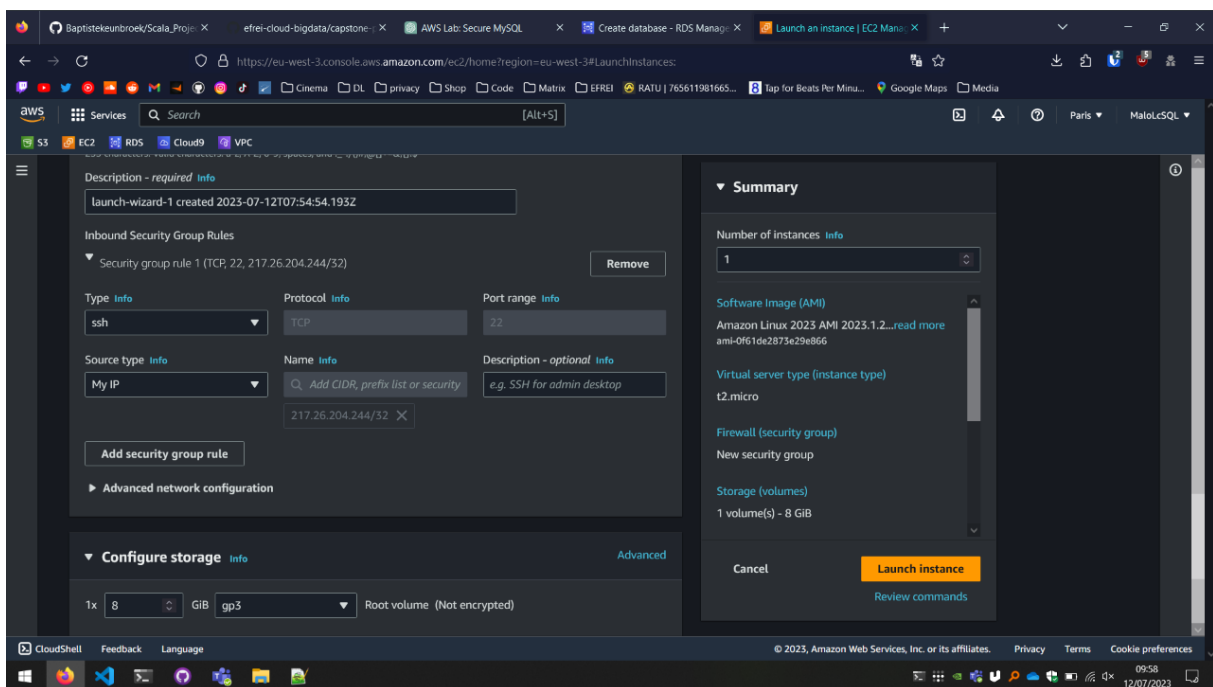
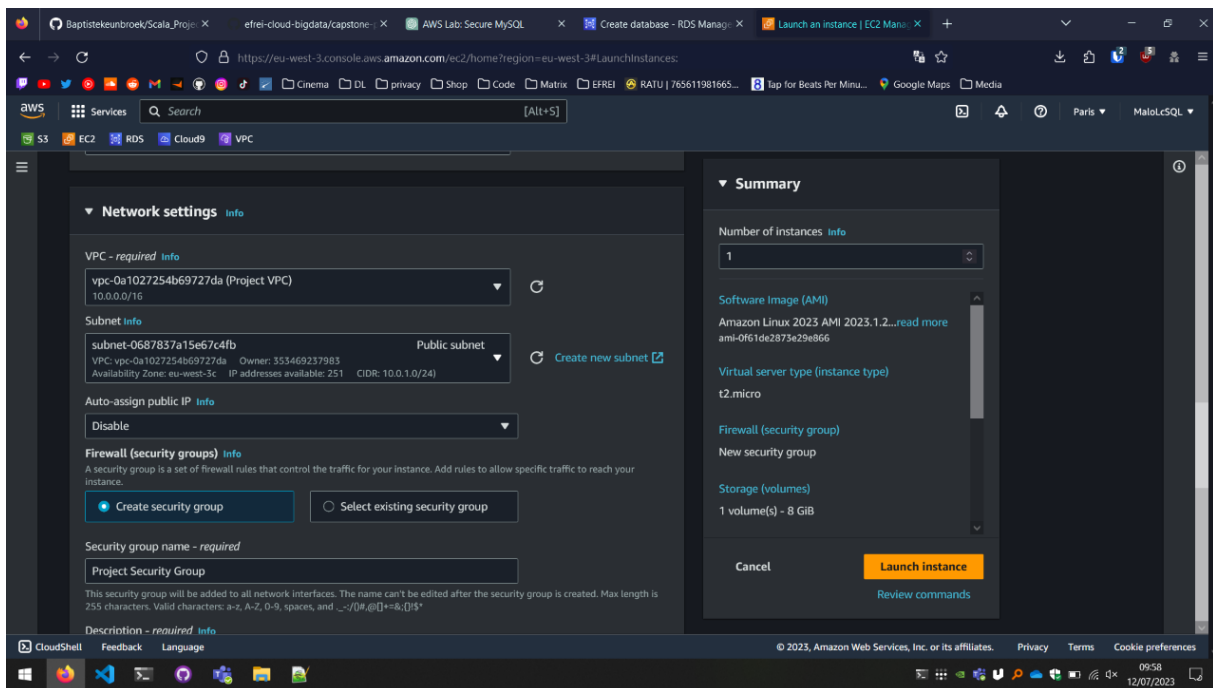
