CRITICALCASE

CRITICALCASE

Navigation and Lifestyle Project

Architecture Low Level Design

Version: <0.1 07/04/2023>

Customer: Wevee

Objective: the goal of this document is to describe the infrastructural architecture realized for the customer by Criticalcase on AWS Cloud.

Limits: the application environment is out of the scope of this document.

Criticalcase S.r.l.

P.IVA: 09733390018 | REA: TO - 1076960
CAP. SOC.: 120.000,00 Euro i.v.

SEDE LEGALE - Via Nicola Fabrizi, 136 - 10145 – Torino
SEDE OPERATIVA - Via Chambery 93/107, 10142 Torino
Tel: 011.5097366 | Fax: 011.04.32.771
info@criticalcase.com | criticalcase.com

CRITICALCASE

Summary

1 Project scope

The main goal of Wevee is to have a single-application-based, UK-based LAMP infrastructure running on AWS Cloud.

The Environments realized are two:

- Stage
- Production

Criticalcase S.r.l.

P.IVA: 09733390018 | REA: TO - 1076960
CAP. SOC.: 120.000,00 Euro i.v.

SEDE LEGALE - Via Nicola Fabrizi, 136 - 10145 – Torino
SEDE OPERATIVA - Via Chambery 93/107, 10142 Torino
Tel: 011.5097366 | Fax: 011.04.32.771
info@criticalcase.com | criticalcase.com

2 Cloud and Infrastructure Services

2.1 Infrastructural Scope

Criticalcase boundary:

- Delivery of VMs and services (Firewall, Load Balancer, Storage, VPC, Backup)
- Setup, configuration and tuning of all the infrastructure services:
    - Firewall (security group)
    - Routing Rules, Subnetting e Networking in general
    - Load Balancer with certificate
    - Backup
    - Cloudwatch Alarms and Logs
- Setup and configuration of the Middleware (Apache) based on customer requirements.
- Create all the Environments via Automation

2.2 Environments

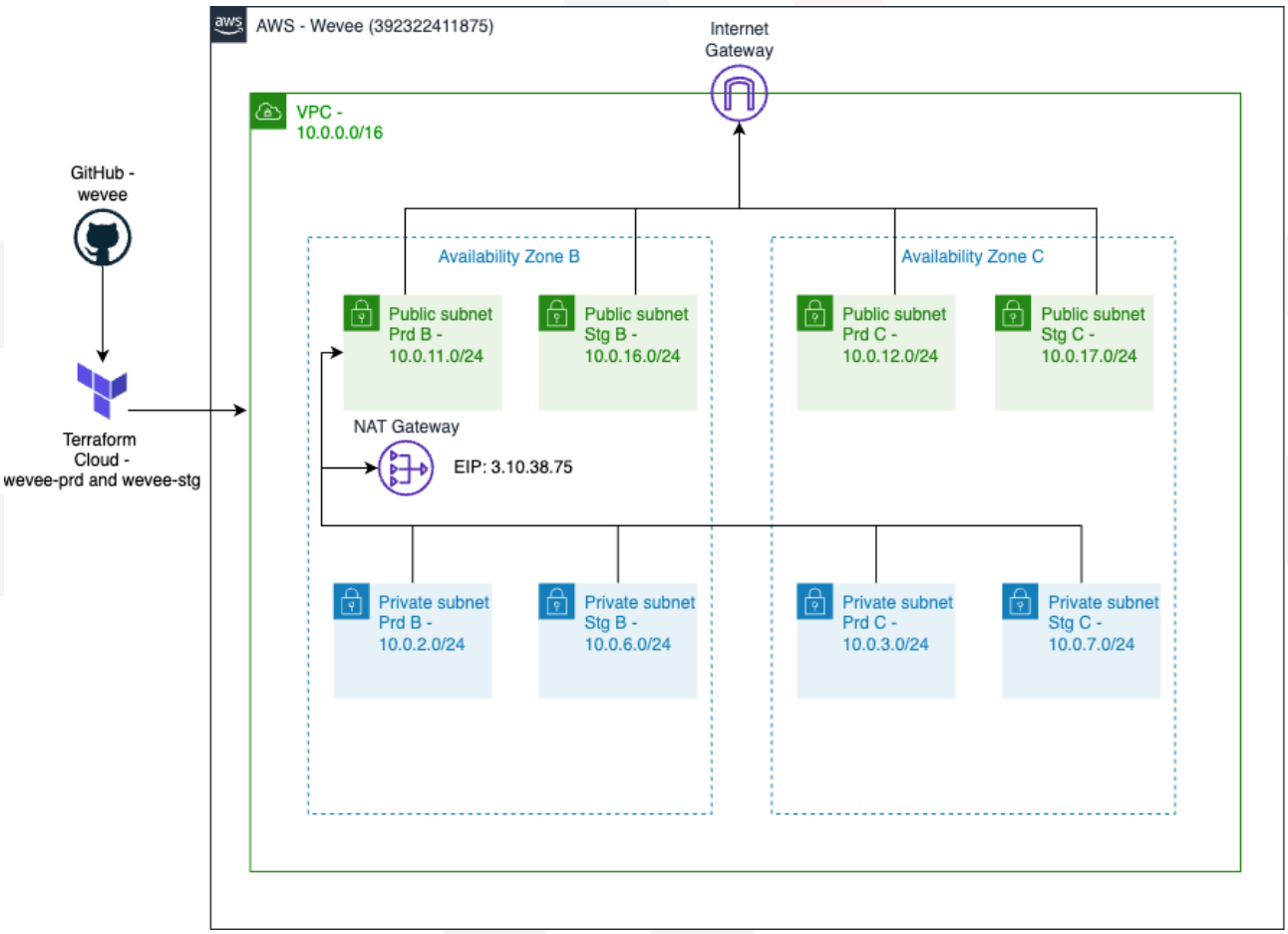
Environments. There are two different Environments, very similar each other:

