CRITICALCASE

CRITICALCASE

Websolute B2C Project

Architecture Low Level Design

Version: <0.1 27/07/2022>

Customer: Websolute

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 Websolute is to activate the Magento services on AWS Cloud.

The Environments realized are three:

- 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
    - EFS
    - WAF
    - Elasticsearch
    - Redis
    - RDS
    - Route53
- Setup and configuration of the Middleware (Nginx, Varnish…) based on customer requirements
- Create all the Environments via Automation

2.2 Environments

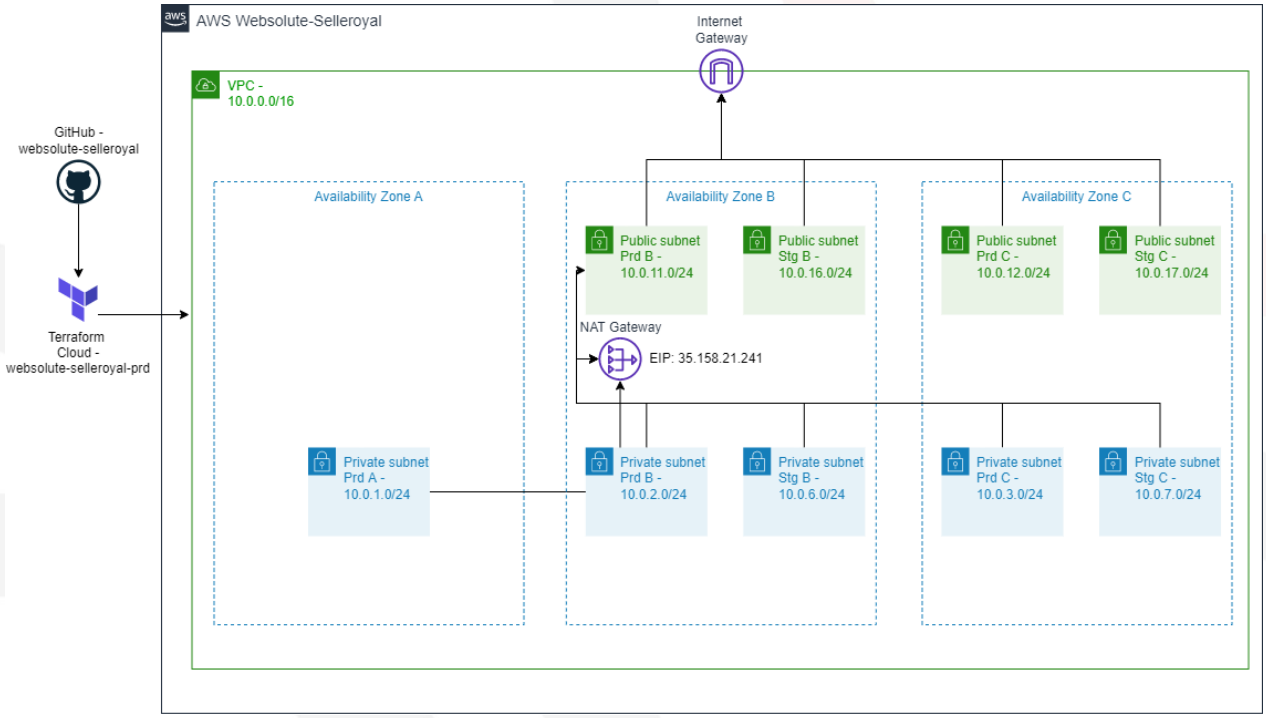
Environments. There are two different Environments, very similar each other:

- **Stage (Stg)** environment, that is the only one deployed as of July 2022.
- **Production (Prd)** environment, to be deployed within July 2022.

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

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-04f9996420520afe3
Private_PROD_B	Private	eu-central-1b	10.0.2.0/24	subnet-08dc043eac36ecebd
Private_PROD_C	Private	eu-central-1c	10.0.3.0/24	subnet-073871995b4fffcce
Public_PROD_B	Public	eu-central-1b	10.0.11.0/24	subnet-0c0b028e8aa96f0c3
Public_PROD_C	Public	eu-central-1c	10.0.12.0/24	subnet-0a8184d16433be4b4
Private_STG_B	Public	eu-central-1b	10.0.6.0/24	subnet-032c8d7e357904cbb
Private_STG_C	Private	eu-central-1c	10.0.7.0/24	subnet-00c9381ffe6615cc1
Public_STG_B	Private	eu-central-1b	10.0.16.0/24	subnet-034187133814d950e
Public_STG_C	Private	eu-central-1c	10.0.17.0/24	subnet-0bf4e0708faa32b71

