



UNIVERSIDADE
LUSÓFONA

Sistemas de Informação na Nuvem

Relatório Laboratório 1

Tomás Nave, a22208623

André Jesus, a22207061

Índice

Índice	2
Introdução.....	3
Exercício 1 – Configuração de IAM	3
a) Criação de Policies de IAM e User Groups	3
b) Criação de IAM Roles para EC2	5
c) Criação do Utilizador IAM.....	6
Exercício 2 – Configuração de Infraestrutura VPC.....	7
a) b) Criação de uma VPC com 3 Subnets	7
c) d) Configuração Internet Gateway e Rotas	8
e) Configuração dos Security Groups	9
f) Configuração ACLs.....	9
Conclusão.....	10

Introdução

Este relatório descreve a execução do Laboratório 1, que envolveu a configuração de permissões IAM, criação de grupos e roles, e a configuração de uma infraestrutura em AWS VPC. O objetivo foi garantir um ambiente seguro para o projeto **DEISI WebSite**.

Exercício 1 – Configuração de IAM

a) Criação de Policies de IAM e User Groups

Passo 1: Criar os Grupos “Alunos” e Professores

- Aceder à AWS Console e navegar até **IAM > User Groups**
- Criar os grupos **Alunos** e **Professores**
- Associar policies aos respetivos grupos

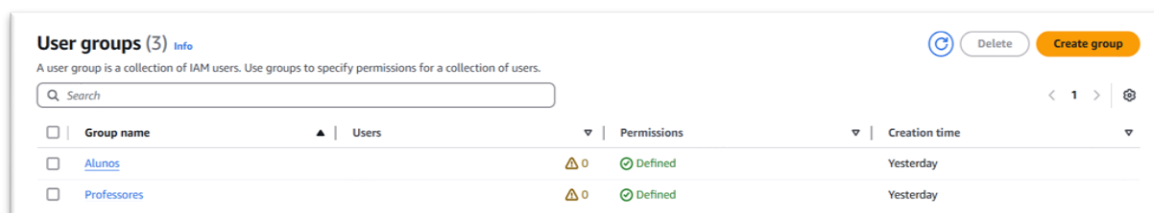


Figura 1- User Groups

Passo 2: Criar as Policies Personalizadas

- **Policy para Alunos:** Criar, modificar, remover e ler recursos dos serviços, EC2, CloudTrail, CodePipeline, CodeCommit e CodeBuild, possibilidade de modificação de tabelas no serviço DynamoDB, possibilidade de atualização no serviço ECS, possibilidade de criação de IAM Roles e Policies.
- **Policy para Professores:** Criar, modificar, ler e remover recursos dos serviços EC2, ECS, CloudTrail, CloudWatch, DynamoDB, VPC (pertence ao serviço EC2), CodeBuild, CodePipeline, CloudFormation, S3, CodeCommit e IAM.

- As policies foram configuradas para permitir operações apenas em recursos com a tag {Key: Project, Value: DEISIWebsite} e fora da região eu-central-1.

AlunosPolicy

Policy details

Type

Customer managed

Creation time

March 24, 2025, 17:22 (UTC)

Edited time

March 24, 2025, 17:35 (UTC)

ARN

arn:aws:iam:084375585515:policy/AlunosPolicy

Permissions

Entities attached

Tags

Policy versions

Last Accessed

Permissions defined in this policy

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

Q Search

Allow (8 of 439 services)

Service

Access level

Resource

Request condition

CloudTrail	Full access	All resources	Multiple
CodeBuild	Full access	All resources	Multiple
CodeCommit	Full access	All resources	Multiple
CodePipeline	Full access	All resources	Multiple
DynamoDB	Limited: Write	All resources	Multiple
EC2	Full access	All resources	Multiple
Elastic Container Service	Limited: Write	All resources	Multiple
IAM	Limited: Permissions management, Write	All resources	Multiple

Show remaining 431 services

Figura 2- Alunos Policies

Professores_Policy

Policy details

Type

Customer managed

Creation time

March 24, 2025, 17:29 (UTC)

Edited time

March 24, 2025, 17:36 (UTC)

ARN

arn:aws:iam:084375585515:policy/Professores_Policy

Permissions

Entities attached

Tags

Policy versions

Last Accessed

Permissions defined in this policy

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

Q Search

Allow (12 of 439 services)

