École Polytechnique de Montréal

Département de génie informatique et génie logiciel

INF8102 - Sécurité dans les environnements infonuagiques

Automne 2025

TP4 - Infrastructure as Code Security

Soumis par :

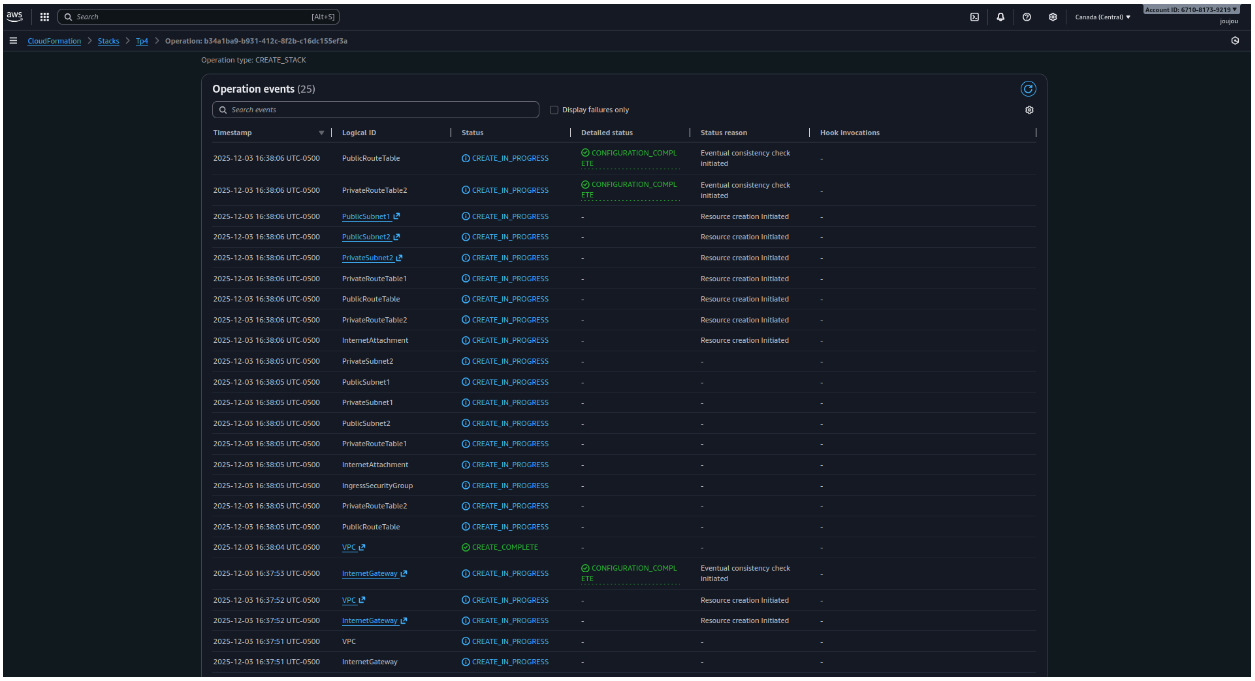
Julien Leduc - 2209094

Julien Lavigne - 2207643

Le 4 décembre 2025

Lien Vers le Repot Git: https://github.com/Joujou58007/INF8102_TP4/tree/main

Après la création du YAML, on peut téléverser ce dernier dans AWS Cloudformation pour créer l'infrastructure VPC automatiquement.


aws
Search
[Alt+S]
Canada (Central) ▾
Account ID: 6710-8173-9219 ▾
joujou
CloudFormation > Stacks > Tp4 > Operation: b34a1ba9-b931-412c-8f2b-c16dc155ef3a
Search events
□ Display failures only

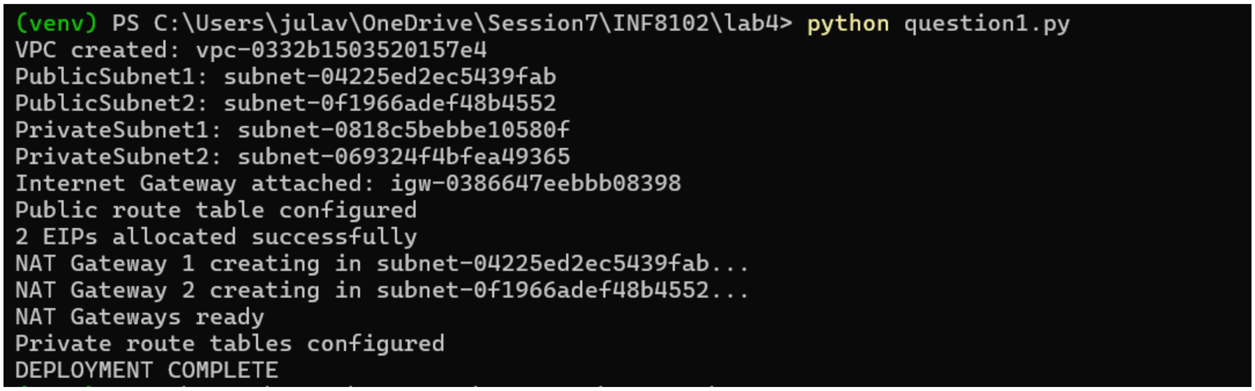
Operation type: CREATE_STACK

Operation events (25)