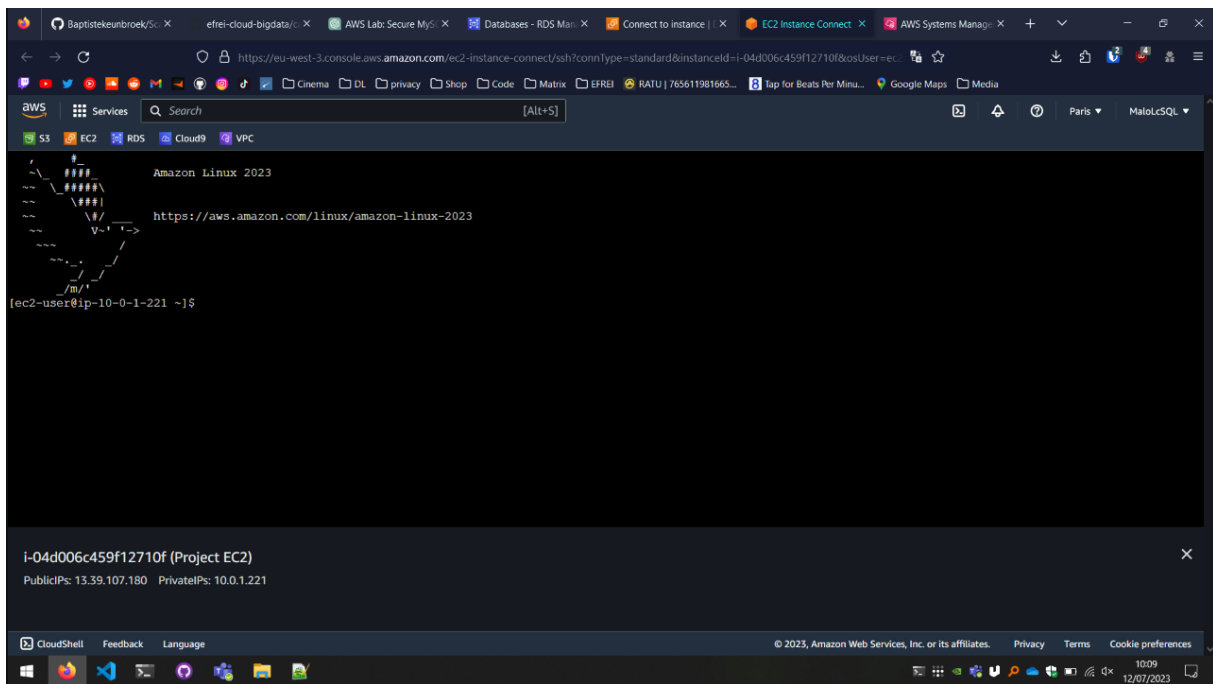
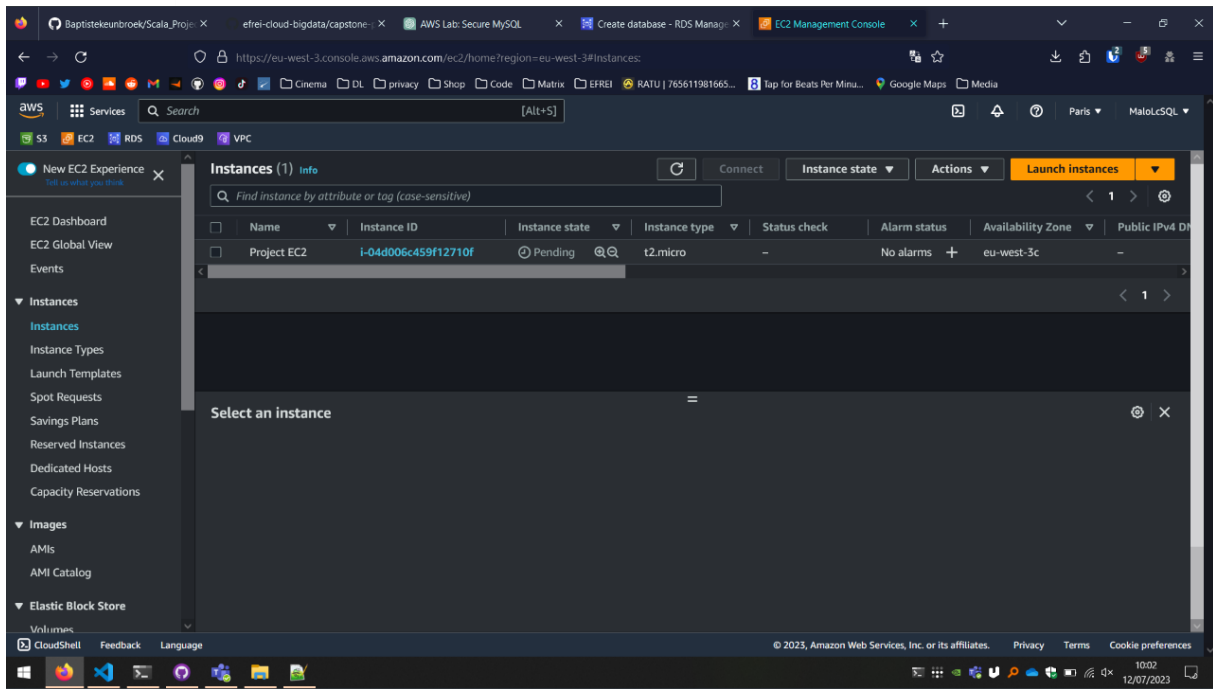