Service

Access level

Resource

Request condition

Cloud Control API	Full access	All resources	Multiple
CloudFormation	Full access	All resources	Multiple
CloudTrail	Full access	All resources	Multiple
CloudWatch	Full access	All resources	Multiple
CodeBuild	Full access	All resources	Multiple
CodeCommit	Full access	All resources	Multiple
CodePipeline	Full access	All resources	Multiple
DynamoDB	Full access	All resources	Multiple
EC2	Full access	All resources	Multiple
Elastic Container Service	Full access	All resources	Multiple
IAM	Full access	All resources	Multiple
S3	Full access	All resources	Multiple

Show remaining 427 services

Figura 3- Professores Policies

b) Criação de IAM Roles para EC2

Passo 1: Criar uma Policy Personalizada

- Criação de uma Policy Personalizada.
- **EC2-S3-Lambda-Policy:** Ler e escrever recursos do serviço S3, invocar funções do serviço AWS Lambda, invocar AWS Translate.

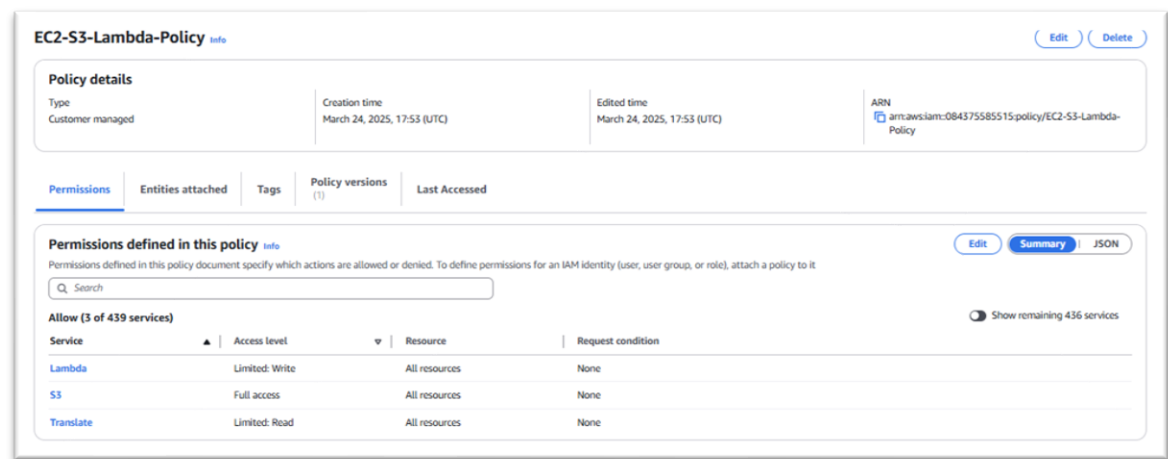


Figura 4- “EC2-S3-Lambda-Policy”

Passo 2: Criar uma IAM Role para EC2

- Criação de uma IAM Role para EC2, a EC2-S3-Lambda-Role.
- Atribuir a IAM Role a Policy EC2-S3-Lambda-Policy.

