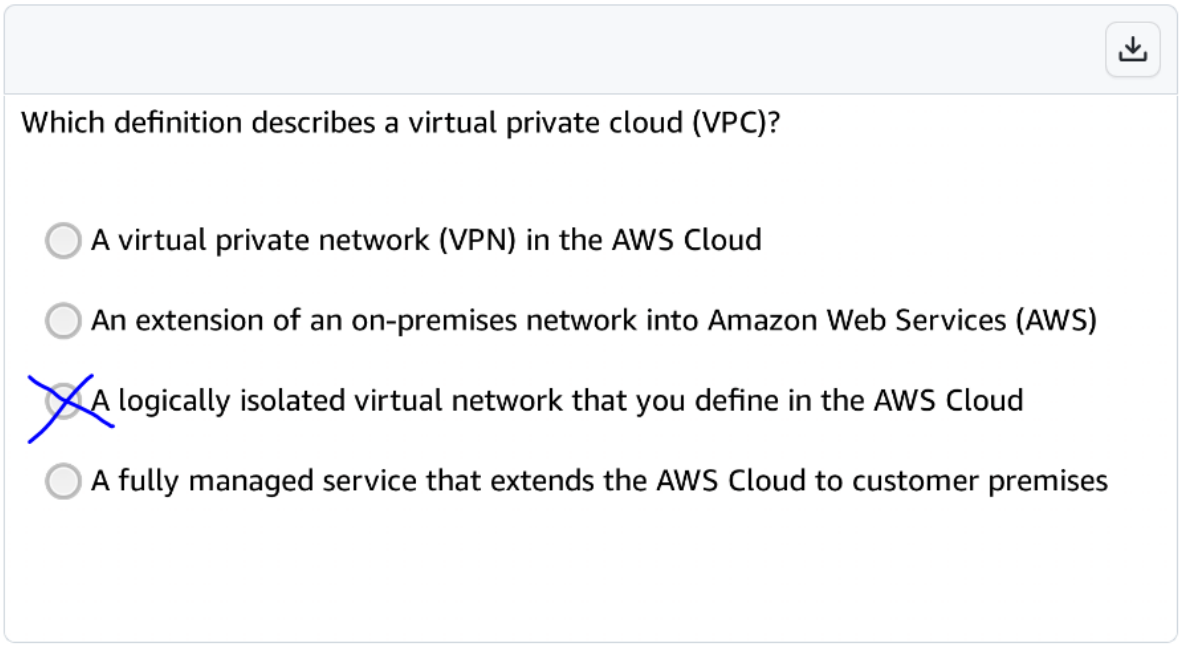
- Create a single IAM user for the developer team and attach the required IAM policies.
- Create an IAM user for each developer, and attach the required IAM policies to each IAM user.
- Create an IAM user for each developer, put them all in an IAM group, and attach the required IAM policies to the IAM group.
- Create a single IAM user for the developer team, place it in an IAM group, and attach the required IAM policies to the IAM group.



How does identity federation increase security for an application that is built in Amazon Web Services (AWS)?

- [x] Users can use single sign-on (SSO) to access the application through an existing authenticated identity.
- [ ] The application can synchronize users' user names and passwords in AWS Identity and Access Management (IAM) with their social media accounts.
- [ ] The browser can establish a trust relationship with the application to bypass the need for multi-factor authentication (MFA).
- [ ] Users can use their AWS Identity and Access Management (IAM) accounts to log in to on-premises systems.

B. NETWORK QUIZZ



Which definition describes a virtual private cloud (VPC)?

- [ ] A virtual private network (VPN) in the AWS Cloud
- [ ] An extension of an on-premises network into Amazon Web Services (AWS)
- [x] A logically isolated virtual network that you define in the AWS Cloud
- [ ] A fully managed service that extends the AWS Cloud to customer premises

187 KB

A company's VPC has the CIDR block 172.16.0.0/21 (2048 addresses). It has two subnets (A and B). Each subnet must support 100 usable addresses now, but this number is expected to rise to at most 254 usable addresses soon. Which subnet addressing scheme meets the requirements and follows AWS best practices?

- Subnet A: 172.16.0.0/25 (128 addresses) Subnet B: 172.16.0.128/25 (1024 addresses)
- Subnet A: 172.16.0.0/25 (128 addresses) Subnet B: 172.16.0.128/25 (128 addresses)
- Subnet A: 172.16.0.0/23 (512 addresses) Subnet B: 172.16.2.0/23 (512 addresses)
- Subnet A: 172.16.0.0/22 (1024 addresses) Subnet B: 172.16.4.0/22 (128 addresses)

Which combination of actions enables direct internet access for IPv4 hosts in a virtual private cloud (VPC)? (Select THREE.)

- [x] Creating a route for 0.0.0.0/0 that points to the internet gateway
- [ ] Enabling Domain Name System (DNS) resolution for the VPC
- [x] Configuring hosts to have or obtain an internet-routable address
- [ ] Configuring the VPC domain name in a Dynamic Host Configuration Protocol (DHCP) options set
- [ ] Creating a default route that points to the virtual private gateway
- [x] Configuring security groups and network access control lists (network ACLs) to permit internet traffic

Several EC2 instances launch in a virtual private cloud (VPC) that has internet access. These instances should not be accessible from the internet, but they must be able to download updates from the internet. How should the instances launch?

