

Rendu TP07

Rendu de TP07 effectué par Thomas PEUGNET .

Nous créons notre VPC.

The screenshot shows the AWS VPC Create VPC workflow page after a successful creation. The top navigation bar includes the AWS logo, Services, a search bar, and account information for N. Virginia and thomaspeu @ thomas-peugnet. The breadcrumb trail shows the path: VPC > Your VPCs > Create VPC > Create VPC resources. The main title is "Create VPC workflow". A "Success" message is displayed, followed by a "Details" section containing a list of 23 successful steps, each preceded by a green circular icon with a checkmark. The steps include creating the VPC itself, enabling DNS hostnames and resolution, verifying the VPC creation, creating subnets, attaching an internet gateway, and associating route tables. At the bottom right of the details section is a "View VPC" button. The footer of the page includes links for CloudShell, Feedback, and various AWS terms and policies.

VPC ID: vpc-08a94e87a2294c188

State: Available

Block Public Access: Off

DNS hostnames: Enabled

Main network ACL: acl-03b5368f9643b6837

IPv6 CIDR: -

Tenancy: Default

Default VPC: No

IPv4 CIDR: 10.150.0.0/16

Network Address Usage metrics: Disabled

Route 53 Resolver DNS Firewall rule groups: -

Main route table: rtb-03b915ab7dd58b5cd

IPv6 pool: -

Owner ID: 794038237731

Nous créons un sécurité group.