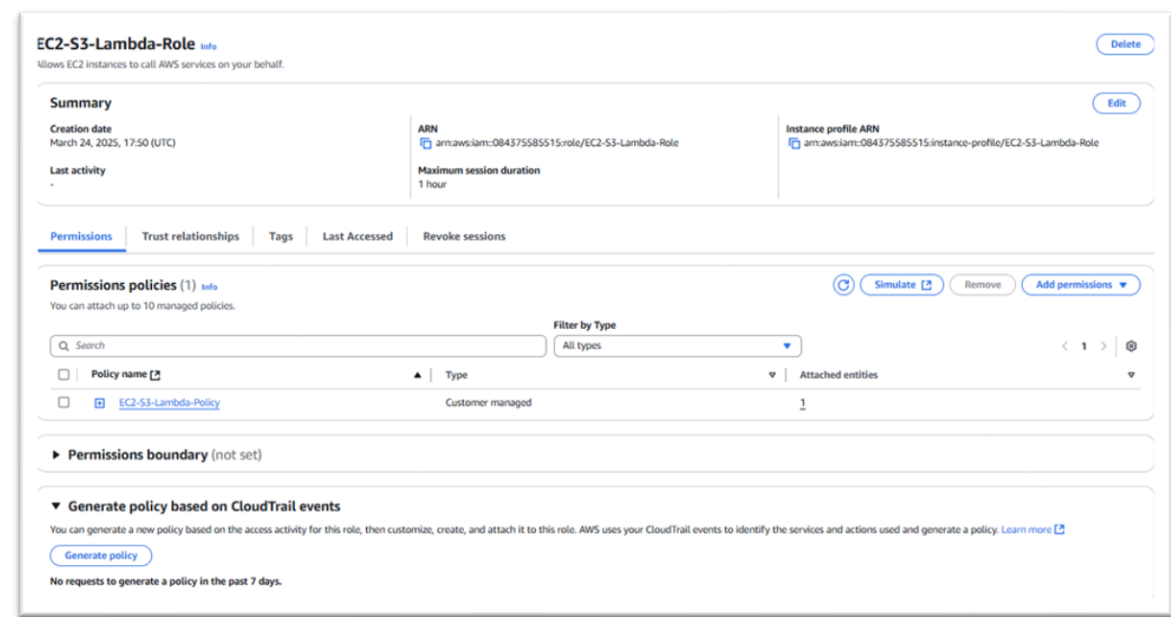


Figura 5- “EC2-S3-Lambda-Role”

c) Criação do Utilizador IAM

Passo 1: Criar Utilizador IAM

- Criar um utilizador IAM com permissões apenas para realizar o Exercício 2.

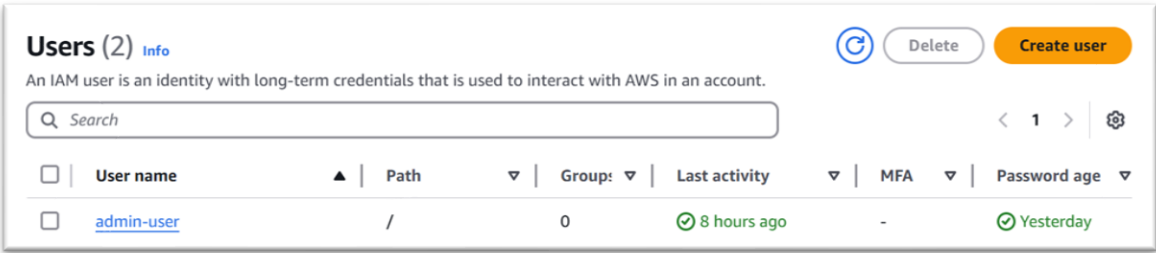


Figura 6- Utilizador IAM

Passo 2: Atribuir Policies ao Utilizador IAM

- Criar uma policy personalizada, que permita a gestão de VPC, subnets, Internet Gateway, rotas, Security Groups e ACLs.
- Atribuir a policy ao Utilizador IAM, para poder então realizar o exercício 2.

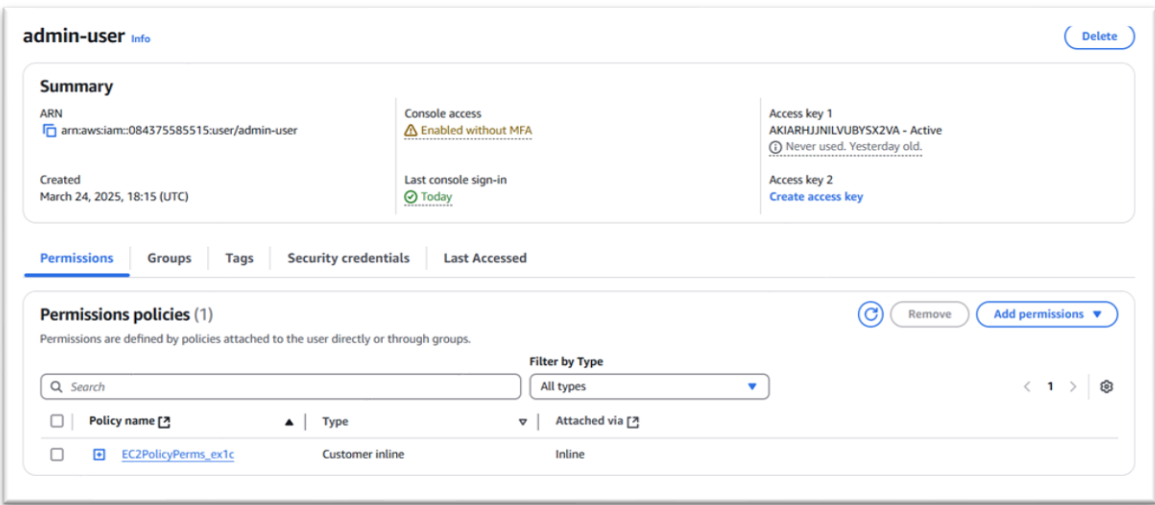


Figura 7- Utilizador IAM com a Policy

Exercício 2 – Configuração de Infraestrutura VPC

Primeiramente tivemos de fazer login, no AWS Console, com o Utilizador IAM que criámos anteriormente no exercício **c) Criação do Utilizador IAM**.

a) b) Criação de uma VPC com 3 Subnets

Passo 1: Criar VPC com 3 Sub

- Navegar para **VPC > Create VPC**.
- Criar a VPC com as 3 subnets.

