CRITICALCASE

CRITICALCASE

Miamo B2C Project

Architecture Low Level Design

Version: <0.2 17/04/2023>

Customer: Medspa

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 Miamo is to activate the Magento services on AWS Cloud.

The Environments realized are three:

- Development
- Stage
- Production

2 Cloud and Infrastructure Services

2.1 Infrastructural Scope

Criticalcase boundary:

- Delivery of VMs and services (Firewall, Load Balancer, Storage, CDN, VPC, Backup)
- User and access management to the Cloud Infrastructure and to the VMs and services
- Setup, configuration and tuning of all the infrastructure services:
    - Firewall
    - Routing Rules, Subnetting e Networking in general
    - Load Balancer
    - CDN – Implementation according to the web layer specs.
    - Backup
    - Cloudwatch Alarms and Logs
    - WAF
    - Elasticsearch
    - Redis
    - RDS
    - Route53
- Setup and configuration of the Middleware (Nginx) based on customer requirements.
- Create all the Environments via Automation

2.2 Environments

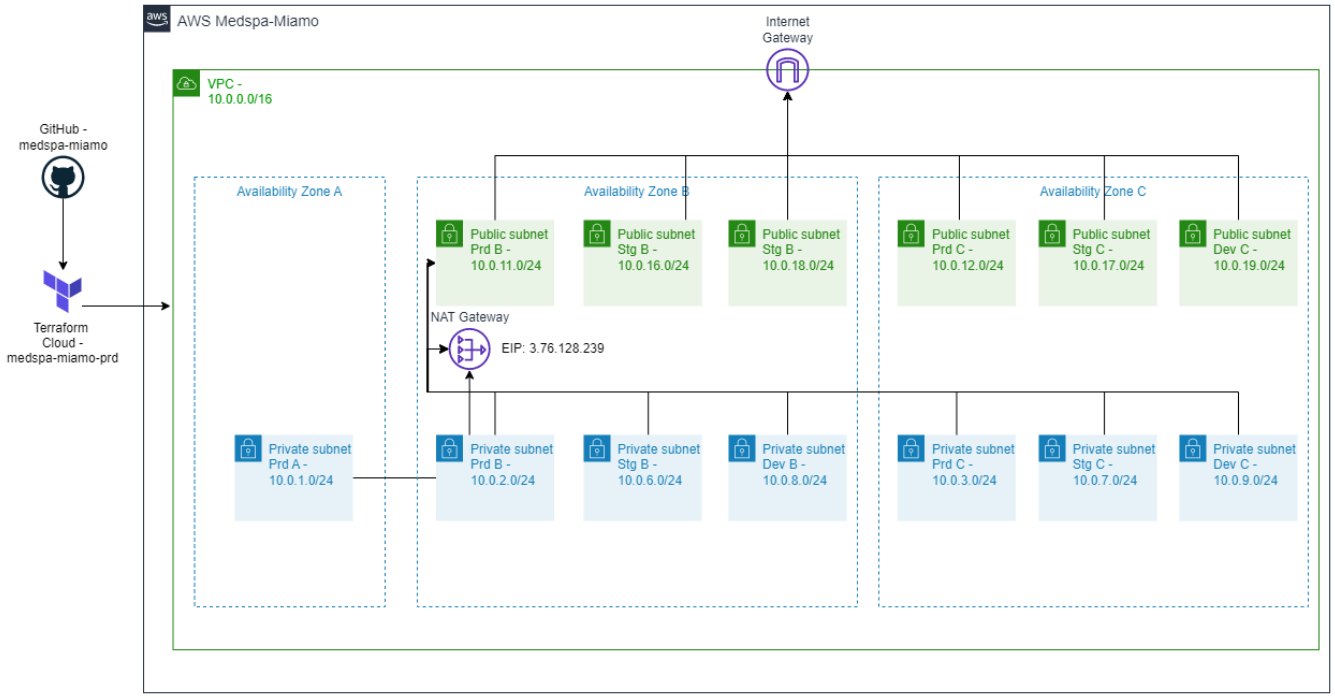
Environments. There are two different Environments, very similar each other:

- **Development (Dev)** environment, that is the only one deployed as of April 2023
- **Stage (Stg)** environment, that is the only one deployed as of January 2023
- **Production (Prd)** environment, to be deployed within February 2023

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

Regions. Within AWS, everything is inside Frankfurt region

2.2.1 Virtual Private Cloud (VPC)



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

3 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_A	Private	eu-central-1a	10.0.1.0/24	subnet-0b538c50c7336f247
Private_PROD_B	Private	eu-central-1b	10.0.2.0/24	subnet-0569dcf993b51337b
Private_PROD_C	Private	eu-central-1c	10.0.3.0/24	subnet-00ed4235bfa0fb441
Public_PROD_B	Public	eu-central-1b	10.0.11.0/24	subnet-0868ff95ca833a6f0
Public_PROD_C	Public	eu-central-1c	10.0.12.0/24	subnet-0110db172dffe675e
Private_STG_B	Private	eu-central-1b	10.0.6.0/24	subnet-00cc4345c2ddb2f6d
Private_STG_C	Private	eu-central-1c	10.0.7.0/24	subnet-08829a38755e9f246