Security group name: SG-Thomas

Security group ID: sg-045f1a071e1b3aaa6

Description: SG-Thomas

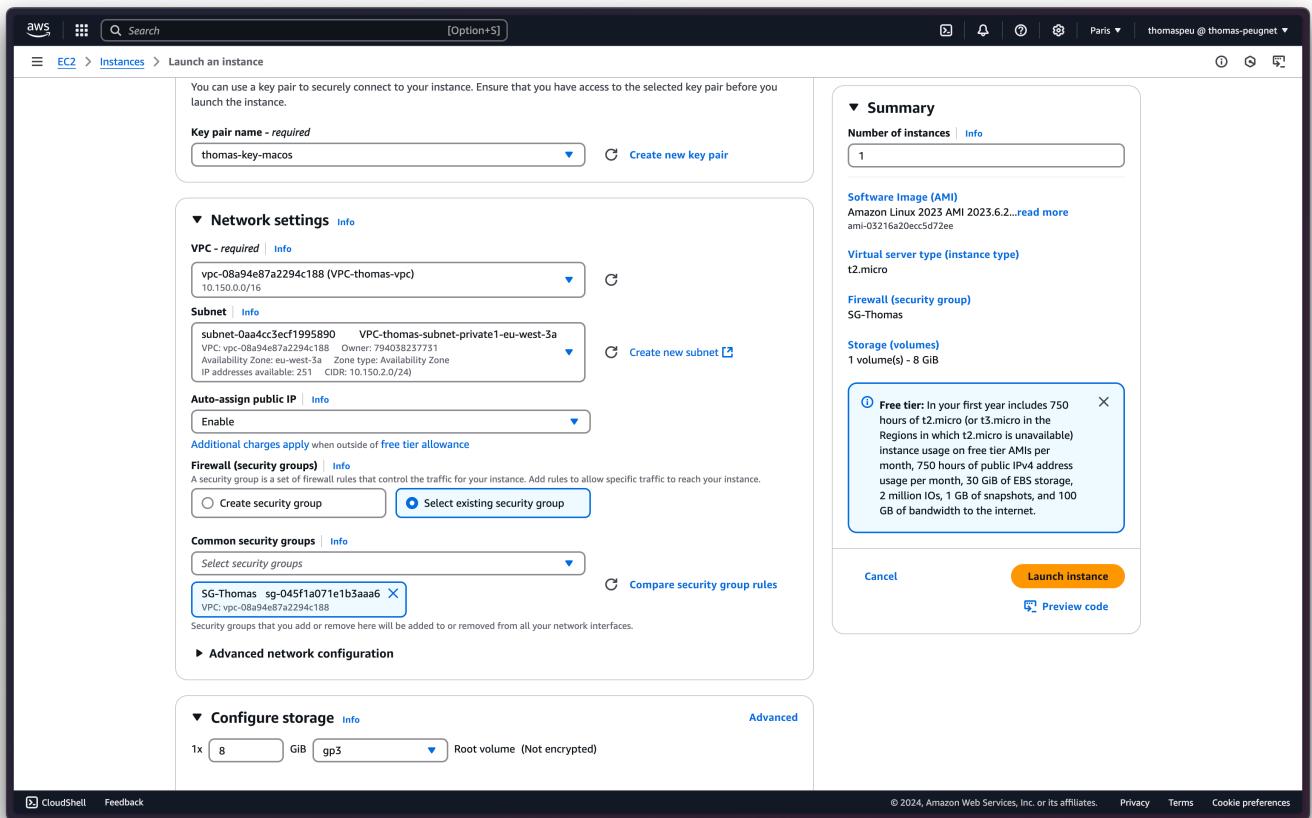
VPC ID: vpc-08a94e87a2294c188

Owner: 794038237731

Inbound rules count: 0 Permission entries

Outbound rules count: 1 Permission entry

Nous créons une instance **EC2-TEST-SG-ACL** sur notre VPC.



Nous y ajoutons, AVANT de lancer l'instance, le code bash suivant.

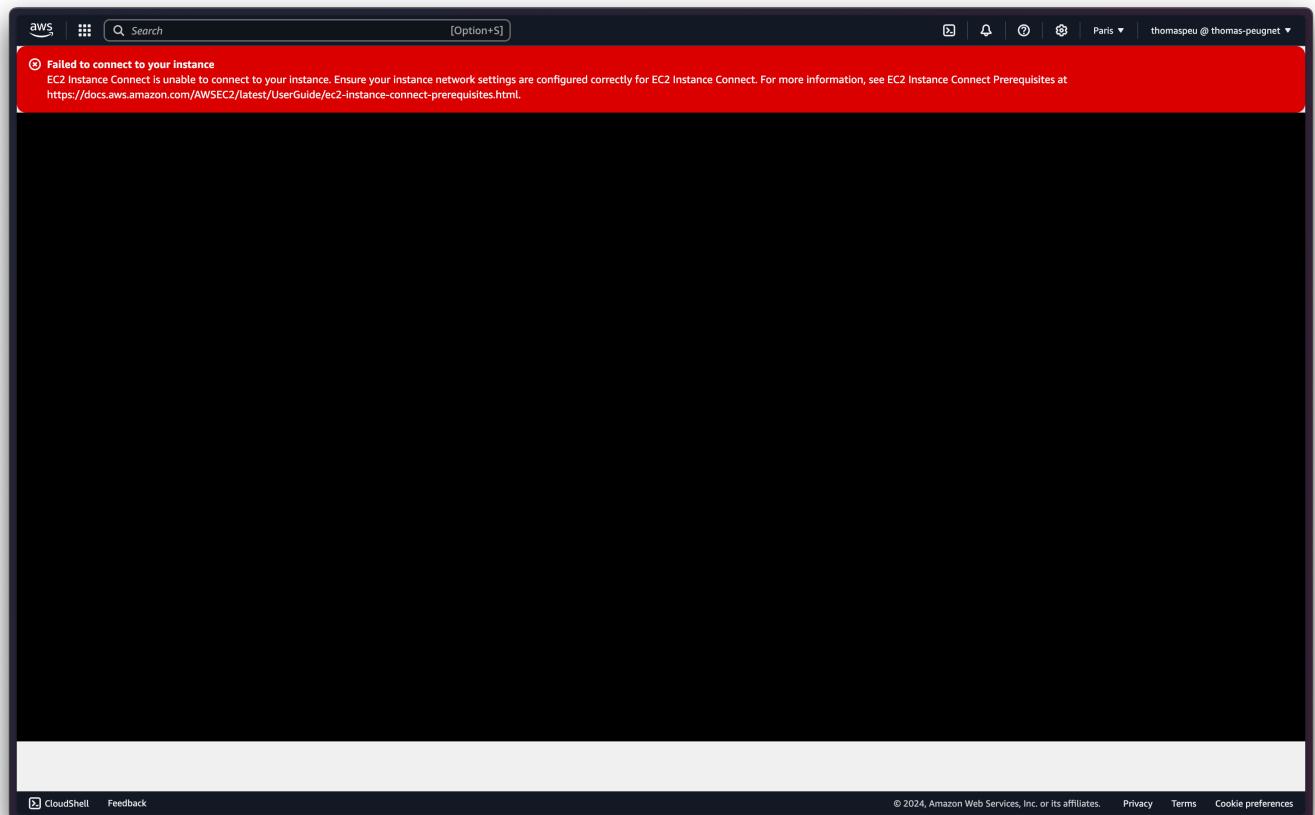
```
#!/bin/bash
yum update -y
yum install -y httpd
systemctl start httpd
systemctl enable httpd
```