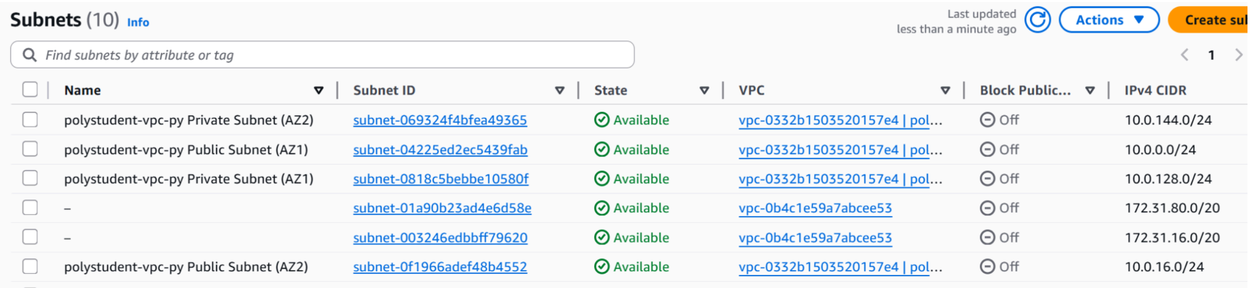
Timestamp	Logical ID	Status	Detailed status	Status reason	Hook invocations
2025-12-03 16:38:06 UTC-0500	PublicRouteTable	ⓘ CREATE_IN_PROGRESS	✓ CONFIGURATION_COMPLETE	Eventual consistency check initiated	-
2025-12-03 16:38:06 UTC-0500	PrivateRouteTable2	ⓘ CREATE_IN_PROGRESS	✓ CONFIGURATION_COMPLETE	Eventual consistency check initiated	-
2025-12-03 16:38:06 UTC-0500	PublicSubnet1	ⓘ CREATE_IN_PROGRESS	-	Resource creation Initiated	-
2025-12-03 16:38:06 UTC-0500	PublicSubnet2	ⓘ CREATE_IN_PROGRESS	-	Resource creation Initiated	-
2025-12-03 16:38:06 UTC-0500	PrivateSubnet2	ⓘ CREATE_IN_PROGRESS	-	Resource creation Initiated	-
2025-12-03 16:38:06 UTC-0500	PrivateRouteTable1	ⓘ CREATE_IN_PROGRESS	-	Resource creation Initiated	-
2025-12-03 16:38:06 UTC-0500	PublicRouteTable	ⓘ CREATE_IN_PROGRESS	-	Resource creation Initiated	-
2025-12-03 16:38:06 UTC-0500	PrivateRouteTable2	ⓘ CREATE_IN_PROGRESS	-	Resource creation Initiated	-
2025-12-03 16:38:06 UTC-0500	InternetAttachment	ⓘ CREATE_IN_PROGRESS	-	Resource creation Initiated	-
2025-12-03 16:38:05 UTC-0500	PrivateSubnet2	ⓘ CREATE_IN_PROGRESS	-	-	-
2025-12-03 16:38:05 UTC-0500	PublicSubnet1	ⓘ CREATE_IN_PROGRESS	-	-	-
2025-12-03 16:38:05 UTC-0500	PrivateSubnet1	ⓘ CREATE_IN_PROGRESS	-	-	-
2025-12-03 16:38:05 UTC-0500	PublicSubnet2	ⓘ CREATE_IN_PROGRESS	-	-	-
2025-12-03 16:38:05 UTC-0500	PrivateRouteTable1	ⓘ CREATE_IN_PROGRESS	-	-	-
2025-12-03 16:38:05 UTC-0500	InternetAttachment	ⓘ CREATE_IN_PROGRESS	-	-	-
2025-12-03 16:38:05 UTC-0500	IngressSecurityGroup	ⓘ CREATE_IN_PROGRESS	-	-	-
2025-12-03 16:38:05 UTC-0500	PrivateRouteTable2	ⓘ CREATE_IN_PROGRESS	-	-	-
2025-12-03 16:38:05 UTC-0500	PublicRouteTable	ⓘ CREATE_IN_PROGRESS	-	-	-
2025-12-03 16:38:04 UTC-0500	VPC	✓ CREATE_COMPLETE	-	-	-
2025-12-03 16:37:53 UTC-0500	InternetGateway	ⓘ CREATE_IN_PROGRESS	✓ CONFIGURATION_COMPLETE	Eventual consistency check initiated	-
2025-12-03 16:37:52 UTC-0500	VPC	ⓘ CREATE_IN_PROGRESS	-	Resource creation Initiated	-
2025-12-03 16:37:52 UTC-0500	InternetGateway	ⓘ CREATE_IN_PROGRESS	-	Resource creation Initiated	-
2025-12-03 16:37:51 UTC-0500	VPC	ⓘ CREATE_IN_PROGRESS	-	-	-
2025-12-03 16:37:51 UTC-0500	InternetGateway	ⓘ CREATE_IN_PROGRESS	-	-	-

Question 1

Après l'exécution du script, on a la création des mêmes ressources que lors de l'importation du fichier vpc.yaml dans CloudFormation.