- With Elastic IP addresses, in a subnet with a default route to an internet gateway
- With public IP addresses, in a subnet with a default route to an internet gateway
- Without public IP addresses, in a subnet with a default route to an internet gateway
- Without public IP addresses, in a subnet with a default route to a network address translation (NAT) gateway

4. IAM

Policies evaluation

Please evaluate below IAM policies:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowEC2AndS3",
      "Effect": "Allow",
      "Action": [
        "ec2:RunInstances",
        "ec2:TerminateInstances",
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource": [
        "arn:aws:ec2:us-east-1:123456789012:instance/*",
        "arn:aws:s3:::example-bucket/*"
      ]
    }
  ]
}
```

Question 1: What actions are allowed for EC2 instances and S3 objects based on this policy? What specific resources are included?

Based on the provided policy, the following actions are allowed for EC2 instances and S3 objects:

- For EC2 instances:
  - `ec2:RunInstances`: Allowing the launch and execution of EC2 instances.
  - `ec2:TerminateInstances`: Allowing the termination of EC2 instances.

- For S3 objects:
  - `s3:GetObject`: Allowing the retrieval of objects from an S3 bucket.
  - `s3:PutObject`: Allowing the upload of objects to an S3 bucket.

The specific resources included in the policy are:

- All instances located in us-east-1 where account id is 123456789012.
- A specific bucket: named example-bucket. The `*` wildcard signifies all objects within that bucket.

A user who has this policy attached would have the permissions to perform actions such as launching and terminating EC2 instances within the specified region and AWS account. Additionally, they would be able to retrieve and upload objects within the specified S3 bucket.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowVPCAccess",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeVpcs",
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "aws:RequestedRegion": "us-west-2"
        }
      }
    }
  ]
}
```

Question 2: Under what condition does this policy allow access to VPC-related information? Which AWS region is specified?

This policy allows access to VPC-related information under the condition that the requested AWS region is "us-west-2". This condition ensures that the access to VPC-related information is granted only when the requested AWS region matches "us-west-2".

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowS3ReadWrite",
      "Effect": "Allow",
      "Action": ["s3:GetObject", "s3:PutObject", "s3:ListBucket"],
      "Resource": [
        "arn:aws:s3:::example-bucket",
        "arn:aws:s3:::example-bucket/*"
      ],
      "Condition": {
        "StringLike": {
          "s3:prefix": ["documents/*", "images/*"]
        }
      }
    }
  ]
}
```

Question 3: What actions are allowed on the "example-bucket" and its objects based on this policy? What specific prefixes are specified in the condition?

Based on this policy, the following actions are allowed on the "example-bucket" and its objects:

- Retrieve objects from the "example-bucket".
- Upload objects to the "example-bucket".
- List objects within the "example-bucket".

The specific prefixes specified in the condition are:

- *documents/**: This prefix allows the actions specified in the policy (*GetObject*, *PutObject*, *ListBucket*) on objects within the "example-bucket" that have a prefix of "documents/".
- *images/**: This prefix allows the actions specified in the policy (*GetObject*, *PutObject*, *ListBucket*) on objects within the "example-bucket" that have a prefix of "images/".

Nevertheless, this policy only allows the specified actions on objects within the specified prefixes and does not grant any other permissions or access beyond that.

Finally, the policy grants the specified actions on both the "example-bucket" itself (`arn:aws:s3:::example-bucket`) and its objects (`arn:aws:s3:::example-bucket/*`).

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowIAMUserCreation",
      "Effect": "Allow",
      "Action": "iam:CreateUser",
      "Resource": "arn:aws:iam::123456789012:user/${aws:username}"
    },
    {
      "Sid": "AllowIAMUserDeletion",
      "Effect": "Allow",
      "Action": "iam:DeleteUser",
      "Resource": "arn:aws:iam::123456789012:user/${aws:username}"
    }
  ]
}
```

Question 4: What actions are allowed for IAM users based on this policy? How are the resource ARNs constructed?

Based on this policy, the following actions are allowed for IAM users:

- Create IAM users.
- Delete IAM users.

The resource ARNs in this policy are constructed using the `"arn:aws:iam::123456789012:user/${aws:username}"` format. The `${aws:username}` is a variable that represents the username of the IAM user being operated on. When an IAM user attempts to perform the actions specified in the policy, the `${aws:username}` variable will be dynamically replaced with the actual username of that user.

The policy allows the specified actions (`CreateUser` and `DeleteUser`) on the IAM user with the corresponding resource ARN constructed for that specific user.

This policy enables users to create and delete their own IAM user accounts within the AWS account identified by `123456789012`. However, it does not grant any additional permissions beyond the user creation and deletion actions specified.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Action": ["iam:Get*", "iam:List*"],
    "Resource": "*"
  }
}
```

Questions:

- Which AWS service does this policy grant you access to?

This policy grants access to the AWS Identity and Access Management (IAM) service.

- Does it allow you to create an IAM user, group, policy, or role?

No, this policy does not allow you to create an IAM user, group, policy, and role. The `iam:Get*` action in this policy allows you to retrieve information about IAM users, groups, policies, and roles.

- Go to https://docs.aws.amazon.com/IAM/latest/UserGuide/ and in the left navigation expand Reference > Policy Reference > Actions, Resources, and Condition Keys. Choose Identity And Access Management. Scroll to the Actions Defined by Identity And Access Management list. Name at least three specific actions that the iam:Get* action allows.

From the AWS IAM documentation, here are three specific actions that the `iam:Get*` action allows:

1. `iam:GetUser`: retrieve information about an IAM user.
2. `iam:GetGroup`: retrieve information about an IAM group.
3. `iam:GetPolicy`: retrieve information about an IAM policy.

These actions, when used with the wildcard `*` in the policy, allow you to perform any "Get" operation within the IAM service, retrieving information about IAM users, groups, policies, roles, and other related resources.

While this policy allows you to retrieve information, it does not grant permissions to create, modify, or delete IAM resources. Those actions would require additional permissions specified in the policy.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Condition": {
        "StringEquals": {
          "ec2:InstanceType": ["t2.micro", "t2.small"]
        }
      },
      "Resource": "arn:aws:ec2:*:*:instance/*",
      "Action": ["ec2:RunInstances", "ec2:StartInstances"],
      "Effect": "Deny"
    }
  ]
}
```

Questions:

- What actions does the policy allow?