Public_STG_B	Public	eu-central-1b	10.0.16.0/24	subnet-0f0dd2102d545debd
Public_STG_C	Public	eu-central-1c	10.0.17.0/24	subnet-06106879e40e4a743
Private_DEV_B	Private	eu-central-1b	10.0.8.0/24	subnet-03b7a530b9d979310
Private_DEV_C	Private	eu-central-1c	10.0.9.0/24	subnet-03b7a530b9d979310
Public_DEV_B	Public	eu-central-1b	10.0.18.0/24	subnet-0989e2b93c3bb3b0a
Public_DEV_C	Public	eu-central-1c	10.0.19.0/24	subnet-01da70dc3a5c116e7

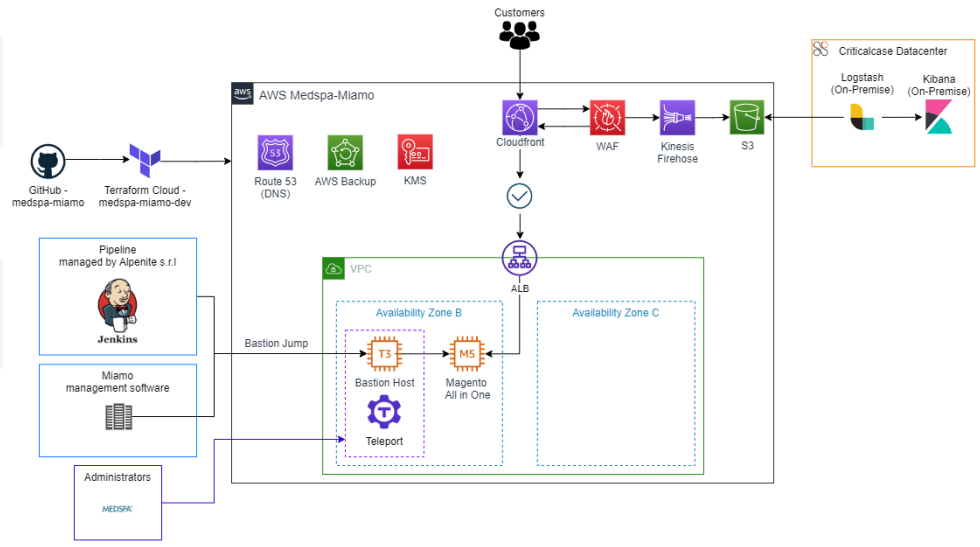
This configuration allows for maximum reliability in the case of highly critical systems, configuring resources on Availability Zone and a greater number of IPs available in the event of future developments. The resources in Stage and Production are created on a single AZ

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 3.74.133.138. If there is a need to increase reliability, we can add another one in availability zone C

2.3 Dev Environment

2.3.1 Architecture



The stage environment has been deployed in a single Availability Zone being a non-critical system, also allowing to reduce costs. Where possible, the default at rest encryption and protection against accidental deletion of resources have been set

2.3.2 Cloudfront

It will oversee distributing content around the world and will have a caching feature for static content. Cloudfront route requests to the load balancer, which will forward them to EC2 frontend Magento. The static content of the following paths is cached: /media/*, /static/* /pub/*. A custom domain with a certificate was chosen: devaws.miamo.com

2.3.3 WAF

Cloudfront shares an Amazon firewall, called WAF, with staging environment which has the task of blocking both malicious requests and IPs deemed not reliable. Malicious ips are automatically updated by Criticalcase. All the information of the actions taken by the WAF are uploaded to a S3 bucket

2.3.4 Application Load Balancer

The balancer accepts only the traffic coming from the Cloudfront (in HTTPS), allowed by a particular header that only the two resources involved know. The traffic will then be forwarded to the Magento EC2 frontend instance

Name	Availability Zone	Type	Listener	Security Group ID
miamo-dev-alb	eu-central-1b, eu-central-1c	Application	HTTPS	sg-08b7fc0c00307d41c