AWS Cloud & Big Data Architectures- Project

Lien GitHub : <https://github.com/Malo-LC/ProjectCloudBigaDataM1>

EC2





```

Failed to enable unit: Access denied
[ec2-user@ip-10-0-1-221 ~]$ sudo !!
sudo chkconfig httpd on
Note: Forwarding request to 'systemctl enable httpd.service'.
Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service -> /usr/lib/systemd/system/httpd.service.
[ec2-user@ip-10-0-1-221 ~]$ sudo service httpd start
Redirecting to /bin/systemctl start httpd.service
[ec2-user@ip-10-0-1-221 ~]$ pxd
-bash: pxd: command not found
[ec2-user@ip-10-0-1-221 ~]$ pwd
/home/ec2-user
[ec2-user@ip-10-0-1-221 ~]$ 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 08:14:43-- 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)... 52.218.153.1, 52.218.169.65, 52.218.234.145, ...
Connecting to aws-tc-largeobjects.s3.us-west-2.amazonaws.com (aws-tc-largeobjects.s3.us-west-2.amazonaws.com) [52.218.153.1]:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 15508 (15K) [application/x-sql]
Saving to: 'Countrydatadump.sql'

Countrydatadump.sql 100%[=====] 15.14K --.-KB/s in 0s

2023-07-12 08:14:44 (164 MB/s) - 'Countrydatadump.sql' saved [15508/15508]

[ec2-user@ip-10-0-1-221 ~]$ ls
Countrydatadump.sql
[ec2-user@ip-10-0-1-221 ~]$

```

i-04d006c459f12710f (Project EC2)

PublicIPs: 13.39.107.180 PrivateIPs: 10.0.1.221

```

perl-DBD-MariaDB-1.22-1.amzn2023.0.4.x86_64
perl-Data-Dumper-2.174-460.amzn2023.0.2.x86_64
perl-FileHandle-2.03-477.amzn2023.0.5.noarch
perl-Math-Complex-1.59-477.amzn2023.0.5.noarch
perl-base-2.27-477.amzn2023.0.5.noarch

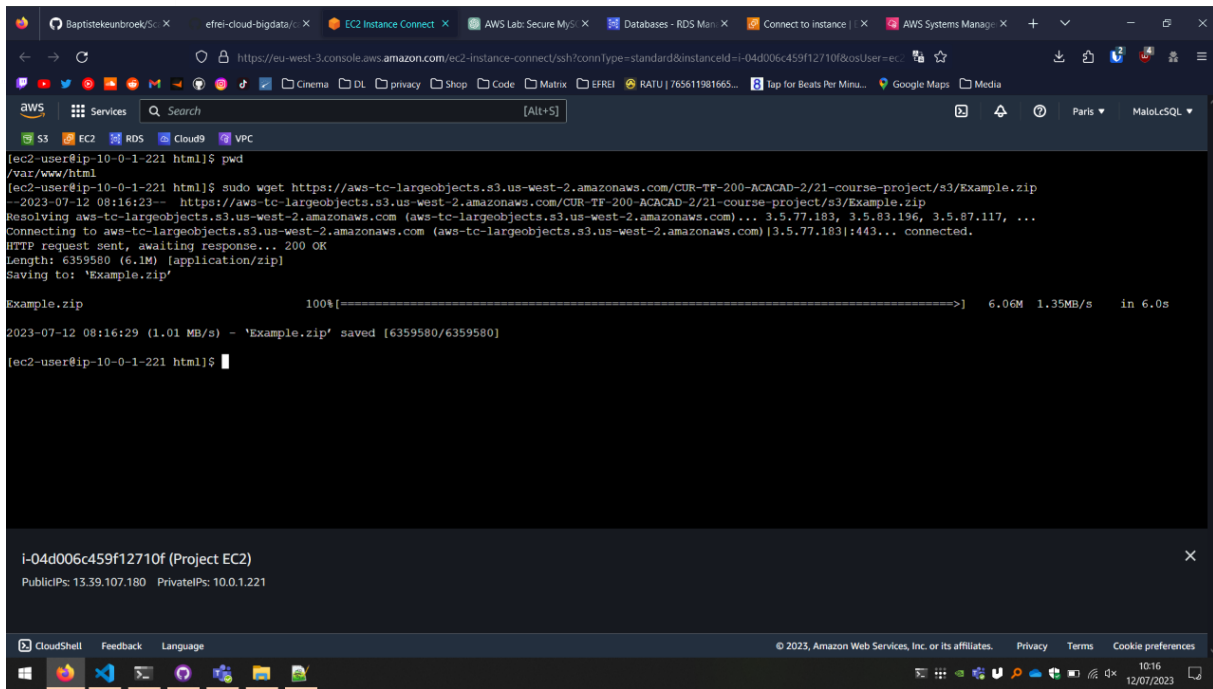
perl-DBI-1.643-7.amzn2023.0.3.x86_64
perl-File-Copy-2.34-477.amzn2023.0.5.noarch
perl-Math-BigInt-1.1.9998.10-458.amzn2023.0.2.noarch
perl-Sys-Hostname-1.23-477.amzn2023.0.5.x86_64

Complete!
[ec2-user@ip-10-0-1-221 ~]$ chkconfig httpd on
Note: Forwarding request to 'systemctl enable httpd.service'.
Failed to enable unit: Access denied
[ec2-user@ip-10-0-1-221 ~]$ sudo !!
sudo chkconfig httpd on
Note: Forwarding request to 'systemctl enable httpd.service'.
Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service -> /usr/lib/systemd/system/httpd.service.
[ec2-user@ip-10-0-1-221 ~]$ sudo service httpd start
Redirecting to /bin/systemctl start httpd.service
[ec2-user@ip-10-0-1-221 ~]$ pxd
-bash: pxd: command not found
[ec2-user@ip-10-0-1-221 ~]$ pwd
/home/ec2-user
[ec2-user@ip-10-0-1-221 ~]$ 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 08:14:43-- 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)... 52.218.153.1, 52.218.169.65, 52.218.234.145, ...
Connecting to aws-tc-largeobjects.s3.us-west-2.amazonaws.com (aws-tc-largeobjects.s3.us-west-2.amazonaws.com) [52.218.153.1]:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 15508 (15K) [application/x-sql]