Nous testons la résolution DNS.

```
nslookup ec2-35-181-169-122.eu-west-3.compute.amazonaws.com
```

```
thomas@MacBook-Pro-de-Thomas:~  
└─ thomas@MacBook-Pro-de-Thomas ~  
    └─ nslookup ec2-35-181-169-122.eu-west-3.compute.amazonaws.com 130 ↵  
Server:      1.1.1.1  
Address:     1.1.1.1#53  
  
Non-authoritative answer:  
Name:  ec2-35-181-169-122.eu-west-3.compute.amazonaws.com  
Address: 35.181.169.122  
  
└─ thomas@MacBook-Pro-de-Thomas ~
```

Nous ne pouvons pas encore accéder à notre instance depuis le client AWS.



Nous créons, dans notre sécurité group, une inbound rule.

Edit inbound rules Info

Inbound rules control the incoming traffic that's allowed to reach the instance.

Security group rule ID	Type	Info	Protocol	Info	Port range	Source	Info	Description - optional	Info
-	Custom TCP	TCP	80	An...	80	0.0.0.0/0	X	web	Delete
-	Custom TCP	TCP	22	An...	22	0.0.0.0/0	X		Delete

[Add rule](#)

⚠ Rules with source of 0.0.0.0/0 or ::/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

[Cancel](#) [Preview changes](#) [Save rules](#)

Inbound security group rules successfully modified on security group (sg-045f1a071e1b3aaa6 | SG-Thomas)

[Details](#)

sg-045f1a071e1b3aaa6 - SG-Thomas

[Actions](#)

Details

Security group name	Security group ID	Description	VPC ID
SG-Thomas	sg-045f1a071e1b3aaa6	SG-Thomas	vpc-08a94e87a2294c188
Owner	Inbound rules count	Outbound rules count	
794038237731	2 Permission entries	1 Permission entry	

[Inbound rules](#) [Outbound rules](#) [Sharing - new](#) [VPC associations - new](#) [Tags](#)

Inbound rules (2)

Name	Security group rule ID	IP version	Type	Protocol	Port range	Source
-	sgr-0519bd1cb7ddac755	IPv4	HTTP	TCP	80	0.0.0.0/0
-	sgr-0d09d3d7d2b3b3828	IPv4	SSH	TCP	22	0.0.0.0/0

[Manage tags](#) [Edit inbound rules](#)

Nous pouvons constater que cela fonctionne.

It works!



Nous créons une seconde instance.