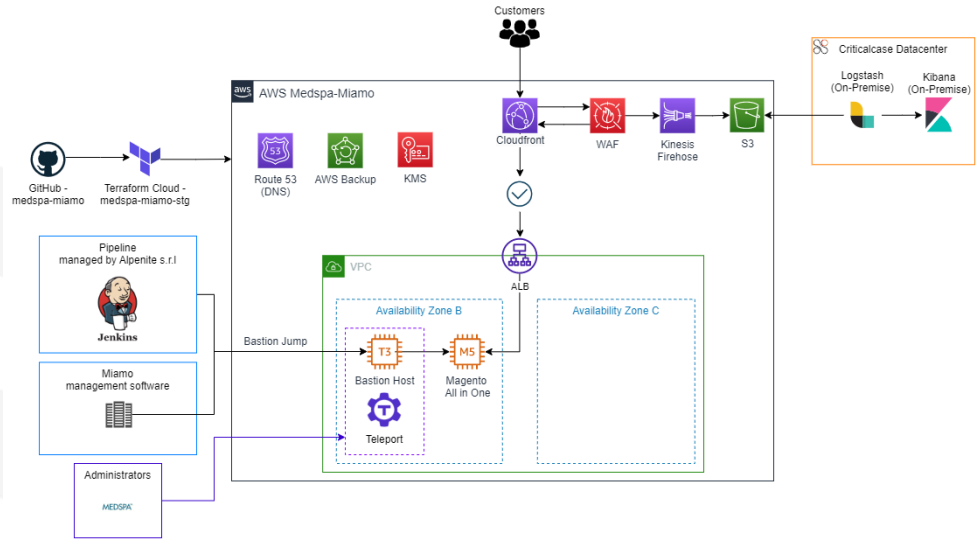
2.3.5 EC2

Frontend servers where is installed Magento application

Name	Availability Zone	Instance Type	CPU	RAM	Engine	Disk	Subnet
magento-dev-1	eu-central-1b	m5.large	2	8 GB	Ubuntu 20.04	32 GB	subnet-03b7a530b9d979310 (Private_DEV_B)

2.4 Stage Environment

2.4.1 Architecture



The stage environment has been deployed in a single Availability Zone being a non-critical system, also allowing to reduce costs. Where possible, the default at rest encryption and protection against accidental deletion of resources have been set

2.4.2 Cloudfront

It will oversee distributing content around the world and will have a caching feature for static content. Cloudfront route requests to the load balancer, which will forward them to EC2 frontend Magento. The static content of the following paths is cached: /media/*, /static/* /pub/*. A custom domain with a certificate was chosen: **staging.miamo.com**

2.4.3 WAF

Cloudfront shares an Amazon firewall, called WAF, with staging environment which has the task of blocking both malicious requests and IPs deemed not reliable. Malicious ips are automatically updated by Criticalcase. All the information of the actions taken by the WAF are uploaded to a S3 bucket

2.4.4 Application Load Balancer

The balancer accepts only the traffic coming from the Cloudfront (in HTTPS), allowed by a particular header that only the two resources involved know. The traffic will then be forwarded to the Magento EC2 frontend instance

Name	Availability Zone	Type	Listener	Security Group ID
miamo-stg-alb	eu-central-1b, eu-central-1c	Application	HTTPS	sg-043ad5ff3683159e5