- **Stage (Stg)** environment deployed as of March 2023
- **Production (Prd)** environment deployed as of March 2023

Cloud providers. The whole infrastructure is deployed on an AWS Cloud account dedicated to Wevee

Regions. Within AWS, everything is inside London region (eu-west-2)

2.2.1 Virtual Private Cloud (VPC)



The VPC is configured with **CIDR 10.0.0.0/16** CIDR in London region.

2 private subnets and 2 public subnets have been created for production environment, 2 private subnets and 2 public subnets for staging:

Name	Type	Availability Zone	CIDR	Subnet ID
Private_PROD_B	Private	eu-west-2b	10.0.2.0/24	subnet-0c261ad6728cd8490
Private_PROD_C	Private	eu-west-2c	10.0.3.0/24	subnet-0f446664dd15bc36f
Public_PROD_B	Public	eu-west-2b	10.0.11.0/24	subnet-0b9a3a6079fd849e8

Public_PROD_C	Public	eu-west-2c	10.0.12.0/24	subnet-000b0cfd3b2404db4
Private_STG_B	Public	eu-west-2b	10.0.6.0/24	subnet-0bba94b4c54d247b5
Private_STG_C	Private	eu-west-2c	10.0.7.0/24	subnet-0317b8a8d50551e82
Public_STG_B	Private	eu-west-2b	10.0.16.0/24	subnet-0be9a0423f9cd91f0
Public_STG_C	Private	eu-west-2c	10.0.17.0/24	subnet-0d10bc043c731843f

