

## Sujet d'épreuves de la 48<sup>e</sup> Compétition Nationale des Métiers

# MÉTIER N°53

# CLOUD COMPUTING

Jour 1

Soumis par :

Jonathan Bruneau Expert adjoint WorldSkills France

# DESIGN AND DEPLOYMENT OF A SECURE, SCALABLE IMAGE PROCESSING PIPELINE ON AWS

DUREE TOTALE DE L'ÉPREUVE	6 heures
---------------------------	----------

DIFFUSION DU SUJET	<b>C1</b> <i>Découvert le jour de la compétition</i>
--------------------	---

**Grading :** The grading for this part is 33 points.

You have the right to the Internet but no AI, whether in a code editor or online or in any other form. Should you be caught using this technology, the sub-section in question will be retrieved and the comment "AI cheats" with a grade of 0 will be awarded. If you're caught a second time, you'll be eliminated from the day's event or even from the competition.

If you're really stuck, or need a break, just raise your hand.

To complete this project, you have access to an AWS account. To demonstrate your ability to properly use this cloud provider, we require that you follow all best practices defined in the Well-Architected Framework.

# PART 1 - INTEGRATION AND DEPLOYMENT OF IMAGE PROCESSING PIPELINE USING AWS SERVICES

## CONTEXT

The company "Ctrl+Z", which specializes in image processing, continuously generates a large number of photos. The division director has tasked the IT department with deploying a serverless application to process these photos

To meet this requirement, you have been hired to implement the solution. As part of this, the development team has provided you with a script designed to meet the objectives set by your director.

## GOAL

Based on the technical details provided, you must design and deploy a cloud architecture to support the image processing pipeline. Your work will be assessed on how well it follows the specifications given and how closely it aligns with AWS best practices, including the Well-Architected Framework.