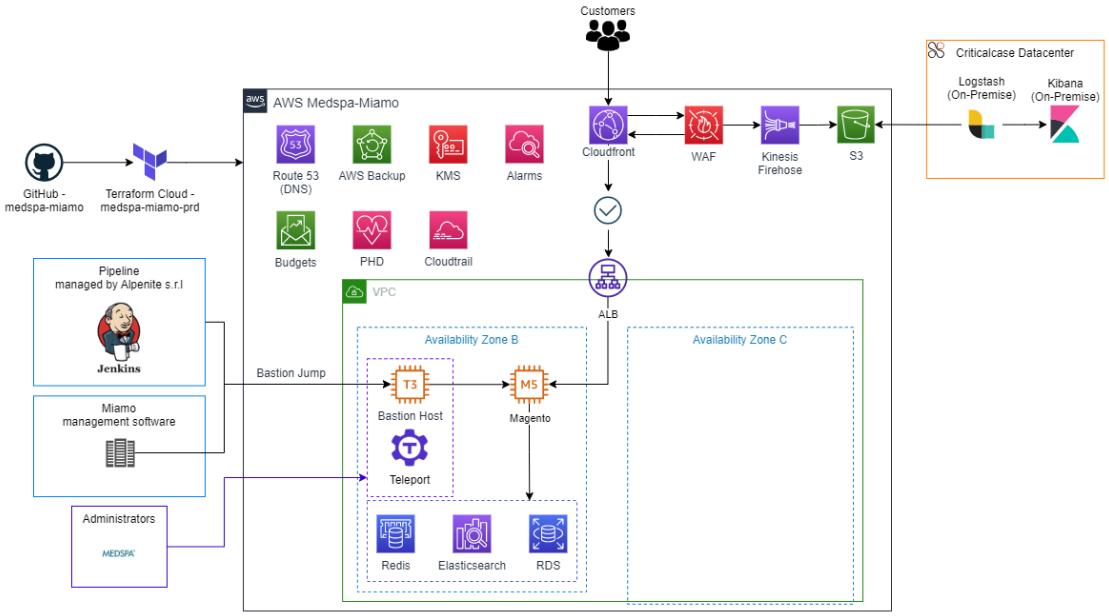
2.4.5 EC2

Frontend servers where is installed Magento application

Name	Availability Zone	Instance Type	CPU	RAM	Engine	Disk	Subnet
magento-stg-1	eu-central-1b	m5.large	2	8 GB	Ubuntu 20.04	64 GB	subnet-0569dcf993b51337b (Private_STAGE_B)

2.5 Production Environment

2.5.1 Architecture



The production environment has been deployed in a one Availability Zone. Where possible, the default at rest encryption and protection against accidental deletion of resources have been set

2.5.2 Cloudfront

It will oversee distributing content around the world and will have a caching feature for static content. Cloudfront route requests to the load balancer, which will forward them to EC2 frontend Magento. The static content of the following paths is cached: /media/*, /static/* /pub/*. custom domain with a certificate was chosen: www.miamo.com, miamo.com

2.5.3 WAF

Cloudfront shares an Amazon firewall, called WAF, with stage environment which has the task of blocking both malicious requests and IPs deemed not reliable. Malicious ips are automatically updated by Criticalcase. All the information of the actions taken by the WAF are uploaded to an S3 bucket

2.5.4 Application Load Balancer

The balancer accepts only the traffic coming from the Cloudfront (in HTTPS), allowed by a particular header that only the two resources involved know. The traffic will then be forwarded to the Magento EC2 frontend instance

Name	Availability Zone	Type	Listener	Security Group ID
magento-prd-alb	eu-central-1b, eu-central-1c	Application	HTTPS	sg-04498bc625ffbbfaa

2.5.5 RDS

Database used from Magento frontend and admin servers

Name	Availability Zone	Instance Type	CPU	RAM	Engine	Subnet	Security Group ID
magento-prd	eu-central-1b	db.m6g.large	2	8 GB	MySQL (8.0)	subnet-0569dcf993b51337b, subnet-00ed4235bfa0fb441	sg-03ae11dbd6e0da31c

2.5.6 EC2

Frontend servers where is installed Magento application

Name	Availability Zone	Instance Type	CPU	RAM	Engine	Disk	Subnet
magento-prd-1	eu-central-1b	m5.large	2	8 GB	Ubuntu 20.04	32 GB	subnet-0569dcf993b51337b (Private_PROD_B)

2.5.7 Bastion Host

Bastion Host is the only way to reach the internal infrastructure via Teleport. Bastion Host has its own public IP address (3.76.128.239).

Name	EIP	Instance Type	CPU	RAM	Engine	Disk	Subnet	Security Group ID
bastion-host-1	3.76.128.239	t3.medium	2	4 GB	Ubuntu 20.04	20 GB	subnet-0868ff95ca833a6f0	sg-0b5746ce84757faf7

2.5.8 Redis

Used for cache in front the RDS and to store user sessions

Name	Availability Zone	Instance Type	CPU	RAM	Engine	Subnet	Security Group
magento-prd	eu-central-1b	cache.m6g.large	2	6,38GB	Redis 7.0.5	subnet-0569dcf993b51337b, subnet-00ed4235bfa0fb441	sg-040e751334fd79096

2.5.9 Elasticsearch

magento-prd-es is used as Dashboard from Magento application

Name	Availability Zone	Instance Type	CPU	RAM	Engine	Disk	Subnet	Security Group
magento-prd-es	eu-central-1b	m6g.large.search	2	8 GB	7.10	30 GB	subnet-0569dcf993b51337b, subnet-00ed4235bfa0fb441	sg-09222f39df86f4b78

2.6 DNS

AWS internal DNS is managed by Route53 to allow you to resolve AWS IPs / DNS in a more understandable way. There is a zone that manages the miamo.internal domain/

Public domains are associated with Cloudfront in order to be reachable by end customers:

staging.miamo.com	CNAME	d1thhexn6zkzja.cloudfront.net
miamo.com, www.miamo.com	CNAME	d253bjn4hhliqk.cloudfront.net

2.7 Backup

All resources (except ElasticSearch and Redis which have a standalone backup), 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
- Daily backup (performed on the first day of the month): Expire after 3 months

2.8 Cloudwatch

2.8.1 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.medspa-miamo.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 "**miamo**", with the pwd provided via email. Once logged in Magento servers will be accessed selectin 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, Stg and Dev environment the following users:

- **miamo**: user used to run the Magento application
- **ssm-user**: user used by AWS to access machines
- **ubuntu**: system default user