The screenshot shows the AWS EC2 Instances "Launch an instance" page. At the top, there is a green success message: "Success Successfully initiated launch of instance (i-0aab9fc1b4bf9dd2)". Below this, there is a "Launch log" section with a link to "View log". Under "Next Steps", there are several cards:

- Create billing and free tier usage alerts**: To manage costs and avoid surprise bills, set up email notifications for billing and free tier usage thresholds. Includes a "Create billing alerts" button.
- Connect to your instance**: Once your instance is running, log into it from your local computer. Includes a "Connect to instance" button and a "Learn more" link.
- Connect an RDS database**: Configure the connection between an EC2 instance and a database to allow traffic flow between them. Includes a "Connect an RDS database" button and a "Learn more" link.
- Create EBS snapshot policy**: Create a policy that automates the creation, retention, and deletion of EBS snapshots. Includes a "Create EBS snapshot policy" button.
- Manage detailed monitoring**: Enable or disable detailed monitoring for the instance. If you enable detailed monitoring, the Amazon EC2 console displays monitoring graphs with a 1-minute period. Includes a "Manage detailed monitoring" button.
- Create Load Balancer**: Create a application, network gateway or classic Elastic Load Balancer. Includes a "Create Load Balancer" button.
- Create AWS budget**: AWS Budgets allows you to create budgets, forecast spend, and take action on your costs and usage from a single location. Includes a "Create AWS budget" button.
- Manage CloudWatch alarms**: Create or update Amazon CloudWatch alarms for the instance. Includes a "Manage CloudWatch alarms" button.

At the bottom right, there is a "View all instances" button. The footer includes links for CloudShell, Feedback, and various AWS terms like Privacy, Terms, and Cookie preferences.

La VM privée n'est pas accessible depuis la VM publique.

The screenshot shows an AWS CloudShell terminal window. The terminal output shows a ping test between two EC2 instances:

```
#          Amazon Linux 2023
#          https://aws.amazon.com/linux/amazon-linux-2023
Last login: Mon Dec  2 15:19:10 2024 from 35.180.112.84
[ec2-user@ip-10-150-0-173 ~]$ ping 10.150.2.144
PING 10.150.2.144 (10.150.2.144) 56(84) bytes of data.
--- 10.150.2.144 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4164ms
[ec2-user@ip-10-150-0-173 ~]$
```

Below the terminal, a modal window displays the instance details:

i-0b27ddc62195a5d43 (EC2-TEST-SG-ACL)
PublicIPs: 13.39.161.62 PrivateIPs: 10.150.0.173

The footer of the CloudShell window includes links for CloudShell, Feedback, and various AWS terms like Privacy, Terms, and Cookie preferences.

On modifie nos règles.

Nous pouvons constater que cela fonctionne.

```

# 
Amazon Linux 2023
/ # 
\# 
( / 
V- -> https://aws.amazon.com/linux/amazon-linux-2023
/ 
/ 
/ 
/ 
Last login: Mon Dec 2 15:19:10 2024 from 35.180.112.84
[ec2-user@ip-10-150-0-173 ~]$ ping 10.150.2.144
PING 10.150.2.144 (10.150.2.144) 56(84) bytes of data.
64 bytes from 10.150.2.144: icmp_seq=1 ttl=127 time=0.614 ms
64 bytes from 10.150.2.144: icmp_seq=2 ttl=127 time=1.04 ms
64 bytes from 10.150.2.144: icmp_seq=3 ttl=127 time=1.49 ms
64 bytes from 10.150.2.144: icmp_seq=4 ttl=127 time=0.908 ms

```

i-0b27ddc62195a5d43 (EC2-TEST-SG-ACL)

PublicIPs: 13.39.161.62 PrivateIPs: 10.150.0.173

Network ACLs.

VPC dashboard > Network ACLs > acl-03b3368f9643b6837

Details

Network ACL ID acl-03b3368f9643b6837	Associated with 4 Subnets	Default Yes	VPC ID vpc-08a94e87a2294c188 / VPC-thomas-vpc
---	------------------------------	----------------	--

Inbound rules | Outbound rules | Subnet associations | Tags

Inbound rules (2)

Rule number	Type	Protocol	Port range	Source	Allow/Deny
100	All traffic	All	All	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny

Nous avons modifié nos règles.