```

i-04d006c459f12710f (Project EC2)

PublicIPs: 13.39.107.180 PrivateIPs: 10.0.1.221



The screenshot shows the AWS Management Console interface with the EC2 Instance Connect terminal open. The terminal displays the following commands and output:

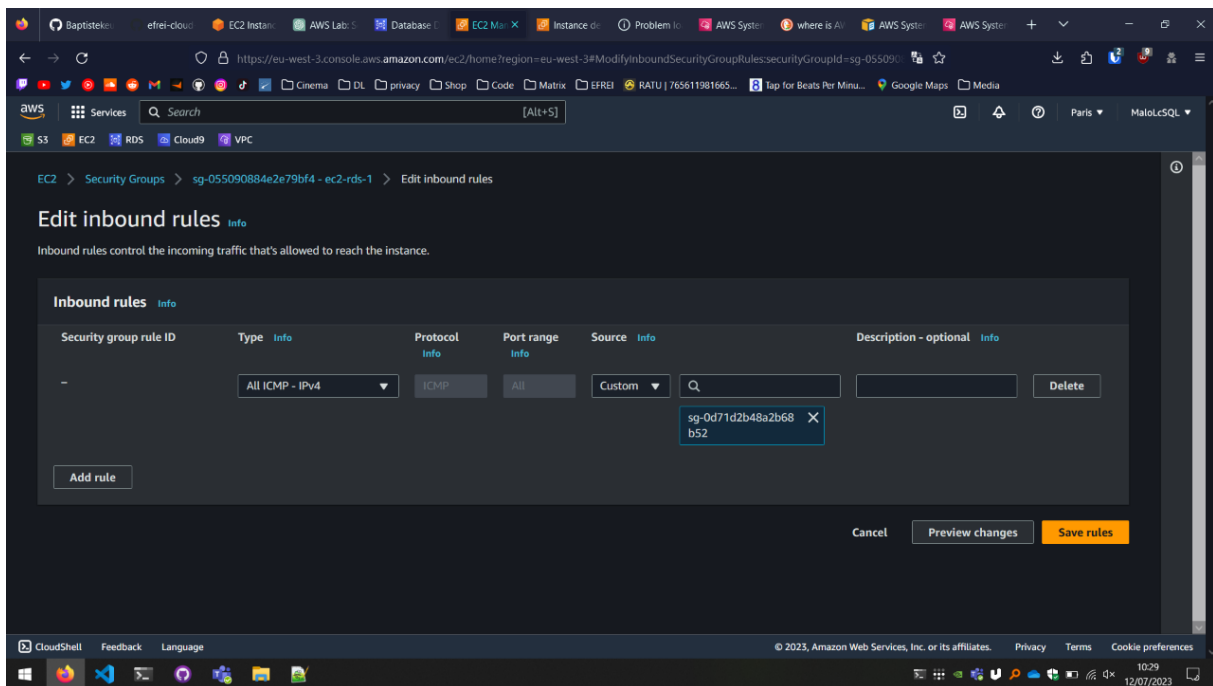
```
[ec2-user@ip-10-0-1-221 html]$ pwd
/var/www/html
[ec2-user@ip-10-0-1-221 html]$ sudo wget https://aws-tc-largeobjects.s3.us-west-2.amazonaws.com/CUR-TF-200-ACACAD-2/21-course-project/s3/Example.zip
--2023-07-12 08:16:23-- https://aws-tc-largeobjects.s3.us-west-2.amazonaws.com/CUR-TF-200-ACACAD-2/21-course-project/s3/Example.zip
Resolving aws-tc-largeobjects.s3.us-west-2.amazonaws.com (aws-tc-largeobjects.s3.us-west-2.amazonaws.com)... 3.5.77.183, 3.5.83.196, 3.5.87.117, ...
Connecting to aws-tc-largeobjects.s3.us-west-2.amazonaws.com (aws-tc-largeobjects.s3.us-west-2.amazonaws.com)|3.5.77.183|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 6359580 (6.1M) [application/zip]
Saving to: 'Example.zip'

Example.zip
100%[=====] 6.06M 1.35MB/s in 6.0s

2023-07-12 08:16:29 (1.01 MB/s) - 'Example.zip' saved [6359580/6359580]

[ec2-user@ip-10-0-1-221 html]$
```

Below the terminal, a summary box for instance **i-04d006c459f12710f (Project EC2)** is visible, showing PublicIPs: 13.39.107.180 and PrivateIPs: 10.0.1.221.