Based on the provided policy, this policy does not allow any action and specifically denies the following actions:

- `ec2:RunInstances`: launch EC2 instances.
- `ec2:StartInstances`: start EC2 instances.

The policy is denying all actions including running and starting EC2 instances for instances with the instance types `t2.micro` and `t2.small`. So, even though the policy technically allows the actions, the effect of "Deny" supersedes it, preventing the actions from being executed for instances with the specified instance types.

-> Say that the policy included an additional statement object, like this example:

```
{
  "Effect": "Allow",
  "Action": "ec2:*"
}
```

- How would the policy restrict the access granted to you by this additional statement?

The effect of this additional statement is to allow all actions (`*`) for the EC2 service. Since it is an "Allow" statement, it grants permissions to perform any EC2 action.

When evaluating both statements, the "Deny" effect takes precedence over the "Allow" effect. Therefore, the "Deny" statement restricts access to instances with instance types `t2.micro` and `t2.small`, regardless of the "Allow" statement.

So, even with the "Allow" statement allowing all EC2 actions, the "Deny" statement explicitly denies the actions of running and starting instances with the specified instance types.

- If the policy included both the statement on the left and the statement in question 2, could you terminate an m3.xlarge instance that existed in the account?

Considering both statements in the policy:

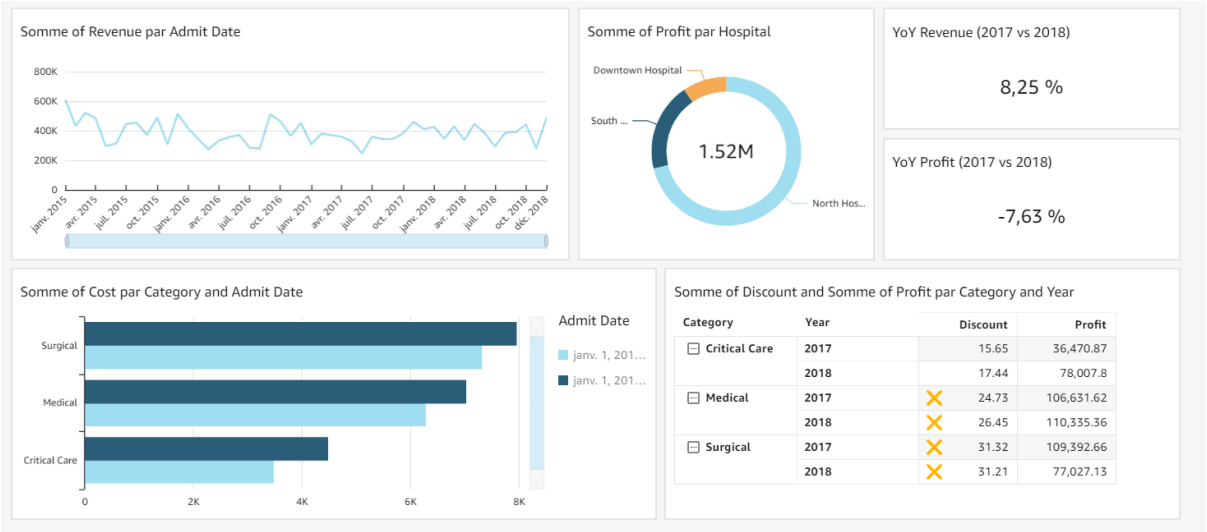
1. Deny statement:
    - Effect: Deny
    - Actions: `ec2:RunInstances`, `ec2:StartInstances`
    - Condition: `"ec2:InstanceType": ["t2.micro", "t2.small"]`

2. Allow statement:
    - Effect: Allow
    - Actions: `ec2:*`

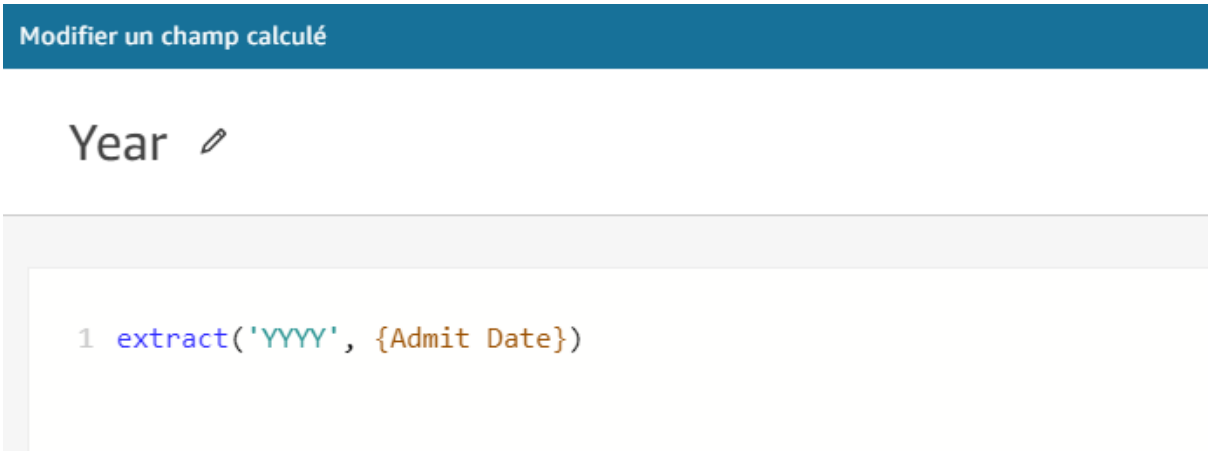
Regarding terminating an `m3.xlarge` instance, since the policy does not contain any explicit "Allow" or "Deny" statement for the `ec2:TerminateInstances` action, assuming that the user has the necessary permissions and privileges granted by other means, the user should be able to terminate an `m3.xlarge` instance that exists in the account.

