



Sujet d'épreuves des Finales Nationales de la 47^e Compétition des Métiers

MÉTIER N°53

CLOUD COMPUTING

Soumis par :

Brandon **ANCELIN**, Expert WorldSkills France

1. EXPLICATION DU SUJET – JOUR 1

DUREE TOTALE DE L'ÉPREUVE	6 heures
DIFFUSION DU SUJET	Découvert le jour de la compétition

Contents

This Test Project consists of the following documentation/files:

- 47_FNAT_53_Cloud-Computing_Day1.pdf
- 47_FNAT_53_Cloud-Computing_Day1-Diagram.pdf

Context

As an AWS Consultant, your primary responsibility is to address customer inquiries and fulfill their specific request to migrate their existing infrastructure to the cloud, building the foundation for this migration process. Fortunately, you have access to a well-defined AWS schema and a comprehensive description which outlines the necessary steps and requirements for this migration process. With your in-depth knowledge of AWS technologies, you will be able to provision and configure the necessary AWS services in the cloud environment. Leveraging your proficiency in AWS technologies, you will play a vital role in enabling the customer to reap the benefits of cloud computing, such as: scalability, flexibility, cost-efficiency, and enhanced business agility – thereby driving their overall digital transformation journey.

AWS

During the competition day, you will utilize the provided AWS Account, which is personal and should not be shared with others. Please ensure exclusive use of this account. Your activities should be confined to the eu-west-3 (Paris) region. It's important to note that certain global services, unrelated to specific regions, might also be required.

Description of project and tasks

Summary

With all the diagram and the descriptions below, create the AWS environment needed to host the application for your customer named **Innovatech**.

Do you best by applying the AWS Pillars rules to fit the customer's need.

The diagrams have been created with the official AWS template; it can be found here:

<https://aws.amazon.com/architecture/icons/>

Diagram – AWS Account Basics

Allocate all AWS services within the Paris region, unless they are global AWS services not associated with any specific region.

Some diagram may not show the Region to make the diagram clearer.

Diagram – Routing View

This diagram shows you at a high level how you should configure the connectivity of your VPC, private subnet and public subnet.

The name of the different AWS Services and route table content in this diagram is to demonstrate only and may not be the names or values that you must use for your customer. Please refer to another diagram or description for specific name if required. The public route tables must be the same for each AZ

With this diagram, you know how you should deploy your infrastructure. You can see the details of the different route tables, both public and private. The default route of the private route tables must be the NAT gateway within its own AZ.

Diagram – Network View.

This diagram shows the configuration of your public and private subnets, including the subnet names, the required Availability Zones, and the associated CIDR blocks.

The VPC name must be **Production VPC**.

Diagram – Application View 1

This Application view Diagram enable you to know how you should deploy the application.

You can see that there are 2 applications, one for the frontend and one for the backend.

The frontend app is in a public subnet to be reachable from internet. The frontend application need to call the backend application.

The frontend application uses a backend API hosted in a private subnet, to call the database hosted on specific private AZs.

You must use two Auto Scaling Group, **prod-app-front-asg** and **prod-app-back-asg**

Diagram – Application View 2

This diagram omits certain details from **Diagram – Application View 1**, such as AZs redundancy, to focus on the application itself like connectivity between AWS Services and its public accessibility through the Application Load Balancer named **prod-app-front-alb**.

The backend app must open port 80/tcp incoming from the front-end, the front-end app must open port 80/tcp incoming from the Application Load Balancer.

The **prod-app-back** should not use internet to reach the Amazon S3 Services, but a specific gateway inside the VPC instead.

The database must open the port 3306/tcp incoming from the backend app.

The bucket name must start with **prod-app-front-assets-**. This bucket is used for the assets used by the front-end app and must be accessible by the **prod-app-back** EC2 instances.