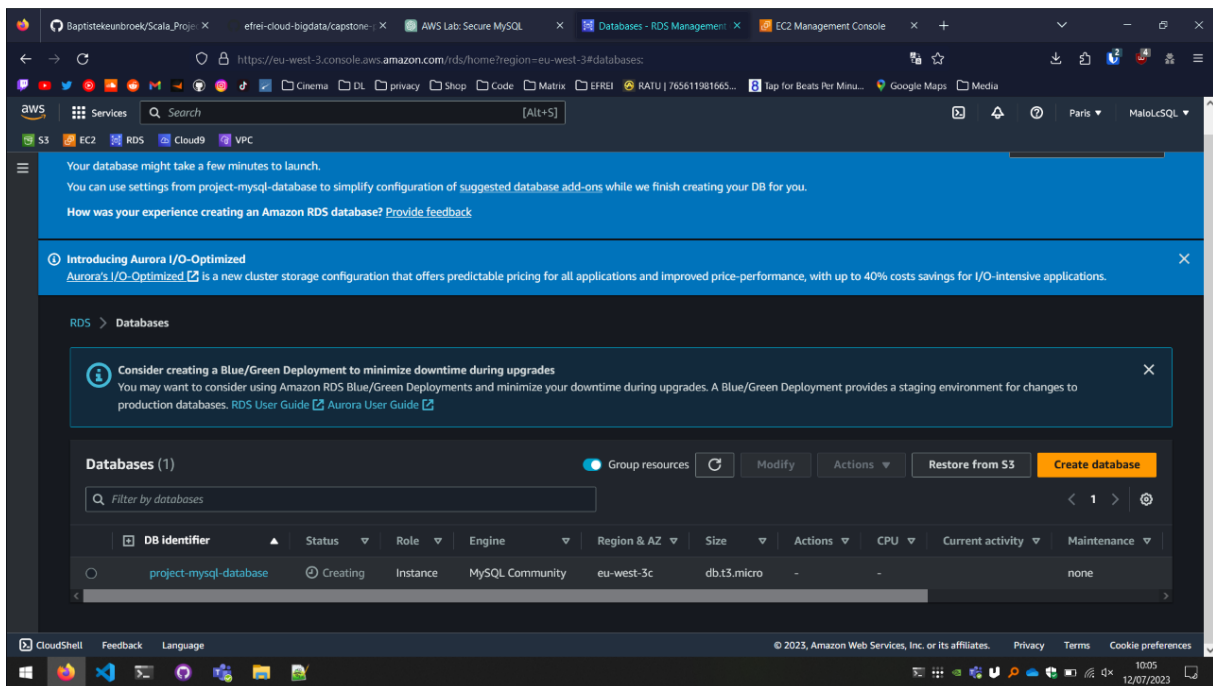
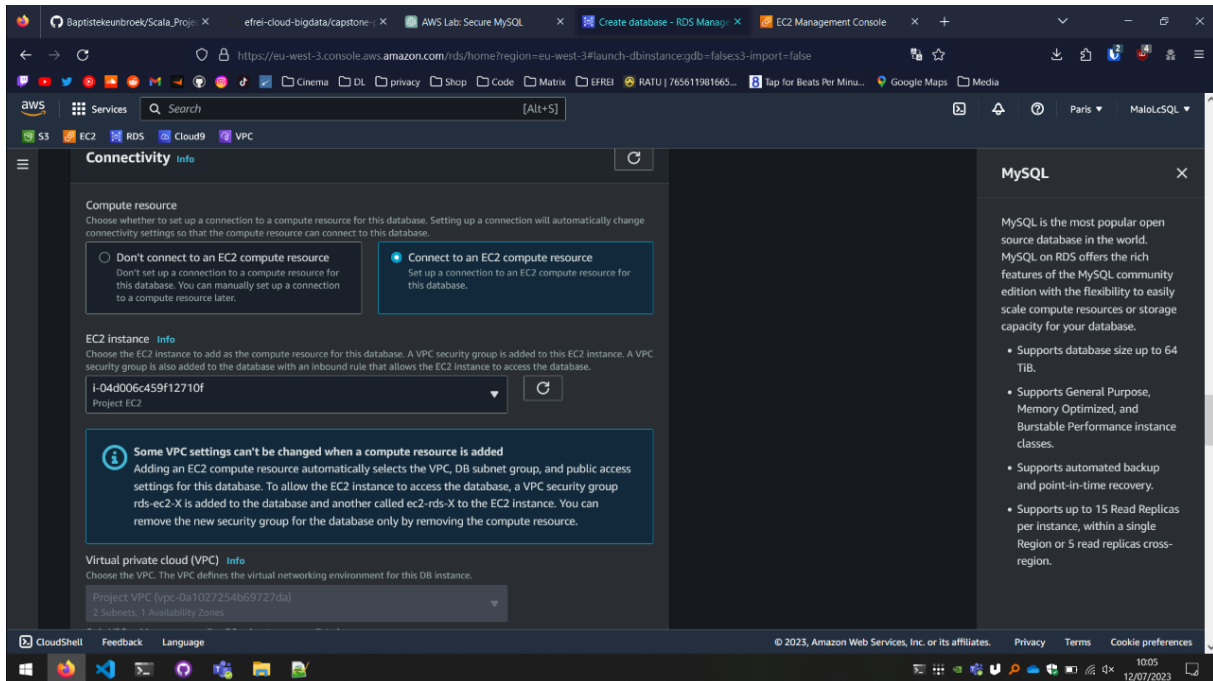


The screenshot shows the AWS Management Console interface with the 'Edit inbound rules' page for a Security Group. The page displays the following information:

- Security group rule ID:** -
- Type:** All ICMP - IPv4
- Protocol:** ICMP
- Port range:** All
- Source:** Custom
- Description - optional:** sg-0d71d2b48a2b68b52

The page also includes an 'Add rule' button and a 'Delete' button. At the bottom, there are 'Cancel', 'Preview changes', and 'Save rules' buttons.