## DIAGRAM

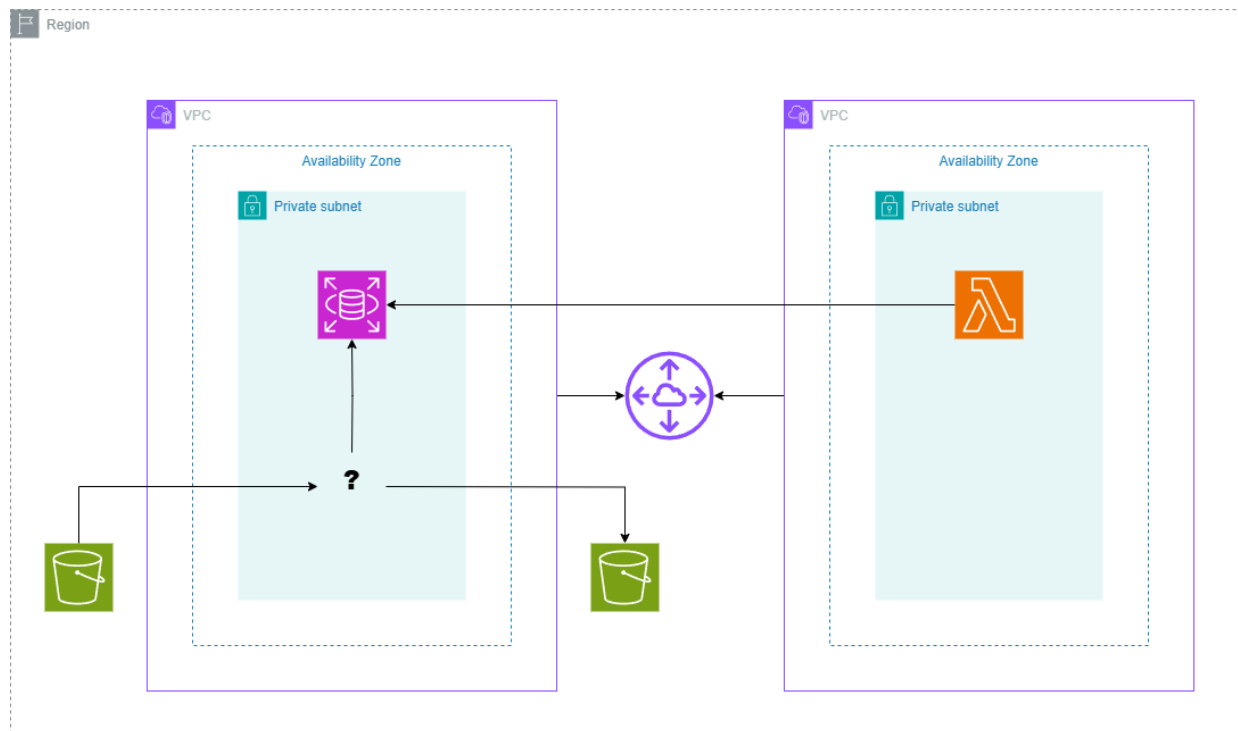


Figure 1 Non-detailed diagram – Step 1

## TECHNICAL DETAILS

### Storage

The infrastructure branch of the IT department will deploy an S3 bucket for you to receive the photos in your environment, as well as another S3 bucket where the director expects to retrieve the results.

To ensure proper integration with your colleagues' software, you are asked not to delete these shared storage spaces.

## Processing

The development branch of the IT department has provided you with the script to process the images. It runs using Python 3.12 and relies on well-known libraries, which are not included. Unfortunately for you, your contacts in that branch have gone on vacation...

From here, deploy the development team's program on the service you would recommend. Don't forget to configure the script to interface with the S3 buckets as well as with an SQL database.

Description	Valeur
Computing resource name and/or tag name	app-processing
Runtime	Python 3.12
Time estimated	>=10s
Memory	1 Gb

## Database

The image processing script relies on a MariaDB database to log the image processing tasks performed. You may choose any service you prefer to deploy this database.

The SQL scheme expected by the script is as follows:

```
CREATE DATABASE IF NOT EXISTS app_data
USE app_data;
CREATE TABLE IF NOT EXISTS file
(
  id INT PRIMARY KEY NOT NULL,
  content_key VARCHAR(260) NOT NULL,
  content_hash VARCHAR(256) NOT NULL
);
```

Description	Valeur
Database name and/or tag name	app_data
Engine	MariaDB
Version	11.4.5
Instance class	db.t3.micro
Allocated storage	10 Gb
Username	Admin

## Extraction

Your director sent you a script before you began your work to list the processing tasks that have been completed. According to him, the script once again runs on Python 3.12 and uses well-known libraries that are not included. He, too, has gone on vacation...

You must deploy this script on the Lambda service and configure it to interface only with the previously deployed database.

Description	Valeur
-------------	--------

Function name and/or tag name	app-extraction
Runtime	Python 3.12
Memory	128 Mb

## Network

For this infrastructure, you need to deploy two VPCs.

- The first will be for the database and the service you choose to run the image processing script.
- The second will be for your director's script.

Considering that other services on different VPCs within the company may need to access the database, choose wisely how to interconnect the VPCs.

Description	Valeur
VPC name and/or tag name	app_vpc_a
VPC CIDR	10.0.0.0/16
Subnet1 name and/or tag name	subnet_a1
Subnet1 CIDR	10.0.1.0/24
Subnet2 name and/or tag name	subnet_a2
Subnet2 CIDR	10.0.2.0/24
Route table name and/or tag name	app_route_a

Table 1 VPC A

Description	Valeur
VPC name and/or tag name	app_vpc_b
VPC CIDR	10.1.0.0/16
Subnet1 name and/or tag name	subnet_b1
Subnet1 CIDR	10.1.1.0/24
Subnet2 name and/or tag name	subnet_b2
Subnet2 CIDR	10.1.2.0/24
Route table name and/or tag name	app_route_b

Table 2 VPC B

# PART 2 - ENHANCING SECURITY AND OBSERVABILITY IN AWS-BASED IMAGE PROCESSING WITH DYNAMODB INTEGRATION

## CONTEXT

The security branch has detected a violation of the company's security policy in the script you just implemented. To address this, they have modified the processing script and would like you to integrate a DynamoDB database into the infrastructure so they can log actions.