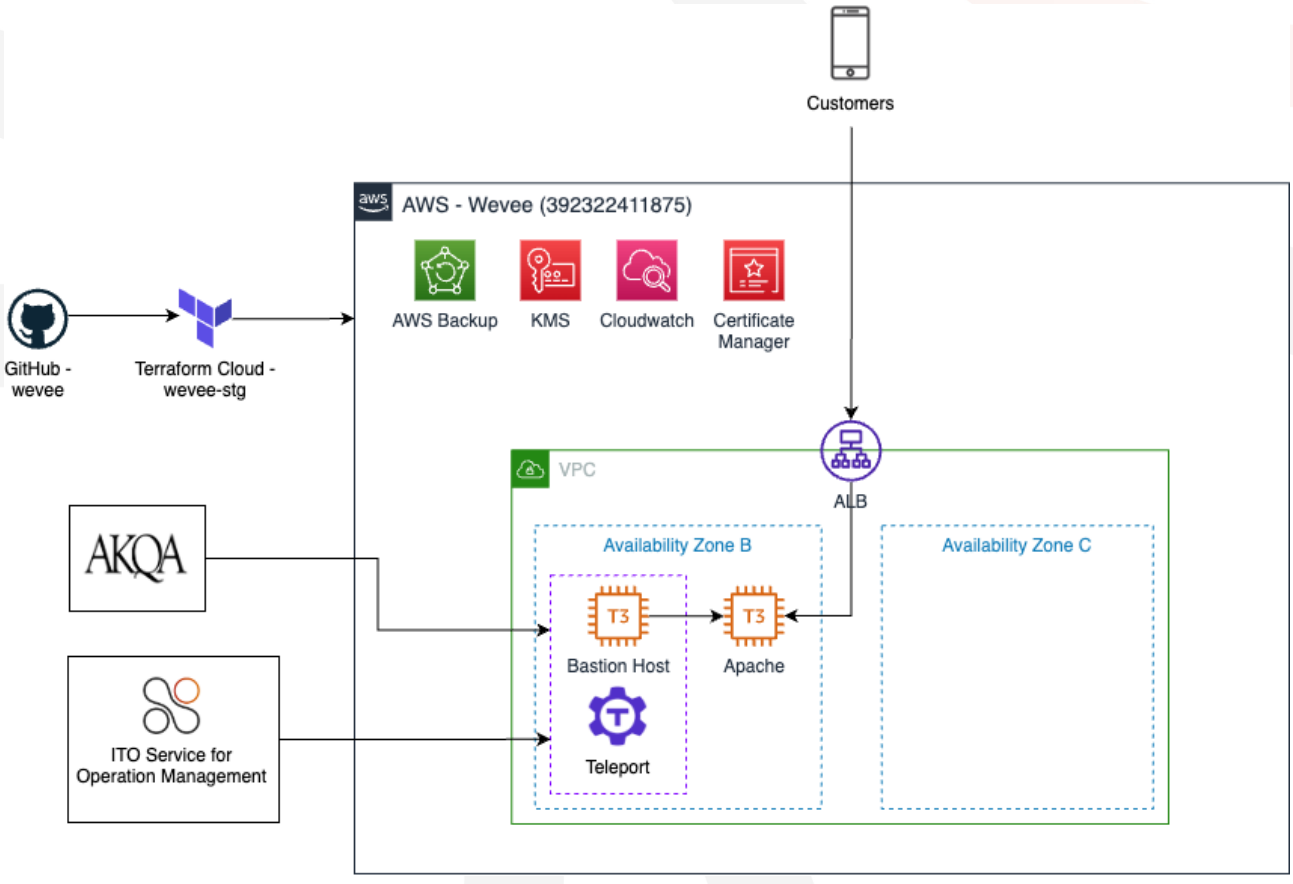
This configuration allows for maximum reliability in the case of highly critical systems, configuring resources on Availability Zone and a greater number of IPs available in the event of future developments. The resources in Stage and Production are created on a single AZ.

The reachability of the resources is guaranteed by the security groups, by default the doors are blocked and open in case of lack of communication with other resources and problems of reachability.

The private subnets of both environments to communicate with the internet use a single NAT Gateway in availability zone B with IP 3.10.38.75. If there is a need to increase reliability, we can add another one in availability zone C.

2.3 Stage Environment

2.3.1 Architecture



The application runs in PHP on an Apache as a web server with the URL: *staging.gatewayhub.wevee.com*.
The DNS is managed by client out of AWS.
Everything that it is possible to encrypt on at Rest would be done with KMS or AWS default keys, keep this convention.