RDS



VPC

The screenshot shows the AWS Management Console for the 'eu-west-3' region. The 'VPC' section is active, displaying a list of VPCs. The table below shows the details of the two VPCs:

Name	VPC ID	State	IPv4 CIDR	IPv6 CIDR	Default
Project VPC	vpc-0a1027254b69727da	Available	10.0.0.0/16	-	do
-	vpc-0569e49a3d5a6e8bf	Available	172.31.0.0/16	-	do

The screenshot shows the AWS Management Console for the 'eu-west-3' region, specifically the 'Subnets' section. A green notification banner at the top states: "You have successfully created 2 subnets: subnet-0687837a15e67c4fb, subnet-0edaeb9c839f769d3". The 'Subnets (2)' section displays a list of subnets. The table below shows the details of the two subnets:

Name	Subnet ID	State	VPC	IPv4 CIDR	IP
Private subnet	subnet-0edaeb9c839f769d3	Available	vpc-0a1027254b69727da Project VPC	10.0.2.0/24	-
Public subnet	subnet-0687837a15e67c4fb	Available	vpc-0a1027254b69727da Project VPC	10.0.1.0/24	-

Internet gateway igw-0aa79a382bee8fe20 successfully attached to vpc-0a1027254b69727da

Internet gateways (1/1) Info

Filter internet gateways

<input checked="" type="checkbox"/>	Name	Internet gateway ID	State	VPC ID	Owner
<input checked="" type="checkbox"/>	Public Internet Ga...	igw-0aa79a382bee8fe20	Attached	vpc-0a1027254b69727da Project VPC	353469237983

igw-0aa79a382bee8fe20 / Public Internet Gateway

Details Tags

Details

Route table rtb-043cb87d1030e59a7 | Project Route Table was created successfully.

Route tables (3) Info

Find resources by attribute or tag

<input type="checkbox"/>	Name	Route table ID	Explicit subnet associati...	Edge associations	Main	VPC
<input type="checkbox"/>	-	rtb-001c04c58b19b1067	-	-	Yes	vpc-0a1027254b69727da Proj...
<input type="checkbox"/>	-	rtb-0e389fb134427b6ea	-	-	Yes	vpc-0569e49a3d5a6e8bf
<input checked="" type="checkbox"/>	Project Route Table	rtb-043cb87d1030e59a7	-	-	No	vpc-0a1027254b69727da Proj...

Select a route table

Updated routes for rtb-043cb87d1030e59a7 / Project Route Table successfully

Route tables (1/3)

Name	Route table ID	Explicit subnet associati...	Edge associations	Main	VPC
-	rtb-001c04c58b19b1067	-	-	Yes	vpc-0a1027254b69727da Proj...
-	rtb-0e389fb134427b6ea	-	-	Yes	vpc-0569e49a3d5a6e8bf
Project Route Table	rtb-043cb87d1030e59a7	-	-	No	vpc-0a1027254b69727da Proj...

rtb-043cb87d1030e59a7 / Project Route Table

Details Routes Subnet associations Edge associations Route propagation Tags

You can now check network connectivity with Reachability Analyzer

Run Reachability Analyzer

Subnets (1/2)

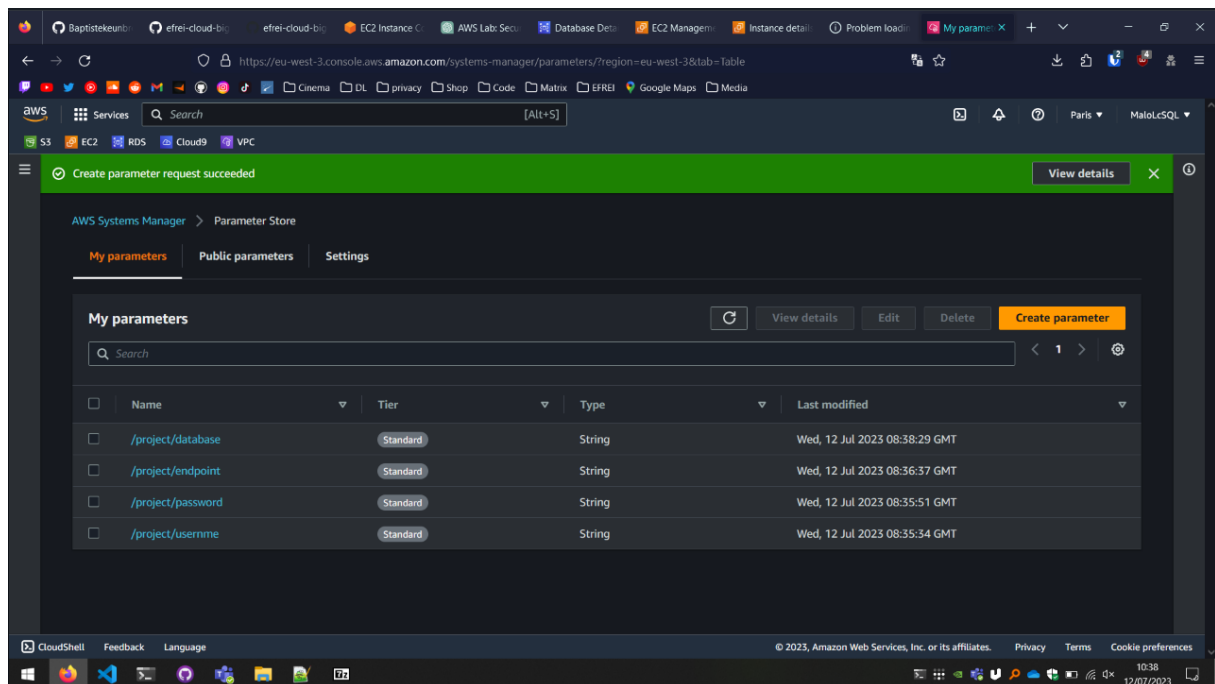
Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR
Private subnet	subnet-0edaeb9c839f769d3	Available	vpc-0a1027254b69727da Pr...	10.0.2.0/24	-
Public subnet	subnet-0687837a15e67c4fb	Available	vpc-0a1027254b69727da Pr...	10.0.1.0/24	-