## GOAL

Following updated security requirements, you are required to modify the existing architecture to include a DynamoDB table for logging processing activity. Using the details provided, update the system to ensure scalability and reliability. Evaluation will be based on your ability to meet the scenario's technical constraints and apply AWS best practices appropriately.

## DIAGRAM

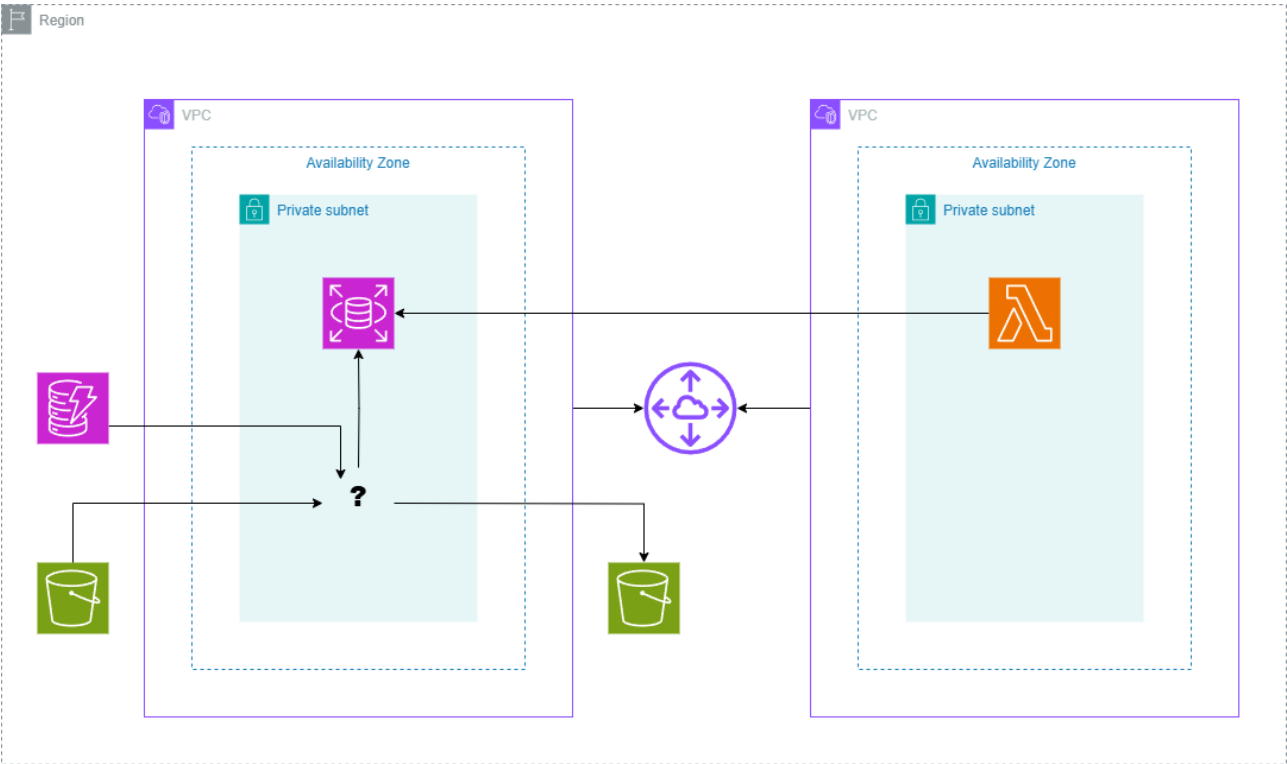


Figure 1 Non-detailed diagram – Step 2

## TECHNICAL DETAILS

### DynamoDB

The DynamoDB database will need to be deployed on your infrastructure account. The script will need to be configured once again to accommodate the new requirements. The DynamoDB database will have two keys:

- "key": The name of the processed image
- "hash": The encrypted value derived from the processed image

You are unsure how many requests will be made to this database, so deploy it with scalability in mind.