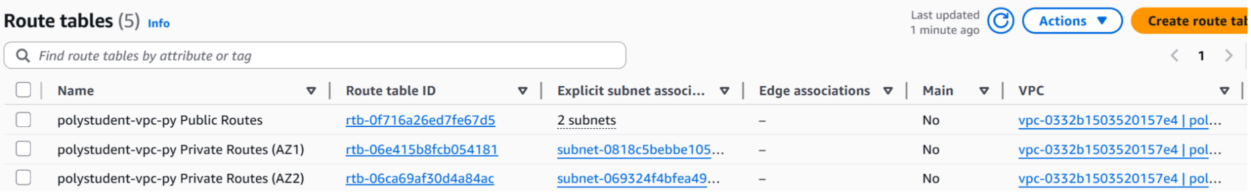


```
(venv) PS C:\Users\julav\OneDrive\Session7\INF8102\lab4> python question1.py
VPC created: vpc-0332b1503520157e4
PublicSubnet1: subnet-04225ed2ec5439fab
PublicSubnet2: subnet-0f1966adef48b4552
PrivateSubnet1: subnet-0818c5bebbe10580f
PrivateSubnet2: subnet-069324f4bfea49365
Internet Gateway attached: igw-0386647eebbb08398
Public route table configured
2 EIPs allocated successfully
NAT Gateway 1 creating in subnet-04225ed2ec5439fab...
NAT Gateway 2 creating in subnet-0f1966adef48b4552...
NAT Gateways ready
Private route tables configured
DEPLOYMENT COMPLETE
```



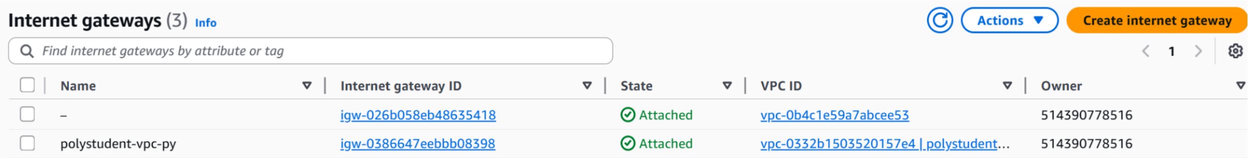
Subnets (10)

Name	Subnet ID	State	VPC	Block Public...	IPv4 CIDR
polystudent-vpc-py Private Subnet (AZ2)	subnet-069324f4bfea49365	Available	vpc-0332b1503520157e4 | pol...	Off	10.0.144.0/24
polystudent-vpc-py Public Subnet (AZ1)	subnet-04225ed2ec5439fab	Available	vpc-0332b1503520157e4 | pol...	Off	10.0.0.0/24
polystudent-vpc-py Private Subnet (AZ1)	subnet-0818c5bebbe10580f	Available	vpc-0332b1503520157e4 | pol...	Off	10.0.128.0/24
–	subnet-01a90b23ad4e6d58e	Available	vpc-0b4c1e59a7abcee53	Off	172.31.80.0/20
–	subnet-003246edbbff79620	Available	vpc-0b4c1e59a7abcee53	Off	172.31.16.0/20
polystudent-vpc-py Public Subnet (AZ2)	subnet-0f1966adef48b4552	Available	vpc-0332b1503520157e4 | pol...	Off	10.0.16.0/24



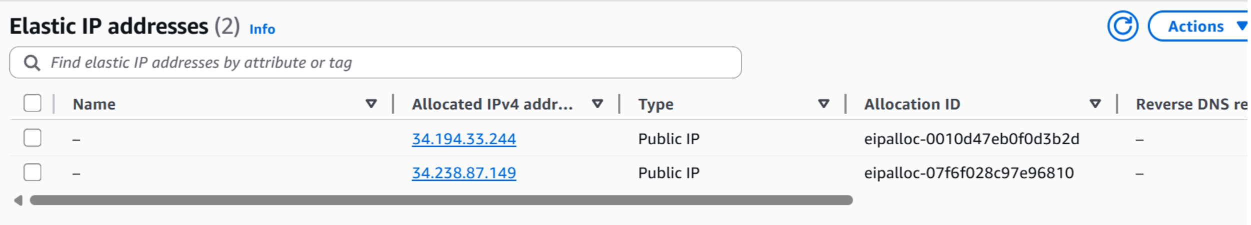
Route tables (5)

Name	Route table ID	Explicit subnet associ...	Edge associations	Main	VPC
polystudent-vpc-py Public Routes	rtb-0f716a26ed7fe67d5	2 subnets	–	No	vpc-0332b1503520157e4 | pol...
polystudent-vpc-py Private Routes (AZ1)	rtb-06e415b8fcb054181	subnet-0818c5bebbe105...	–	No	vpc-0332b1503520157e4 | pol...
polystudent-vpc-py Private Routes (AZ2)	rtb-06ca69af30d4a84ac	subnet-069324f4bfea49...	–	No	vpc-0332b1503520157e4 | pol...



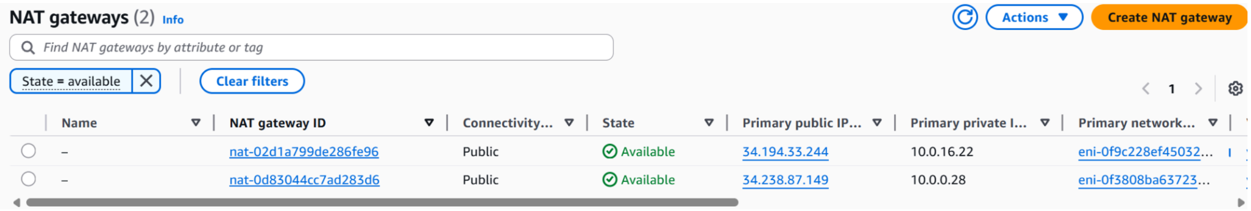
Internet gateways (3)

Name	Internet gateway ID	State	VPC ID	Owner
–	igw-026b058eb48635418	Attached	vpc-0b4c1e59a7abcee53	514390778516
polystudent-vpc-py	igw-0386647eebbb08398	Attached	vpc-0332b1503520157e4 | polystudent...	514390778516