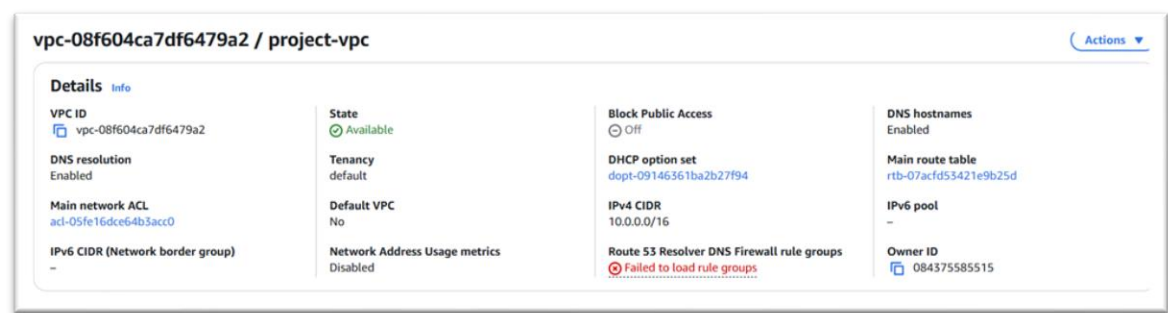


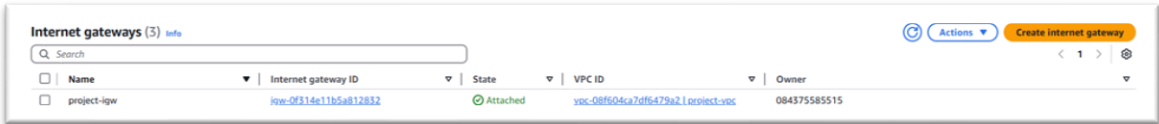
Figura 8- VPC



Figura 9- Resource Map VPC

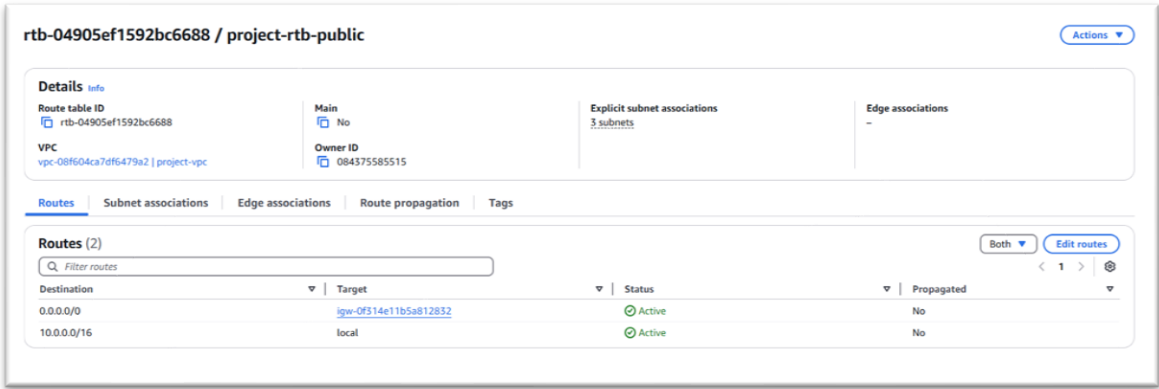
c) d) Configuração Internet Gateway e Rotas

- Criar um Internet Gateway e associá-lo à VPC.
- Criar uma Route Table e adicionar uma rota padrão (0.0.0.0/0) para o Internet Gateway.



Internet gateways (3)				
Name	Internet gateway ID	State	VPC ID	Owner
project-igw	igw-0f314e11b5a812832	Attached	vpc-08f604ca7df6479a2 project-vpc	084375585515

Figura 10- Internet Gateway



rtb-04905ef1592bc6688 / project-rtb-public			
Details		Main	Explicit subnet associations
Route table ID	rtb-04905ef1592bc6688	No	3 subnets
VPC	vpc-08f604ca7df6479a2 project-vpc	Owner ID	084375585515
Routes (2)			
Destination	Target	Status	Propagated
0.0.0.0/0	igw-0f314e11b5a812832	Active	No
10.0.0.0/16	local	Active	No

Figura 11- Route Table

e) Configuração dos Security Groups

- Criar Security Group com:
 - **Outbound:** permitir todas as portas.
 - **Inbound:** permitir apenas 22 (SSH), 80 (HTTP) e 443 (HTTPS).