5. Data Visualization With AWS QuickSight

We use the dataset to create this dashboard:

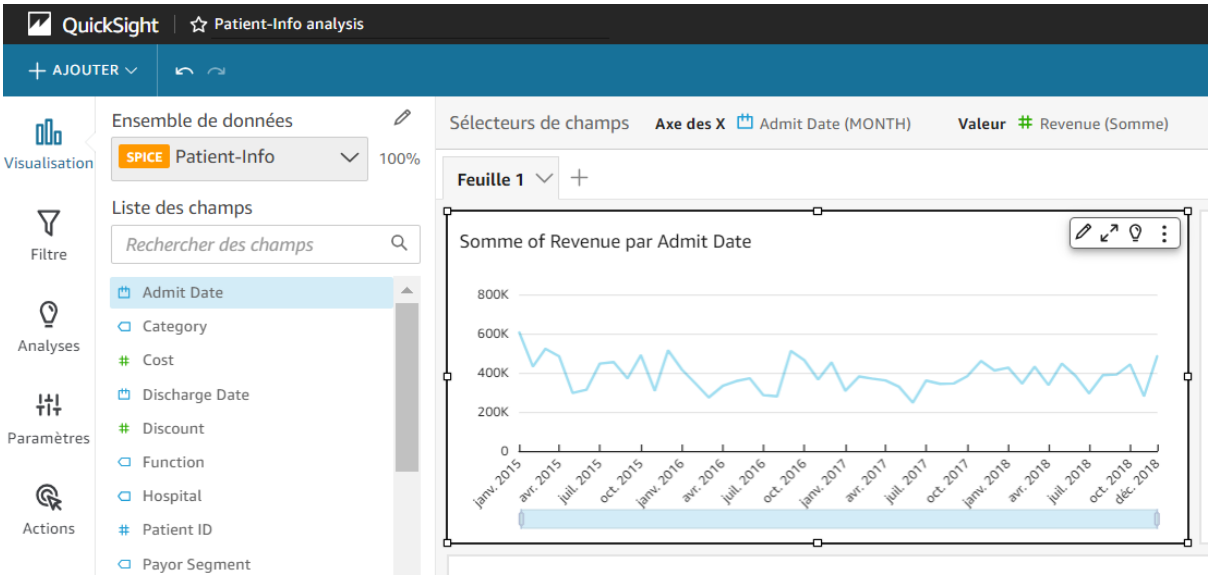


We have created a new field into the dataset to have the year of each Row and not all the dates with day, month and year with Admit_Date. This will simplified the calculations for to create the visual representation:

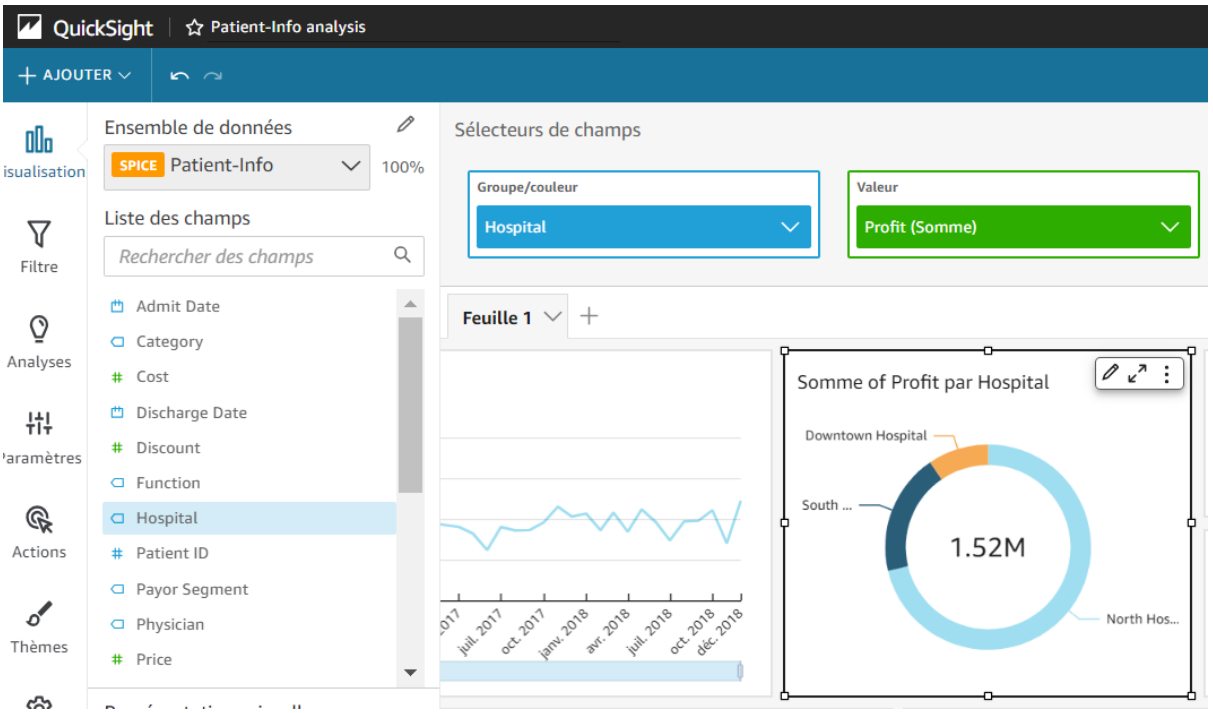


Below you have the detail of each visual representation:

To make this representation we have used a line graph with in the horizontal axis the admit date group by month and on the vertical axis the sum of the revenue.



For this visual representation we use the donut chat, this representation shows the sum of the profit by the hospital.