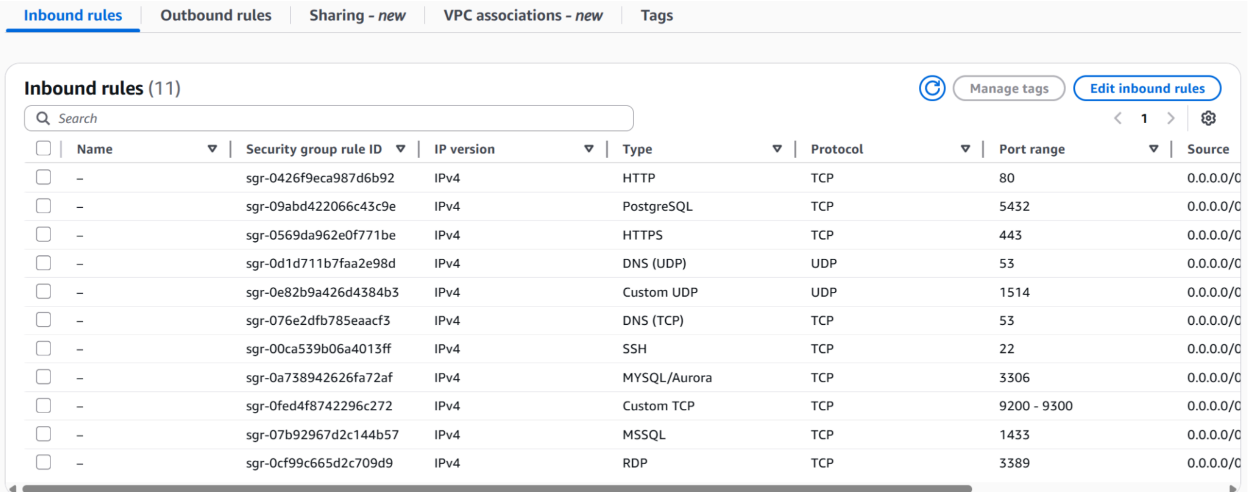
Elastic IP addresses (2)

Name	Allocated IPv4 addr...	Type	Allocation ID	Reverse DNS re
–	34.194.33.244	Public IP	eipalloc-0010d47eb0f0d3b2d	–
–	34.238.87.149	Public IP	eipalloc-07f6f028c97e96810	–



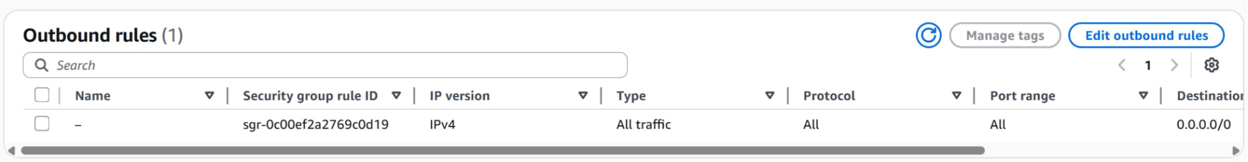
NAT gateways (2)

Name	NAT gateway ID	Connectivity...	State	Primary public IP...	Primary private I...	Primary network...
–	nat-02d1a799de286fe96	Public	Available	34.194.33.244	10.0.16.22	eni-0f9c228ef45032...
–	nat-0d83044cc7ad283d6	Public	Available	34.238.87.149	10.0.0.28	eni-0f3808ba63723...



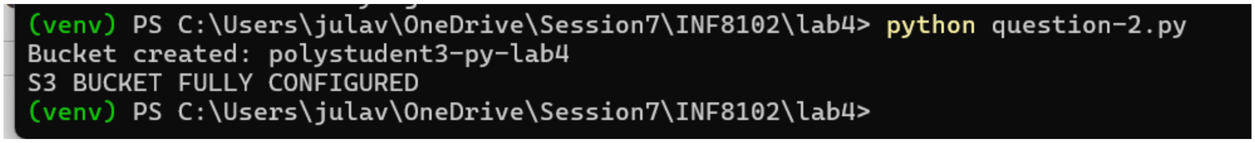
Inbound rules (11)

Name	Security group rule ID	IP version	Type	Protocol	Port range	Source
–	sgr-0426f9eca987d6b92	IPv4	HTTP	TCP	80	0.0.0.0/0
–	sgr-09abd422066c43c9e	IPv4	PostgreSQL	TCP	5432	0.0.0.0/0
–	sgr-0569da962e0f771be	IPv4	HTTPS	TCP	443	0.0.0.0/0
–	sgr-0d1d711b7faa2e98d	IPv4	DNS (UDP)	UDP	53	0.0.0.0/0
–	sgr-0e82b9a426d4384b3	IPv4	Custom UDP	UDP	1514	0.0.0.0/0
–	sgr-076e2dfb785eaacf3	IPv4	DNS (TCP)	TCP	53	0.0.0.0/0
–	sgr-00ca539b06a4013ff	IPv4	SSH	TCP	22	0.0.0.0/0
–	sgr-0a738942626fa72af	IPv4	MYSQL/Aurora	TCP	3306	0.0.0.0/0
–	sgr-0fed4f8742296c272	IPv4	Custom TCP	TCP	9200 - 9300	0.0.0.0/0
–	sgr-07b92967d2c144b57	IPv4	MSSQL	TCP	1433	0.0.0.0/0
–	sgr-0cf99c665d2c709d9	IPv4	RDP	TCP	3389	0.0.0.0/0