Description	Valeur
-------------	--------

Table name and/or tag name	app-log
Partition key	key

# PART 3 - SECURING CREDENTIAL MANAGEMENT WITH AWS SECRETS MANAGER IN IMAGE PROCESSING PIPELINES

## CONTEXT

The security branch wants the database password to **not** be stored in the environment variables of the scripts you just deployed. They have therefore modified the scripts once again to introduce **Secret Manager** into your infrastructure.

## GOAL

To enhance credential security, adapt the infrastructure by integrating AWS Secrets Manager. Configure it to store and rotate the database password securely, and modify the script to use this new setup. Your solution will be reviewed based on how well it respects the given requirements and incorporates security best practices from the AWS Well-Architected Framework.

## DIAGRAM

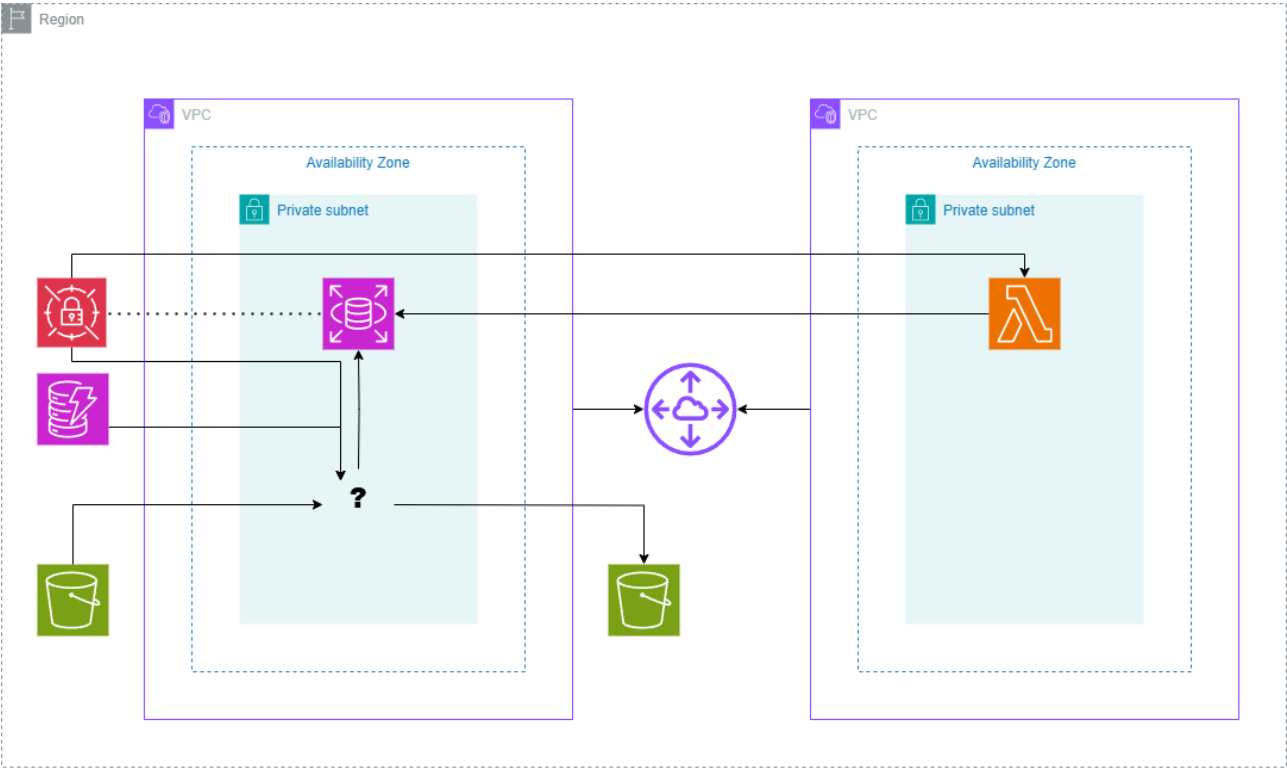


Figure 1 Non-detailed diagram – Step 3

## TECHNICAL DETAILS

### Secret Manager

Deploy a secret on Secret Manager and modify the script to account for it. The script will need to be configured once again to meet the new requirements.

Description	Valeur
Secret name and/or tag name	app-secret



Rotation	Every 14 days
----------	---------------