You have successfully updated inbound rules for acl-03b3368f9643b6837

Network ACLs (1/2) Info

Name	Network ACL ID	Associated with	Default	VPC ID	Inbound rules count
acl-0ac748f9102da714e	3 Subnets	Yes	vpc-024ad8fd0fd5c5446	2 Inbound rules	
acl-03b3368f9643b6837	4 Subnets	Yes	vpc-08a94e87a2294c188 / VPC-thoma...	3 Inbound rules	

acl-03b3368f9643b6837

Inbound rules (3)

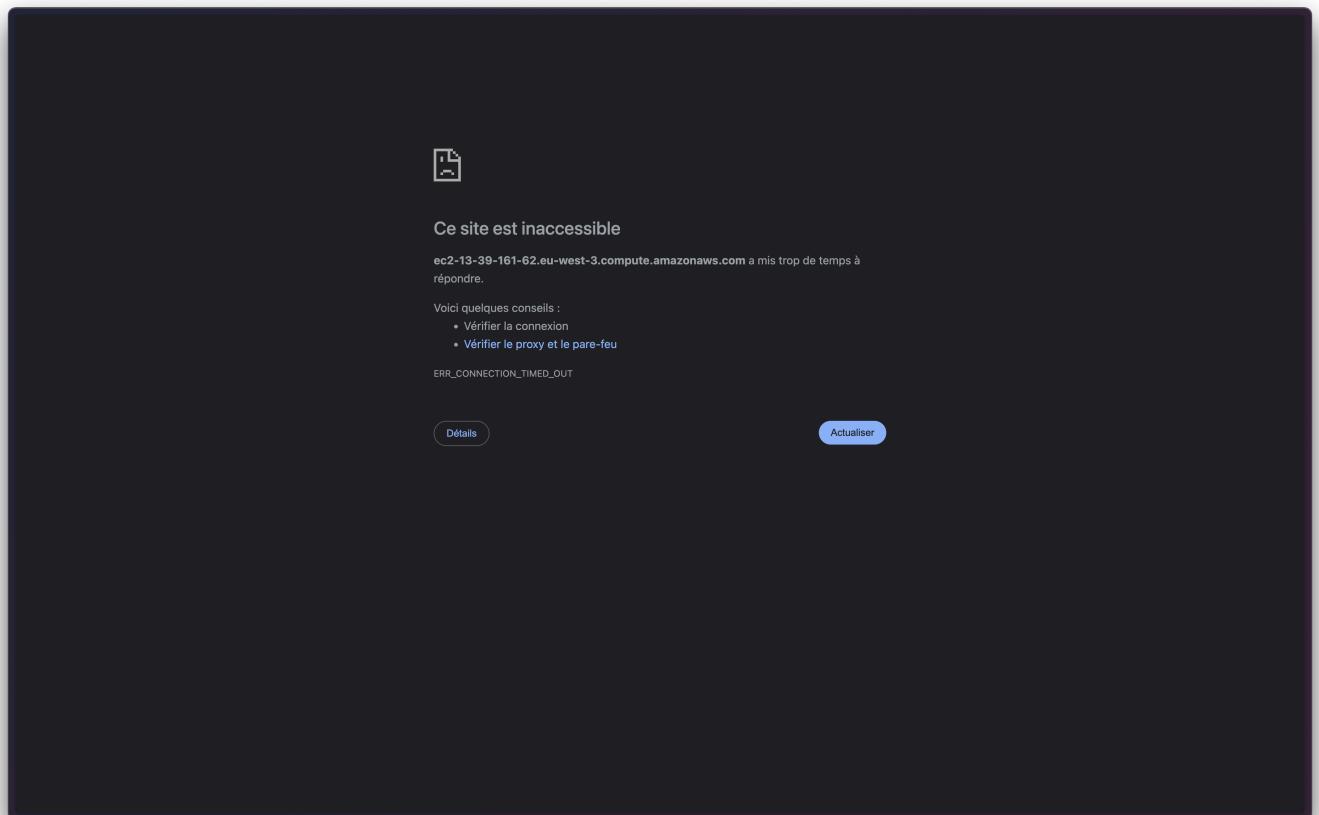
Rule number	Type	Protocol	Port range	Source	Allow/Deny
90	HTTP (80)	TCP (6)	80	0.0.0.0/0	Deny
100	All traffic	All	All	0.0.0.0/0	Allow
*	All traffic	All	All	0.0.0.0/0	Deny