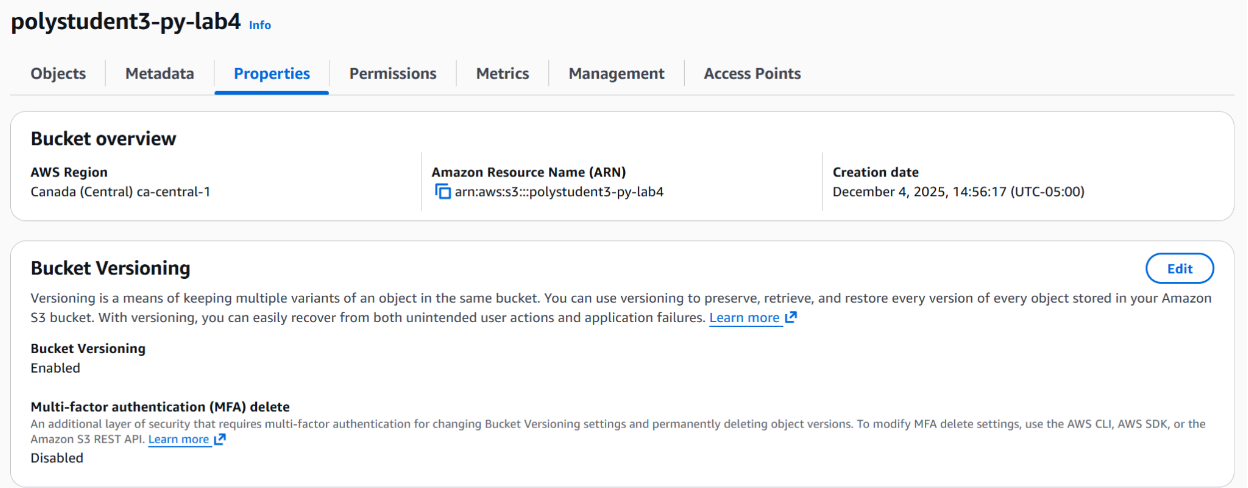


	Name	Security group rule ID	IP version	Type	Protocol	Port range	Destinatio
□	–	sgr-0c00ef2a2769c0d19	IPv4	All traffic	All	All	0.0.0.0/0

Question 2



```
(venv) PS C:\Users\julav\OneDrive\Session7\INF8102\lab4> python question-2.py
Bucket created: polystudent3-py-lab4
S3 BUCKET FULLY CONFIGURED
(venv) PS C:\Users\julav\OneDrive\Session7\INF8102\lab4>
```



Bucket overview

AWS Region
Canada (Central) ca-central-1

Amazon Resource Name (ARN)
arn:aws:s3:::polystudent3-py-lab4

Creation date
December 4, 2025, 14:56:17 (UTC-05:00)

Bucket Versioning

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. Learn more

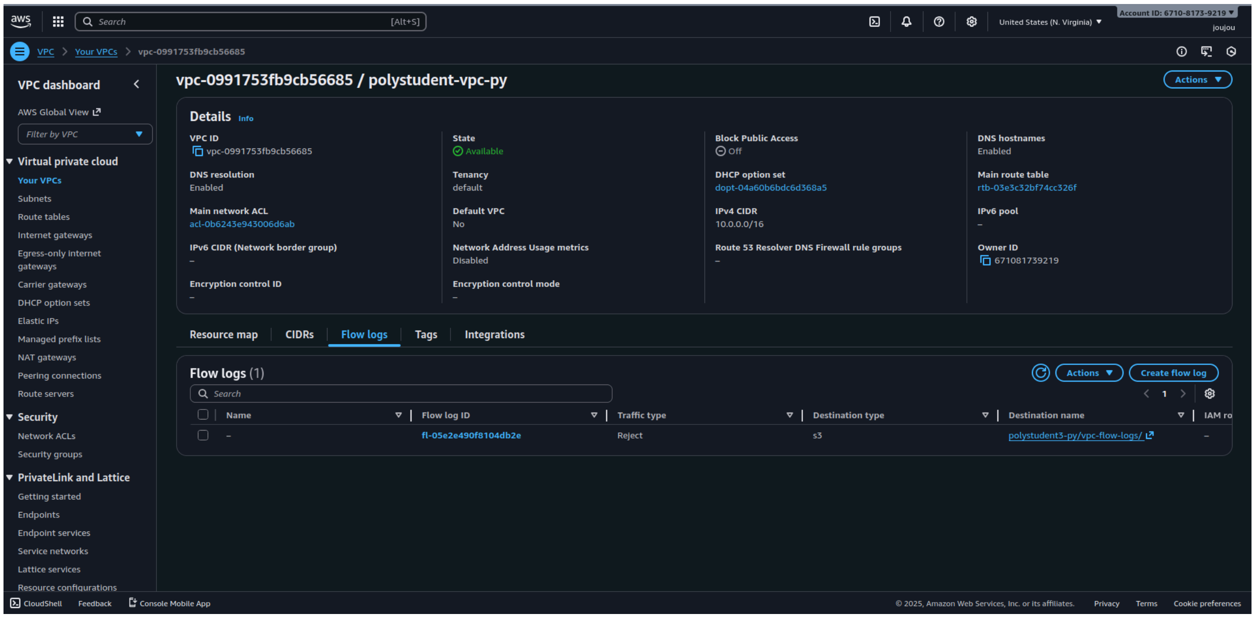
Bucket Versioning
Enabled

Multi-factor authentication (MFA) delete
An additional layer of security that requires multi-factor authentication for changing Bucket Versioning settings and permanently deleting object versions. To modify MFA delete settings, use the AWS CLI, AWS SDK, or the Amazon S3 REST API. Learn more
Disabled