Apache is installed on the EC2 machine, on port 80.
The apache configuration file is /etc/apache2/apache2.conf.

2.3.2 Application Load Balancer

There is one Application Load Balancer shared between the stage and production environments separated by rules with different target groups.
The stage target group navigationAndlifecycle-stg has EC2 apache-stg-1 as target.
All the HTTP traffic are redirected to use HTTPS with certificate.
The traffic will be forwarded from load balancer to the Apache EC2 instance.

Name	Availability Zone	Type	Listener	Security Group ID
navigationAndlifecycle-prd-alb	eu-west-2b, eu-west-2c	Application	HTTP with redirect to HTTPS	sg-023b7571b66e57754
			HTTPS	

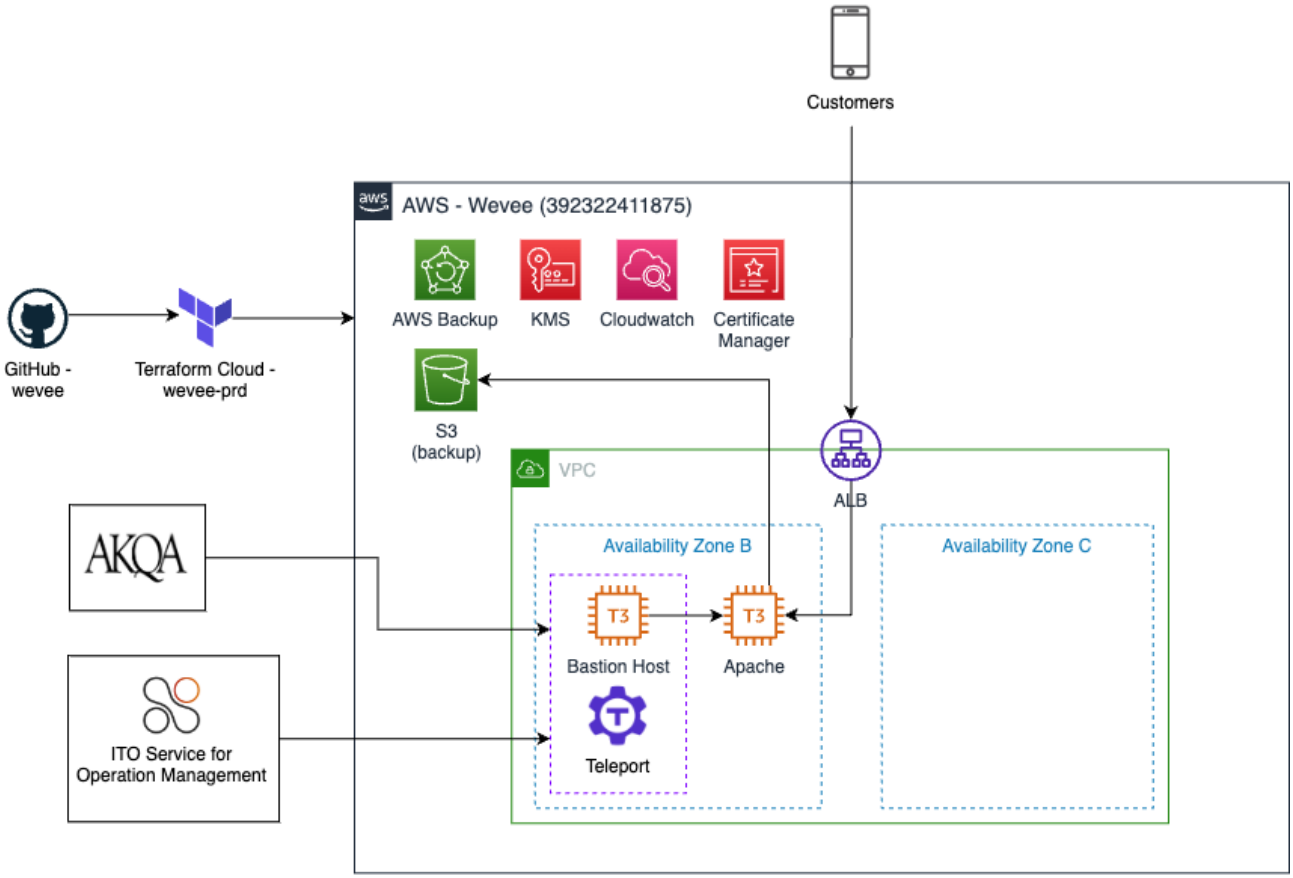
2.3.3 EC2

Web server where is installed the application.