Route table: rtb-043cb87d1030e59a7 / Project Route Table

Routes (2)

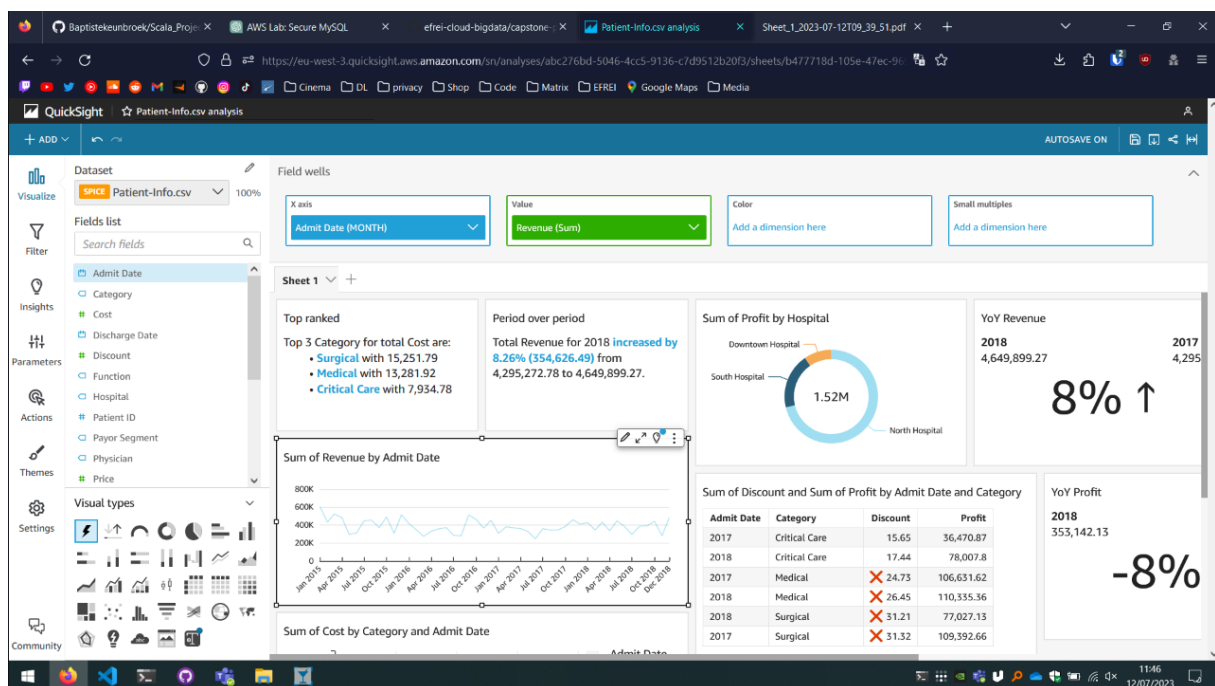
Destination	Target
10.0.0.0/16	local
0.0.0.0/0	igw-0aa79a382bee8fe20

Parameters and Sheet



The screenshot shows the AWS Systems Manager Parameter Store console. A green banner at the top indicates "Create parameter request succeeded". The interface is divided into three tabs: "My parameters", "Public parameters", and "Settings". The "My parameters" tab is active, displaying a table of parameters.

Name	Tier	Type	Last modified
/project/database	Standard	String	Wed, 12 Jul 2023 08:38:29 GMT
/project/endpoint	Standard	String	Wed, 12 Jul 2023 08:36:37 GMT
/project/password	Standard	String	Wed, 12 Jul 2023 08:35:51 GMT
/project/username	Standard	String	Wed, 12 Jul 2023 08:35:34 GMT



The screenshot shows the Amazon QuickSight console with a dashboard for "Patient-Info.csv analysis". The dashboard includes several visualizations:

- Top ranked:** Top 3 Category for total Cost are:
 - Surgical with 15,251.79
 - Medical with 13,281.92
 - Critical Care with 7,934.78
- Period over period:** Total Revenue for 2018 increased by 8.26% (354,626.49) from 4,295,272.78 to 4,649,899.27.
- Sum of Profit by Hospital:** A donut chart showing profit distribution for Downtown Hospital, South Hospital, and North Hospital. North Hospital has 1.52M profit.
- YoY Revenue:** 2018: 4,649,899.27; 2017: 4,295. A large "8% ↑" indicates an increase.
- Sum of Revenue by Admit Date:** A line chart showing revenue trends from Jan 2015 to Dec 2018.
- Sum of Discount and Sum of Profit by Admit Date and Category:** A table showing data for 2017 and 2018 across categories: Critical Care, Medical, and Surgical.
- YoY Profit:** 2018: 353,142.13; 2017: 385,000. A large "-8%" indicates a decrease.