Question 3

Question 3.1

On peut voir qu'après l’exécution du script modifier, un VPC flow logs est crée sur le VPC et que l’information des paquets rejetés vers le bucket.



vpc-0991753fb9cb56685 / polystudent-vpc-py

Details

VPC ID vpc-0991753fb9cb56685	State Available	Block Public Access Off	DNS hostnames Enabled
DNS resolution Enabled	Tenancy default	DHCP option set dopt-04a60b6bdc6d368a5	Main route table rtb-03e3c32bf74cc326f
Main network ACL acl-0b6243e943006d6ab	Default VPC No	IPv4 CIDR 10.0.0.0/16	IPv6 pool –
IPv6 CIDR (Network border group) –	Network Address Usage metrics Disabled	Route 53 Resolver DNS Firewall rule groups –	Owner ID 671081739219
Encryption control ID –	Encryption control mode –		

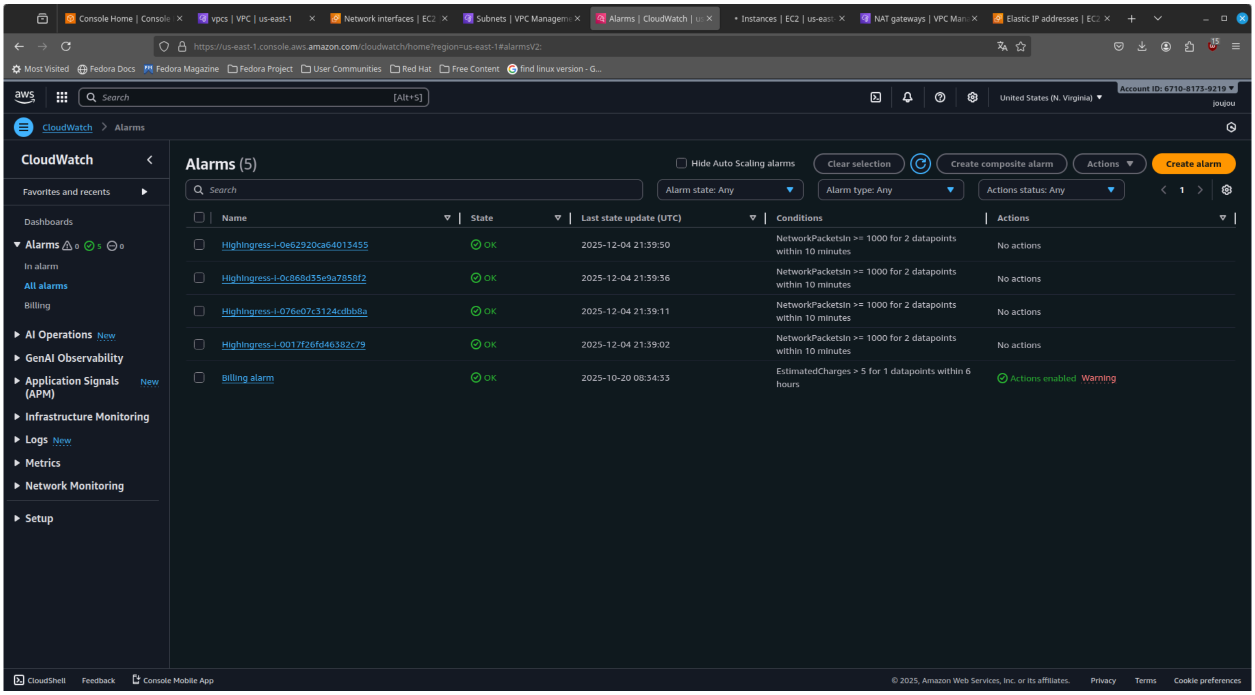
Resource map | CIDRs | Flow logs | Tags | Integrations

Flow logs (1)

Name	Flow log ID	Traffic type	Destination type	Destination name	IAM ro
–	fl-05e2e490f8104db2e	Reject	s3	polystudent3-py/vpc-flow-logs/	–