Nous pouvons constater que cela ne fonctionne plus.

```
curl http://ec2-13-39-161-62.eu-west-3.compute.amazonaws.com/
↳ thomas@MacBook-Pro-de-Thomas ~/Downloads
  curl http://ec2-13-39-161-62.eu-west-3.compute.amazonaws.com/ 255 ↵
```

Nous modifions notre règle pour mettre uniquement notre adresse IP.

Nous ne pouvons plus accéder au site.



Nous modifions les règles pour ne plus y avoir accès via SSH.

The screenshot shows a web browser window with the URL yulip.org in the address bar. The page has a blue header with the text "Utiliser le site YulP pour découvrir votre adresse IP pour vérifier les ports ouverts, testez également le temps d'attente à plusieurs serveurs dans le monde et donner la commande PING en ligne." Below the header is a sidebar with icons and text for "Montrez votre IP", "vérifier les ports", "commande ping", "Test latence", and "changement de langue". A message "Votre adresse IP sur Internet" is shown with the value "2a01:e0a:a86:af28::10". The main content area contains a form to "Test si un port TCP est ouvert ou fermé." It includes fields for "Entrez l'adresse IP ou hôte" with the value "ec2-13-39-161-62.eu-wes" and "Entrez le numéro de port" with the value "22". A blue button labeled "ESSAI" is present. Below the form, the result is displayed: "ec2-13-39-161-62.eu-west-3.compute.amazonaws.com/:22 à huis clos". A note below the result says: "la plupart liste des ports TCP commun que vous pouvez tester".

Nous pouvons constater que cela fonctionne.

Si nous nous connectons via SSH, nous pouvons constater également que cela fonctionne.

```

ec2-user@ip-10-150-0-173:~ 
└─ thomas@MacBook-Pro-de-Thomas ~/Downloads
    └─ ssh -i "thomas-key-macos.pem" ec2-user@ec2-13-39-161-62.eu-west-3.compute.amazonaws.com
The authenticity of host 'ec2-13-39-161-62.eu-west-3.compute.amazonaws.com (13.39.161.62)' can't be established.
ED25519 key fingerprint is SHA256:JTSHZNp1kxcuwI+qpryiG3z02gi0dqhj0hDipfftOS8.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'ec2-13-39-161-62.eu-west-3.compute.amazonaws.com' (ED25519) to the list of known hosts.

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

Last login: Mon Dec 2 15:21:34 2024 from 35.180.112.85
[ec2-user@ip-10-150-0-173 ~]$

```

On supprime nos instances.

The screenshot shows the AWS CloudWatch Metrics Insights interface. A green banner at the top indicates "Successfully initiated termination (deletion) of i-0b27ddc62195a5d43, i-0dc6a831140b42728, i-0b6a8b3c531099da5, i-0aeab9fc1b4bf9dd2". Below this, the "Instances (4/4) Info" section lists four terminated t2.micro instances with their respective IDs and details. The main pane displays four line charts under the heading "4 instances selected": CPU utilization (%), Network in (bytes), Network out (bytes), and Network packets in (count). Each chart shows data over a one-hour period from 14:30 to 15:30. The bottom of the screen shows the AWS navigation bar and footer links.

Nous nettoyons nos règles Network ACLs.

Nous supprimons notre VPC.