Name	Availability Zone	Instance Type	CPU	RAM	Engine	Disk	Subnet
apache-stg-1	eu-west-2b	t3.medium	2	4 GB	Ubuntu 20.04	32 GB	subnet-0bba94b4c54d247b5 (Private_STG_B)

2.4 Production Environment

2.4.1 Architecture



The application runs in PHP on an Apache as a web server with the URL: gatewayhub.wevee.com.
The DNS is managed by client out of AWS.

Everything that it is possible to encrypt on at Rest would be done with KMS or AWS default keys, keep this convention.
Apache is installed on the EC2 machine, on port 80.
The apache configuration file is /etc/apache2/apache2.conf.

2.4.2 Application Load Balancer

There is one Application Load Balancer shared between the stage and production environments separated by rules with different target groups.
The production target group navigationAndlifecycle-prd has EC2 apache-prd-1 as target.
All the HTTP traffic are redirected to use HTTPS with certificate.
The traffic will be forwarded from load balancer to the Apache EC2 instance.

Name	Availability Zone	Type	Listener	Security Group ID
navigationAndlifecycle-prd-alb	eu-west-2b, eu-west-2c	Application	HTTP with redirect to HTTPS	sg-023b7571b66e57754
			HTTPS	

2.4.3 EC2

Web server where is installed the application.

Name	Availability Zone	Instance Type	CPU	RAM	Engine	Disk	Subnet
apache-prd-1	eu-west-2b	t3.large	2	8 GB	Ubuntu 20.04	32 GB	subnet-0c261ad6728cd8490 (Private_PROD_B)

2.4.4 Bastion Host

Bastion Host is the only way to reach the internal infrastructure via Teleport. Bastion Host has its own public IP address (18.170.251.201).

Name	EIP	Instance Type	CPU	RAM	Engine	Disk	Subnet	Security Group ID
bastion-host-1	18.170.251.201	t3.medium	2	4 GB	Ubuntu 20.04	20 GB	subnet-0b9a3a6079fd849e8 (Public_PROD_B)	sg-07f17c7bd8ba06cee

2.5 Backup

All instances and their disks are backed up through the AWS Backup service. Backups work like this:

- Daily backup: Expire after 1 week
- Weekly backup (performed Monday): Expire after 4 weeks
- Monthly backup (performed on the first day of the month): Expire after 3 months

2.6 Cloudwatch

2.6.1 Cloudwatch Alarms

All production resources are monitored by checking the resource metrics defaults. If the set thresholds are exceeded, Criticalcase will receive an email so that you can activate and check the problem.

3 Users and Accesses

Bastion Access is a VM used to allow SSH access to the private VPC, which can be accessed via traditional ssh or via Teleport with this URL:

https://tp.wevee-navigationandlifecycle.criticalcasecloud.com/

Teleport is an open-source tool for providing zero trust access to servers and cloud applications using SSH, Kubernetes and HTTPS. It is installed on Bastion host and eliminates the need for VPNs by providing a single gateway to access computing infrastructure via SSH.
The user to login is "**wevee**", with the pwd provided via email. Once logged in application servers will be accessed selecting in the list of machines taking in count of the "env tag" to select the proper environment.

All the access sessions are recorded by teleport and saved on an encrypted dedicated private Bucket inside AWS Criticalcase account.

3.1 VM users

Inside every VM in both the Prd and Stg environment the following users:

- **www-data**: user used for the application
- **ssm-user**: user used by AWS to access machines
- **ubuntu**: system default user
- **zabbix**: user used for monitoring