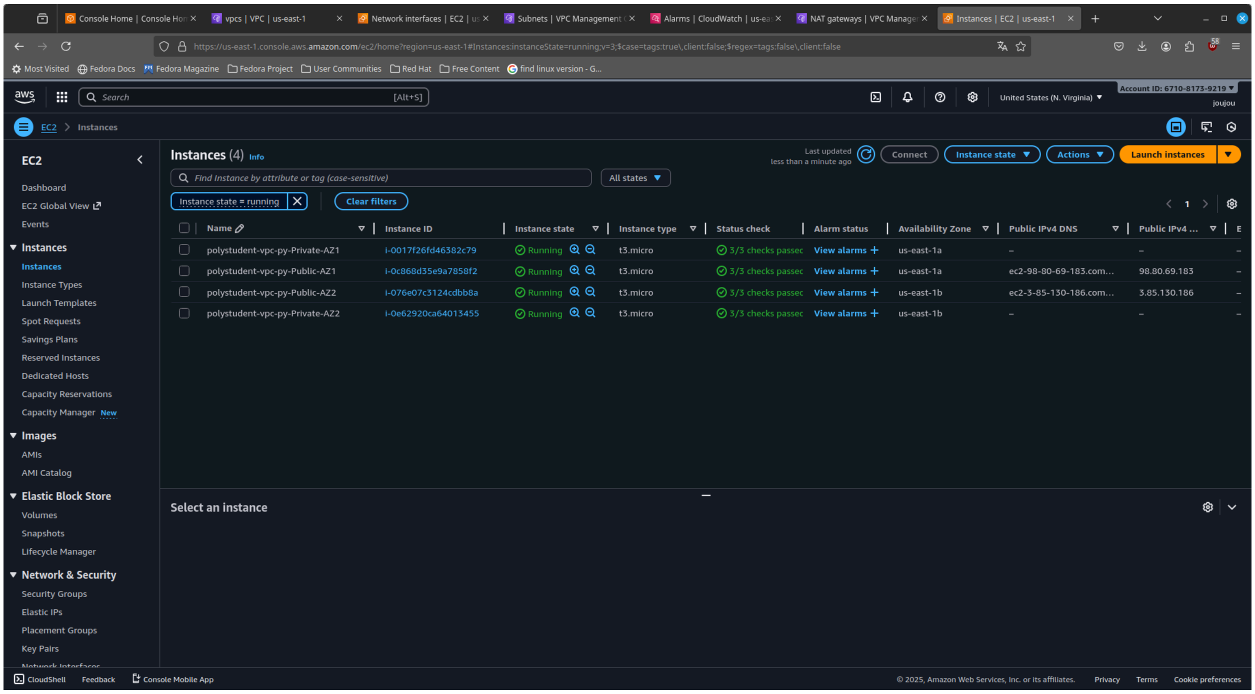
Question 3.2

Après la modification du script, il y a la création de 4 instances EC2 liées à un des sous réseaux (2 privés et 2 publics). Aussi, il y a la création d'alarme qui permet de signaler s'il y a plus de 1000 requêtes dans une fenêtre de 10 minutes.



Alarms (5)

Name	State	Last state update (UTC)	Conditions	Actions
HighIngress-i-0e62920ca64013455	OK	2025-12-04 21:39:50	NetworkPacketsIn >= 1000 for 2 datapoints within 10 minutes	No actions
HighIngress-i-0c868d35e9a7858f2	OK	2025-12-04 21:39:36	NetworkPacketsIn >= 1000 for 2 datapoints within 10 minutes	No actions
HighIngress-i-076e07c3124cdbb8a	OK	2025-12-04 21:39:11	NetworkPacketsIn >= 1000 for 2 datapoints within 10 minutes	No actions
HighIngress-i-0017f26fd46382c79	OK	2025-12-04 21:39:02	NetworkPacketsIn >= 1000 for 2 datapoints within 10 minutes	No actions
Billing alarm	OK	2025-10-20 08:34:33	EstimatedCharges > 5 for 1 datapoints within 6 hours	Actions enabled Warning



https://us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#Instances:instanceState=running;v=3;$case=tags:true\,client:false;$regex=tags:false\,client:false

United States (N. Virginia)

Account ID: 6710-8173-9219

joujou

Instances (4)

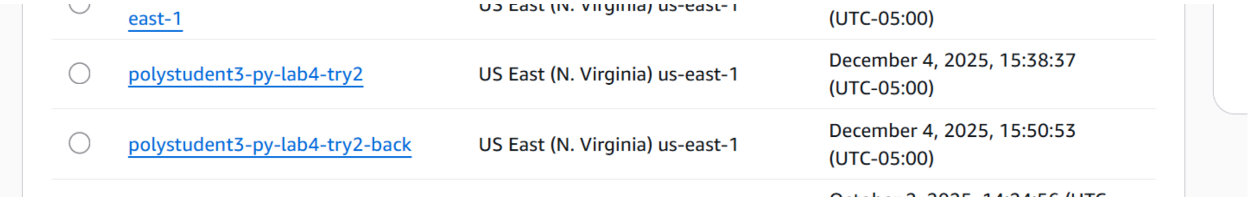
Last updated less than a minute ago

Instance state = running

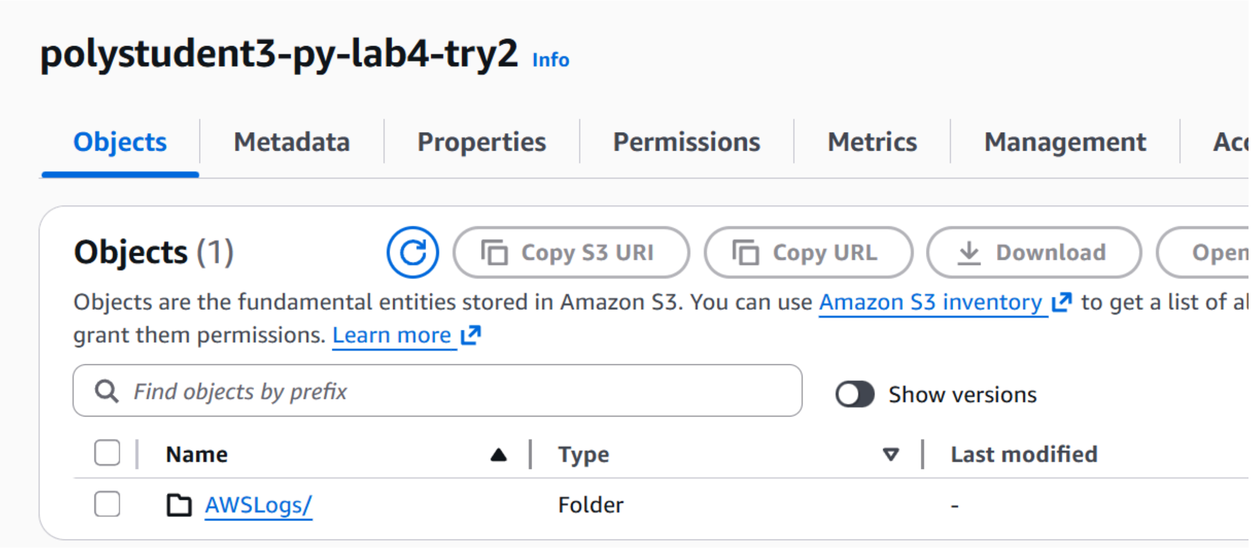
Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4 ...
polystudent-vpc-py-Private-AZ1	i-0017f26fd46382c79	Running	t3.micro	3/3 checks passec	View alarms	us-east-1a	–	–
polystudent-vpc-py-Public-AZ1	i-0c868d35e9a7858f2	Running	t3.micro	3/3 checks passec	View alarms	us-east-1a	ec2-98-80-69-183.com...	98.80.69.183
polystudent-vpc-py-Public-AZ2	i-076e07c3124cdbb8a	Running	t3.micro	3/3 checks passec	View alarms	us-east-1b	ec2-3-85-130-186.com...	3.85.130.186
polystudent-vpc-py-Private-AZ2	i-0e62920ca64013455	Running	t3.micro	3/3 checks passec	View alarms	us-east-1b	–	–