Technical Details – prod-app-db

DESCRIPTION	VALUE
Amazon RDS database	Serverless v2 (Aurora MySQL Compatible)
DB Cluster identifier	prod-app-db
Minimum ACUs	0.5
Maximum ACUs	2
Database name	innovatech
Database username	admin
Database password	init1234*
Number of writer node	1
Number of reader node	1
Connectivity	Only accessible from prod-app-back instances

You can find the export database here:

<http://wsfrskill53.s3.eu-west-3.amazonaws.com/47CNAT/C1/innovatech.sql>

Technical Details – S3

DESCRIPTION	VALUE
S3 Bucket prefix name	prod-app-front-assets-
Object Lock (WORM)	Disabled
Permissions	prod-app-back EC2 instances: Read Only
Access rules	Only by S3 Bucket policies

All best practices about security but also recovery object in case of mistakes must be enabled.

Technical Details – prod-app-back-asg

DESCRIPTION	VALUE
Minimum number of hosts	1
Maximum number of hosts	5
Desired host	3

The ASG must recreate new host if the EC2 instance check failed or if the api is down.

Technical Details – prod-app-front-asg

DESCRIPTION	VALUE
Minimum number of hosts	1
Maximum number of hosts	5
Desired host	3

The ASG must recreate new host if the EC2 instance check failed or if the web server is down.

Technical Details – prod-app-front-alb

DESCRIPTION	VALUE
Target group name	prod-app-front-tg

Technical Details – prod-app-back-alb

DESCRIPTION	VALUE
Target group name	prod-app-back-tg

Technical Details – Application Details

There are two applications: one for the front-end, another one for the backend. The apps must be hosted on EC2 instances with Amazon Linux 2023 image.

The front-end application must be hosted on EC2 instances named **prod-app-front** in a ASG (as shown in the **Application View 1**). The program is a binary executable ready to use. You might need to use -h parameter to see the available options.

The backend application must be hosted on EC2 instances named **prod-app-back** in a ASG (as show in the **Application View 1**). The program is a binary executable ready to use. You might need to use -h parameter to see the available options.

The MySQL database is hosted on a Serverless Amazon RDS Aurora (MySQL Compatibility).

Technical Details – prod-app-back and prod-app-front role

If you need to connect to the instance, create and use a IAM Role as below:

DESCRIPTION	VALUE
prod-app-back instance role name	prod-app-back-role
prod-app-front instance role name	prod-app-front-role

The IAM Role must use AWS Managed policy.

Technical Details – Security Groups

Ensure that the security groups for ALB, EC2 instances, and RDS share the same name followed by '-sg.'

Example: EC2 instances “prod-app-front” should use a security group named “prod-app-front-sg”

Technical Details – IAM Role / IAM User:

An IAM user **Alice** must have permission which allow the user to do anything with all resources in the AWS Account using a AWS managed policy.

The IAM role of **prod-app-front** must have a role containing the same name + append -role at the end. For prod-app-front, it should be **prod-app-front-role** and must have the permission to the AWS Services needed for the web service. Same for prod-app-back.

Technical Details – Front-end and backend binaries

The server application has two versions, depending on your environment: x86_64 and ARM. They are both statically linked and are binaries executable, ready to use. It has been tested on Amazon Linux 2023.

You can find the binaries here:

https://wsfrskill53.s3.eu-west-3.amazonaws.com/47CNAT/C2/CR01/webserver_arm

https://wsfrskill53.s3.eu-west-3.amazonaws.com/47CNAT/C2/CR01/webserver_x86_64

Règlement

En plus du règlement officiel de la compétition, s'ajoute :

Utilisation d'internet

L'accès à internet est autorisé. Vous pouvez naviguer sur les forums, documentations, etc...

Cependant, quelques restrictions s'appliquent :

- Interdiction de se connecter à des sites internet nécessitant :
 - Un nom d'utilisateur et/ou mot de passe
- Utilisation de site publique uniquement.
 - Pas de site personnel (même ouvert publiquement)
- Assistance IA
 - ChatGPT
 - Tout autre possibilité de se reposer sur une IA

Liste des Annexes

- **Annexe 1: 47_FNAT_53_Cloud-Computing_Day1.pdf**
- **Annexe 2: 47_FNAT_53_Cloud-Computing_Day1-Diagram.pdf**
- **Annexe 3: <https://aws.amazon.com/architecture/icons/>**