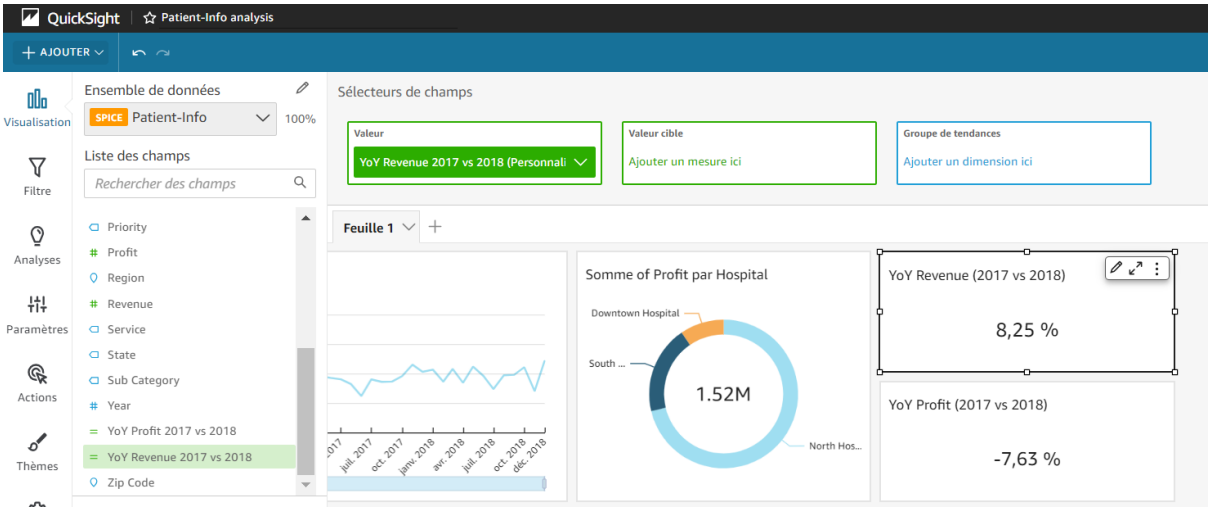


For the next representation, we have created a calculated field for the YoY Revenue. This is in this calculated field that the field year is used.

YoY Revenue 2017 vs 2018

```
((sumIf(Revenue, Year=2018)-sumIf(Revenue, Year=2017))/sumIf(Revenue, Year=2017))
```

For this representation we used KPI to show the value of the YoY Revenue between 2017 and 2018.

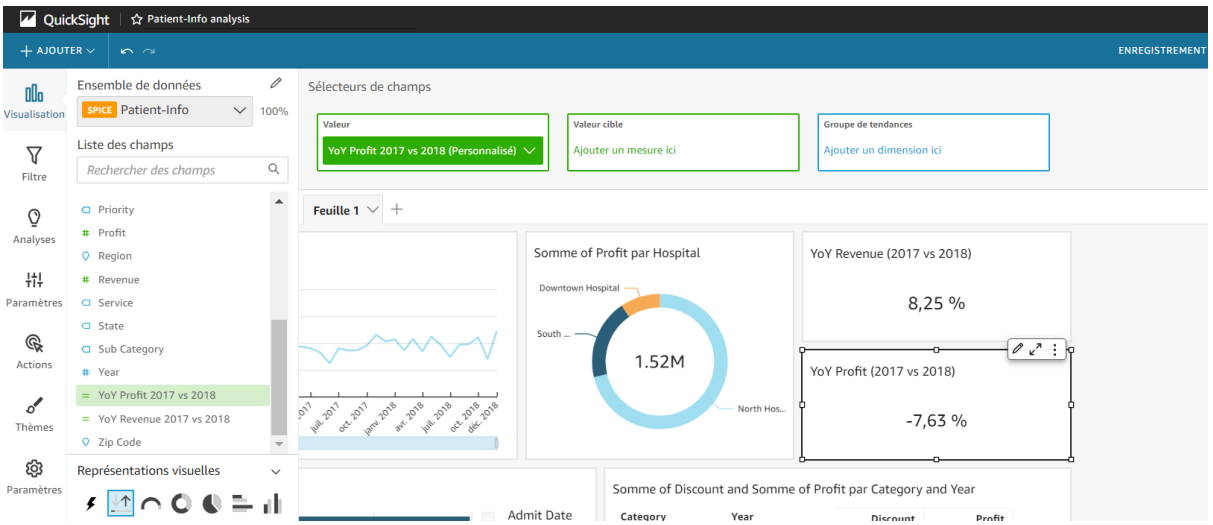


As seen before, we have created a calculated field for the YoY Profit:

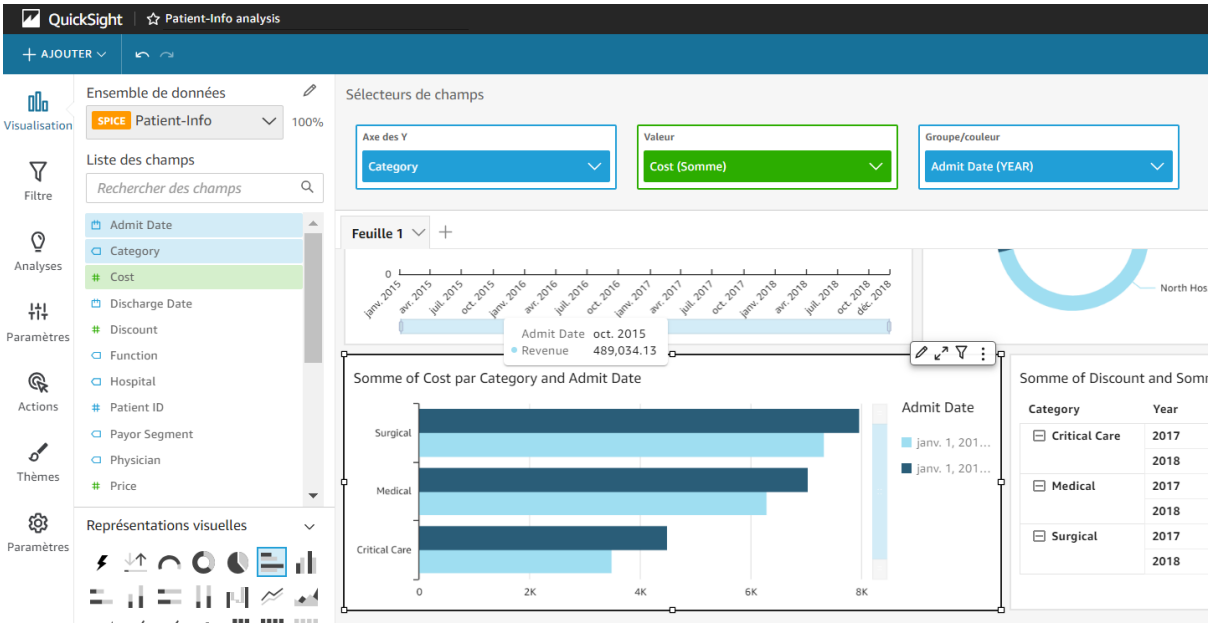
YoY Profit 2017 vs 2018

```
((sumIf(Profit, Year=2018)-sumIf(Profit, Year=2017))/sumIf(Profit, Year=2017))
```