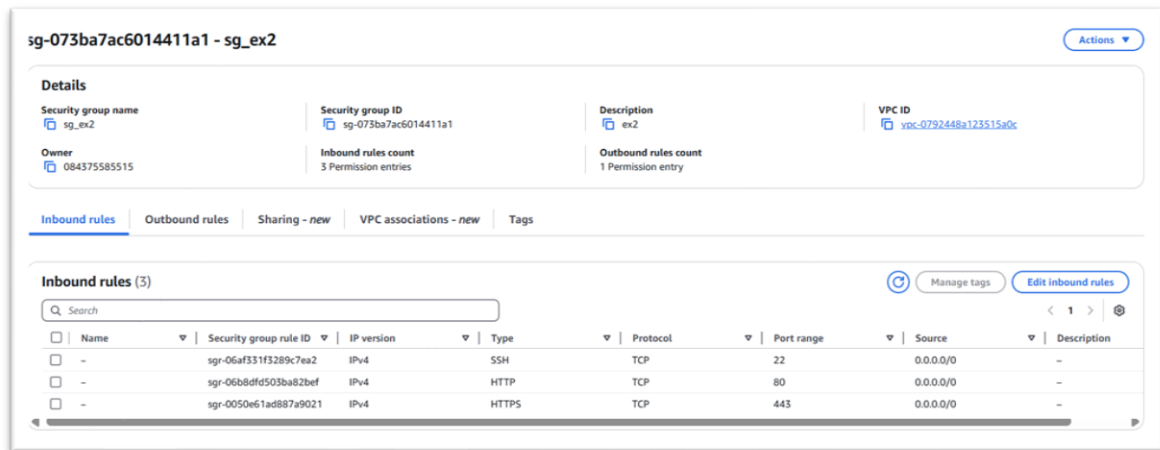


Figura 12- Security Group

f) Configuração ACLs

- Criar Network ACL e definir:
 - **Outbound:** permitir todos os destinos.
 - **Inbound:** permitir apenas portas 22, 80 e 443, bloqueando as restantes.

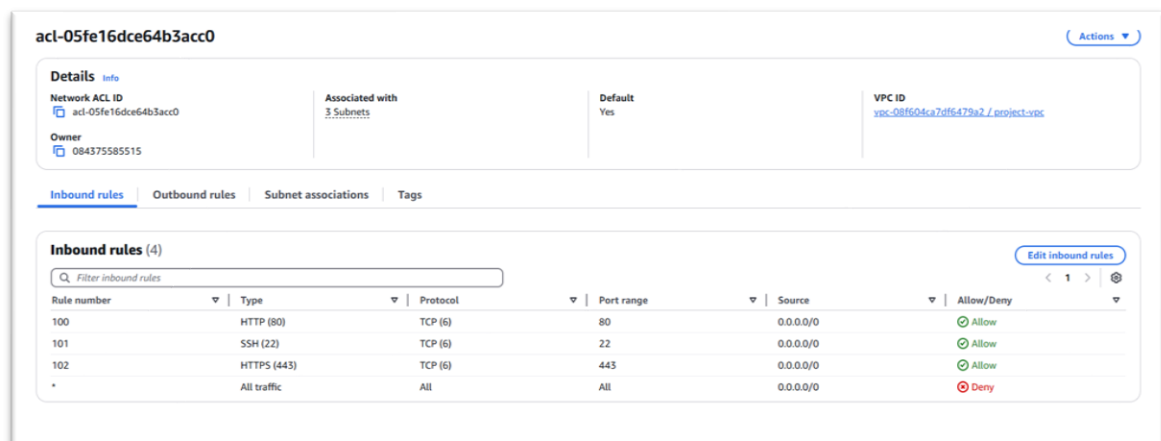


Figura 13- Network ACL

Conclusão

Para concluir este Laboratório 1 proporcionou uma aplicação prática dos conceitos de gestão de permissões IAM e configuração de infraestrutura VPC na AWS, permitindo uma melhor compreensão da segmentação de acessos, restrições baseadas em tags e regiões, bem como a implementação de uma infraestrutura segura e eficiente na nuvem.