Quizz Part

IAM Quizz

Which statement describes AWS identity and access Management IAM users ?

-Every IAM user for an account must have a unique name.

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

-Apply an AWS IAM policy to an IAM group.

Which statements describe AWS Identity and Access Management IAM roles (select two)

-They can be assumed by individuals, applications or services.

-They provide temporary security credentials.

Which Statement describes a resources based policy ?

-It is always an inline policy

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

-It checks for explicit deny statements before it checks for explicit allow statements.

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 IAM user for each developer, put them all 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 ?

-Users can use SSO to access the application through an existing authenticated identity.

Network Quizz

Which definition describes a virtual private cloud VPC ?

-A logically isolated virtual network that you define in the AWS Cloud

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: 172.16.0.0/23 (512 addresses) Subnet B: 172.16.2.0/23 (512 addresses)

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

-Configuring hosts to have or obtain an internet-routable address

-Creating a route for 0.0.0.0/0 that points to the internet gateway

-Configuring security groups and network ACLs to permit internet traffic

Policies evaluation Quiz

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

For EC2 instances: `ec2:DescribeVpcs`: This action allows the user to describe the virtual private clouds (VPCs) in the AWS account. `ec2:DescribeSubnets`: This action allows the user to describe the subnets in the AWS account. `ec2:DescribeSecurityGroups`: This action allows the user to describe the security groups in the AWS account. For S3 objects: There are no specific actions related to S3 objects mentioned in this policy. The policy only allows actions related to EC2 instances. Resources: The policy applies to all resources (denoted by `"*"`). It doesn't limit the scope to specific resources within EC2 or S3.

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

Condition: `s3:prefix`: This condition specifies that the access is allowed only when the S3 object key prefix matches either `"documents/"` or `"images/"`. Effect: `Allow`: This effect allows the specified actions when the conditions are met. Actions: `s3:GetObject`: Allows getting (reading) objects from the specified S3 bucket and objects matching the specified prefix. `s3:PutObject`: Allows putting (writing) objects into the specified S3 bucket and objects matching the specified prefix. `s3:ListBucket`: Allows listing the contents (objects) of the specified S3 bucket. Resources: `"arn:aws:s3:::example-bucket"`: Refers to the specified S3 bucket named `"example-bucket"`. `"arn:aws:s3:::example-bucket/*"`: Refers to objects within the `"example-bucket"` that match any key prefix. The policy does not specify any AWS region. Therefore, it applies to all regions where the specified S3 bucket exists.

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

`iam:CreateUser` and `iam>DeleteUser`. The actions are allowed for IAM users, and the specific IAM user is determined by the variable `${aws:username}`. Actions: `iam:CreateUser`: Allows creating IAM users. `iam>DeleteUser`: Allows deleting IAM users. Resources: `"arn:aws:iam::123456789012:user/${aws:username}"`: Refers to the IAM user resource with the AWS account ID `"123456789012"` and the specific IAM username determined by `${aws:username}`. The policy doesn't specify any specific S3 bucket or object actions. It solely focuses on IAM user creation and deletion.

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

Actions: `iam:Get*`: Allows all actions that start with `"iam:Get"`. This includes actions like `iam:GetUser`, `iam:GetGroup`, `iam:GetRole`, etc. It allows retrieving information about IAM users, groups, roles, policies, and other related resources. `iam:List*`: Allows all actions that start with `"iam:List"`. This includes actions like `iam:ListUsers`, `iam:ListGroups`, `iam:ListRoles`, etc. It allows listing information about IAM users, groups, roles, policies, and other related resources. Resources: `"*"`: The resource ARN is constructed using the wildcard `()` character, which matches any IAM resource. It allows the specified actions (`iam:Get*` and `iam:List*`) to be performed on any IAM resource in the AWS account.

Questions:

Which AWS service does this policy grant you access to?

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

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.

The Policy grants access to the AWS service called Amazon Elastic Compute Cloud (EC2). The policy allows two actions on EC2 instances: **ec2:RunInstances**: This action allows users to launch new EC2 instances. **ec2:StartInstances**: This action allows users to start existing EC2 instances. Regarding IAM-related actions, the policy does not explicitly mention permissions for creating IAM users, groups, policies, or roles. It focuses on EC2 instance-related actions. Here are three specific actions that the **iam:Get*** action allows: **iam:GetUser**: Retrieves information about an IAM user. **iam:GetGroup**: Retrieves information about an IAM group. **iam:GetRole**: Retrieves information about an IAM role.

Questions:

What actions does the policy allow?

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

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

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?

The Policy allows two actions: **ec2:RunInstances**: This action allows users to launch new EC2 instances. **ec2:StartInstances**: This action allows users to start existing EC2 instances. The additional statement allows all EC2 actions (wildcard), which means it grants full access to all EC2 actions available in the AWS API. In this case, the original policy's Deny effect for the **ec2:RunInstances** and **ec2:StartInstances** actions would be overridden by the new Allow statement that allows all EC2 actions. Therefore, you would have permission to terminate an m3.xlarge instance if it existed in the account since the **ec2:TerminateInstances** action is part of the **ec2:** set of actions.