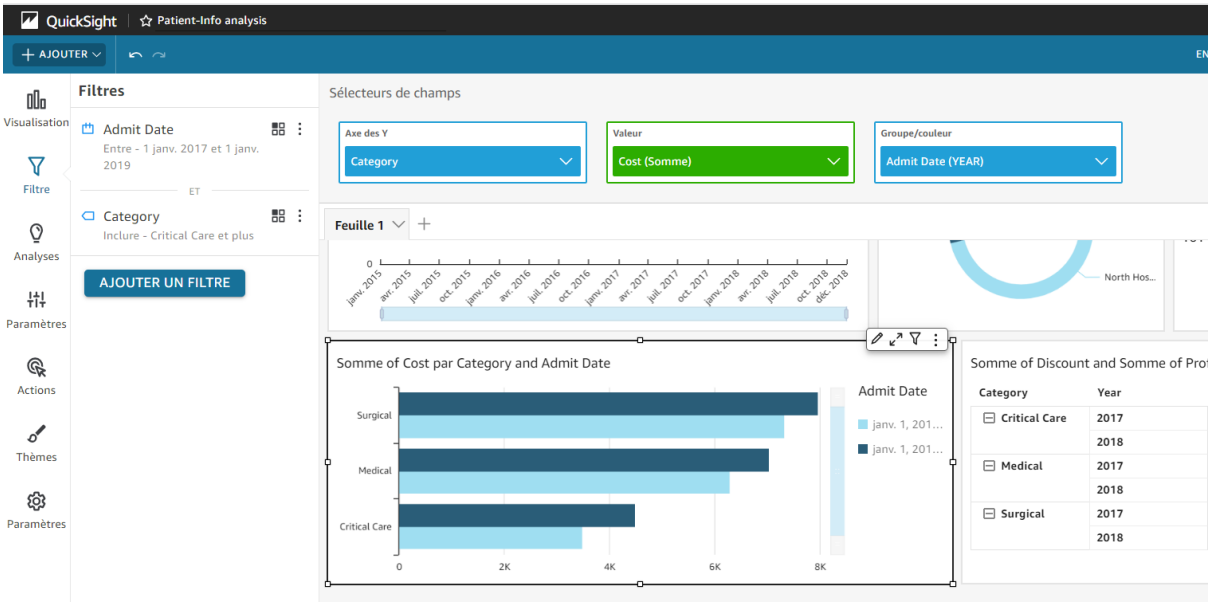
We use KPI to show the value of the YoY Profit between 2027 and 2028.



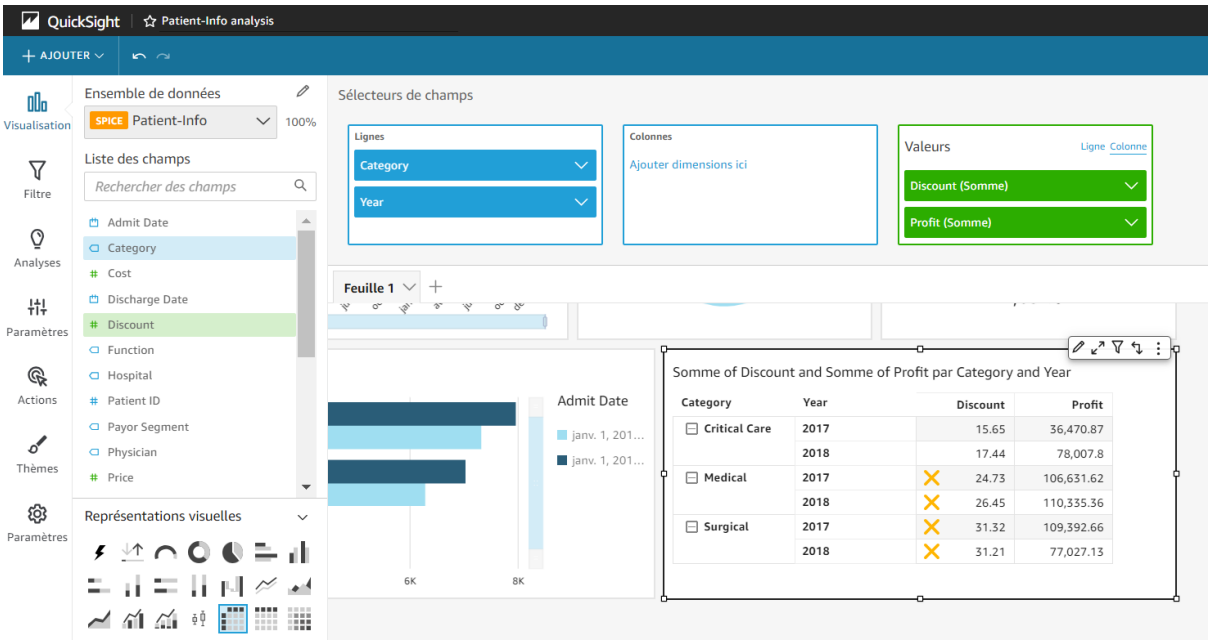
For this representation we have used the horizontal bar chart to show the sum of the cost by category and by admit date. So on the horizontal axis we have the category, the value to study is the sum of the cost and we want to group them by year.