© 2025, Amazon Web Services, Inc. or its affiliates.

Question 3.3



○	east-1	US East (N. Virginia) us-east-1	(UTC-05:00)
○	polystudent3-py-lab4-try2	US East (N. Virginia) us-east-1	December 4, 2025, 15:38:37 (UTC-05:00)
○	polystudent3-py-lab4-try2-back	US East (N. Virginia) us-east-1	December 4, 2025, 15:50:53 (UTC-05:00)



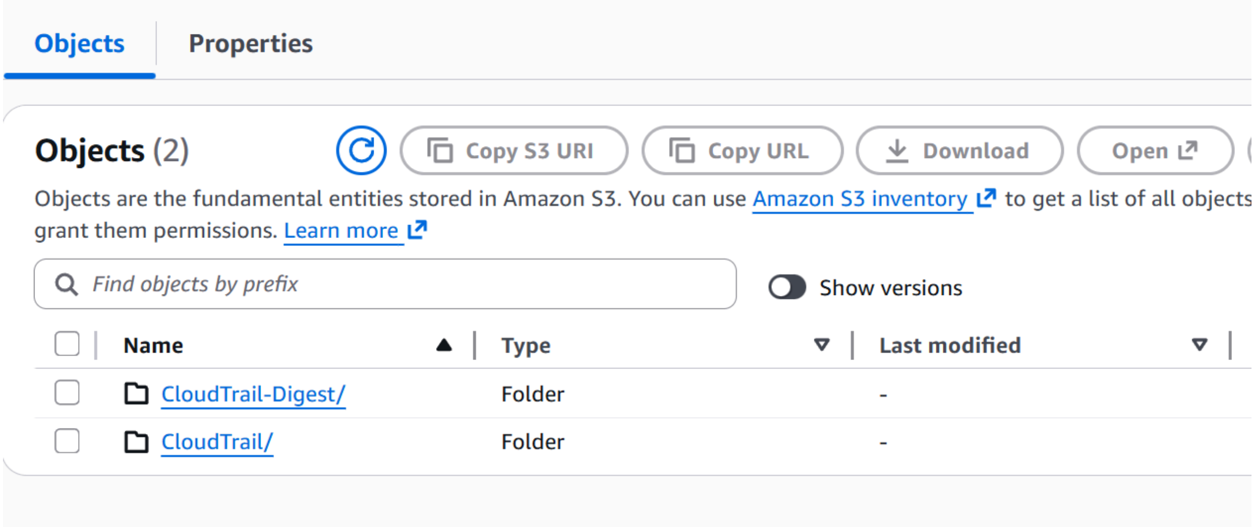
polystudent3-py-lab4-try2 Info

Objects (1)

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of al grant them permissions. Learn more

Find objects by prefix

	Name	Type	Last modified
□	AWSLogs/	Folder	-



Objects (2)

Objects are the fundamental entities stored in Amazon S3. You can use Amazon S3 inventory to get a list of all objects grant them permissions. Learn more

☐	Name	Type	Last modified
☐	CloudTrail-Digest/	Folder	-
☐	CloudTrail/	Folder	-

4.3

1. Les données de logs ne sont pas encryptées. On peut activer l’encryption des logs avec une clé personnelle en ajoutant ce paramètre dans la configuration CloudTrail.
2. Il n’est pas recommandé d’ouvrir autant de ports avec un accès public. Il est recommandé de seulement donner accès au port avec des adresses spécifiques ou utiliser un plage d’adresse pour éviter l’accès à trop de ressources.
3. Ajouter une gateway pour que les instances à l’intérieur des subnets public ne soient pas directement accessibles par l’extérieur.
4. Les groupes de sécurité n’ont pas de description. Un manque de description peut mener à une confusion sur les permissions de chaque groupe. En plus d’augmenter la maintenabilité de l’infrastructure, une description permet de ne pas donner le mauvais rôle au mauvais utilisateur, ouvrant ainsi la porte à un attaquant.
5. Il faut également limiter l’accès aux ressources depuis des adresses privées. En effet, il faut réduire cet accès au plus possible et seulement données accès pour les besoins de l'application.