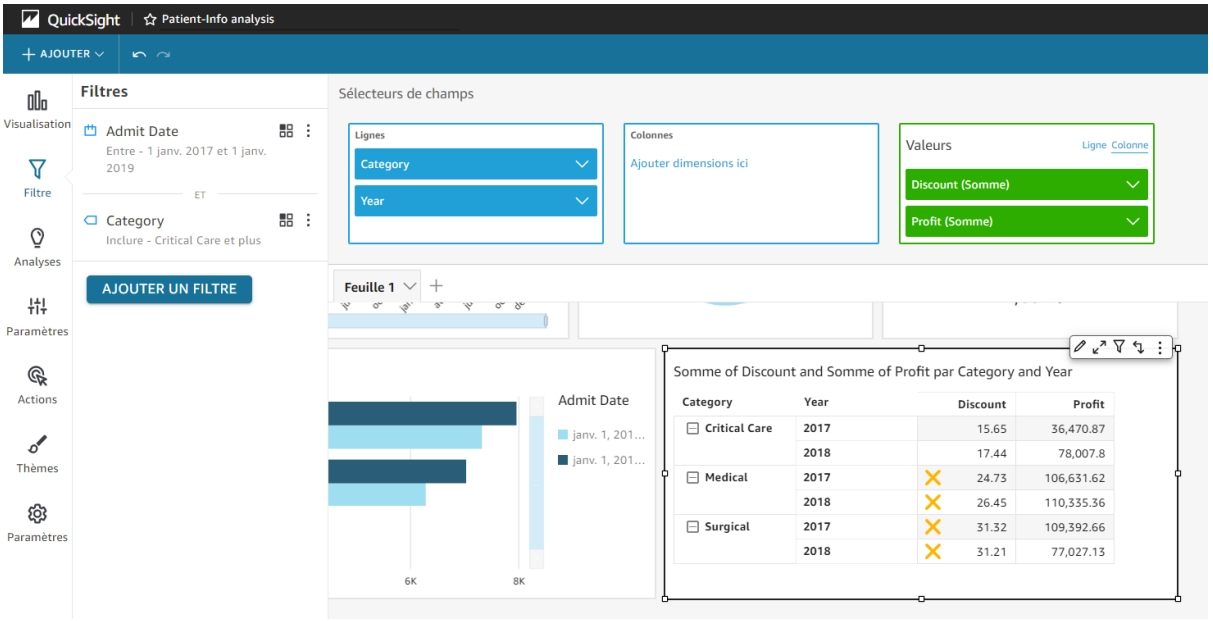
To have only Surgical, Medical and Critical Care categories we use a filter to select only these categories. We also select only the year 2017 and 2018 with a filter on admit date.



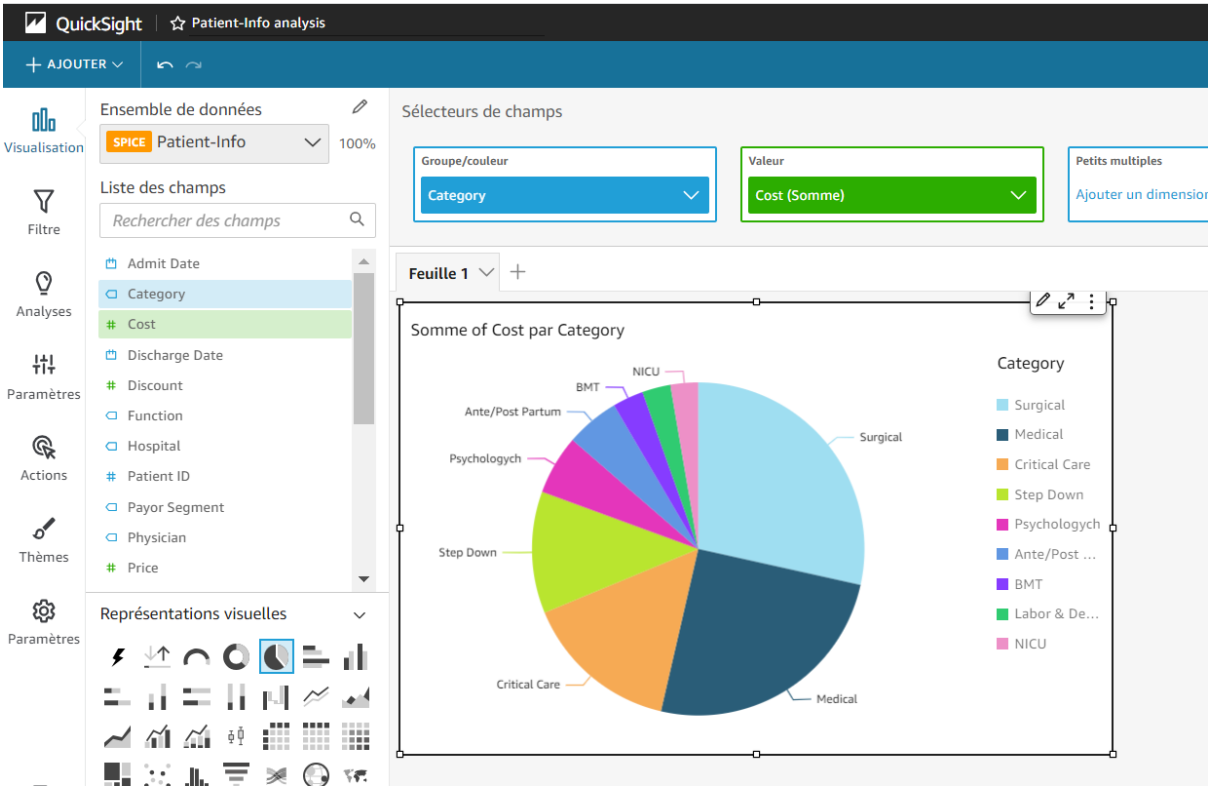
For this representation we use a pivot table to show the sum of discount and the sum of profit by category and by year. To do this we select category and year as lines of our table and sum of discount and sum of profit as the values.



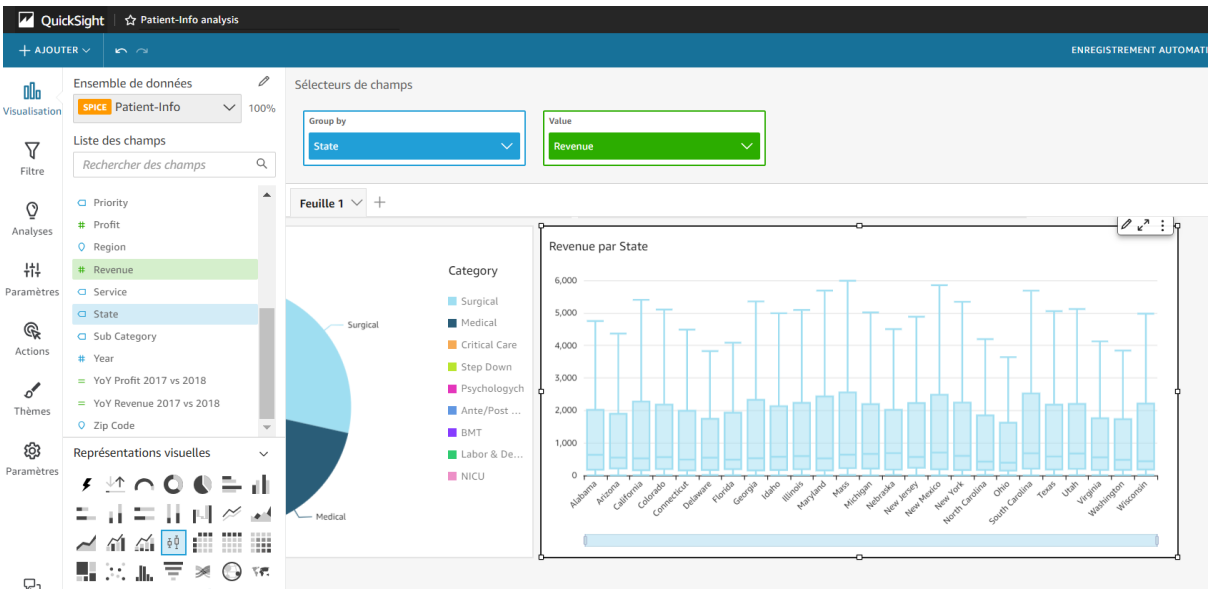
To have only Surgical, Medical and Critical Care categories we use a filter to select only these categories. We also select only the year 2017 and 2018 with a filter on admit date.



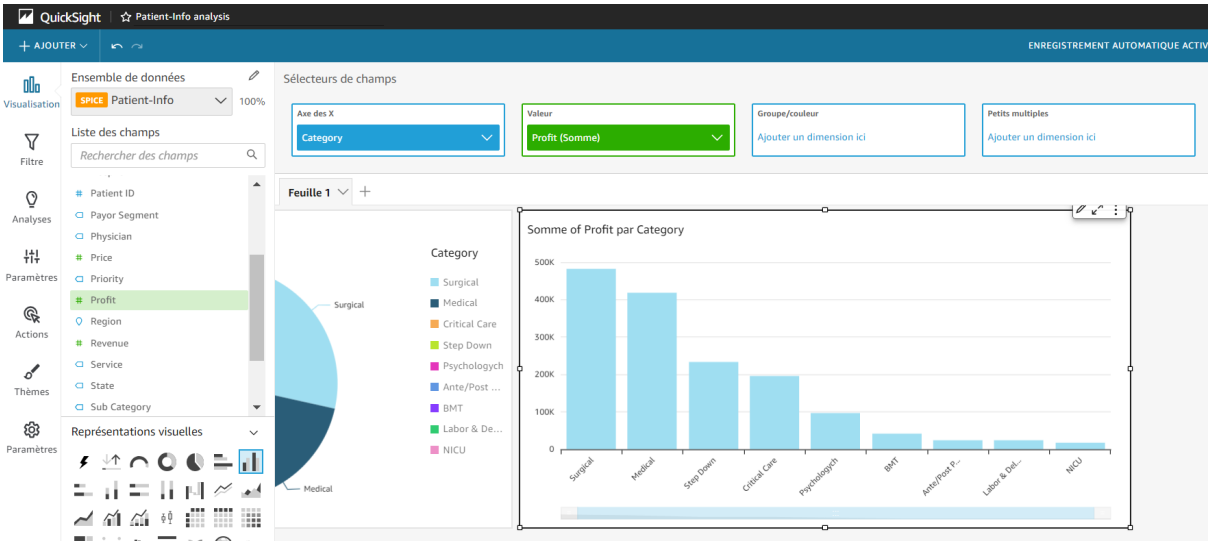
It is also possible to make other representations like a pie chart which can show the sum of the cost by category.



Or use a surface diagram to show for example the revenue by state.



Or use a vertical bar chart to show the sum of profit by category.



And apply a filter to see only the category where the sum of the profit is over 200K.