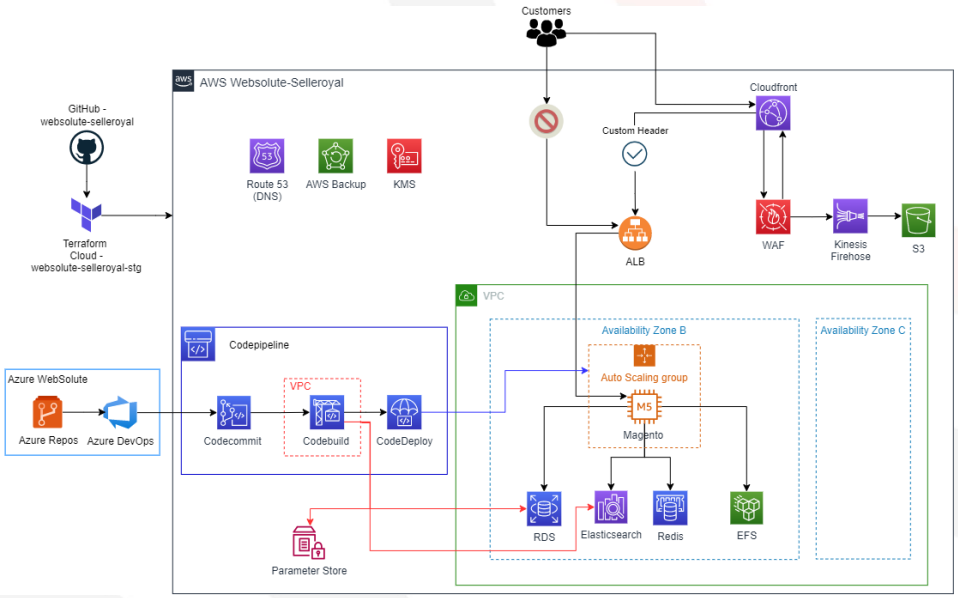
This configuration allows for maximum reliability in the case of highly critical systems, configuring resources on Availability Zone and a greater number of IPs available in the event of future developments. The resources in Stage are created on a single AZ not being critical, currently production on 2 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 35.158.21.241. 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 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/* and /statics/*. A custom domain with a certificate was chosen: **stage-m2.selleroyal.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
Magento-stg-alb	eu-central-1b, eu-central-1c	Application	HTTPS	sg-0a74ac5026ec2446a

2.3.5 RDS

Database used from Magento frontend servers

Name	Availability Zone	Instance Type	CPU	RAM	Engine	Subnet	Security Group ID
magento-stg	eu-central-1b	db.r6g.large	2	16 GB	Aurora MySQL (8.0)	subnet-032c8d7e357904cbb, subnet-00c9381ffe6615cc1	sg-047edcbc570613b80

2.3.6 EC2

Frontend server where Magento application is installed is under autoscaling group. The VMs that will be created will have this configuration

Name	Min Size	Max Size	Availability Zone	Instance Type	CPU	RAM	Engine	Disk	Subnet	Security Group ID
magento-stg	1	2	eu-central-1b	m5.large	2	8 GB	Ubuntu 20.04	50 GB	subnet-032c8d7e357904cbb	sg-08f616fbb0ac7e670

2.3.7 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-stg	eu-central-1b	cache.t3.small	2	1,37 GB	Redis 6.2.6	subnet-032c8d7e357904cbb, subnet-00c9381ffe6615cc1	sg-0b8f2f5825c7b0349

2.3.8 Elasticsearch

It is used as Dashboard from Magento application

Name	Availability Zone	Instance Type	CPU	RAM	Engine	Disk	Subnet	Security Group
magento-stg-es	eu-central-1b	t3.medium.elasticsearch	2	4 GB	7.10	10 GB	subnet-032c8d7e357904cbb	sg-014617518714fc8b1

2.3.9 EFS

It is used to share magento upload/media between Magento instances.

Name	File System ID	Availability Zone	Subnet	Security Group
magento-stg-efs	fs-06c459ea8403852cf	eu-central-1b, eu-central-1c	subnet-032c8d7e357904cbb, subnet-00c9381ffe6615cc1	sg-014617518714fc8b1

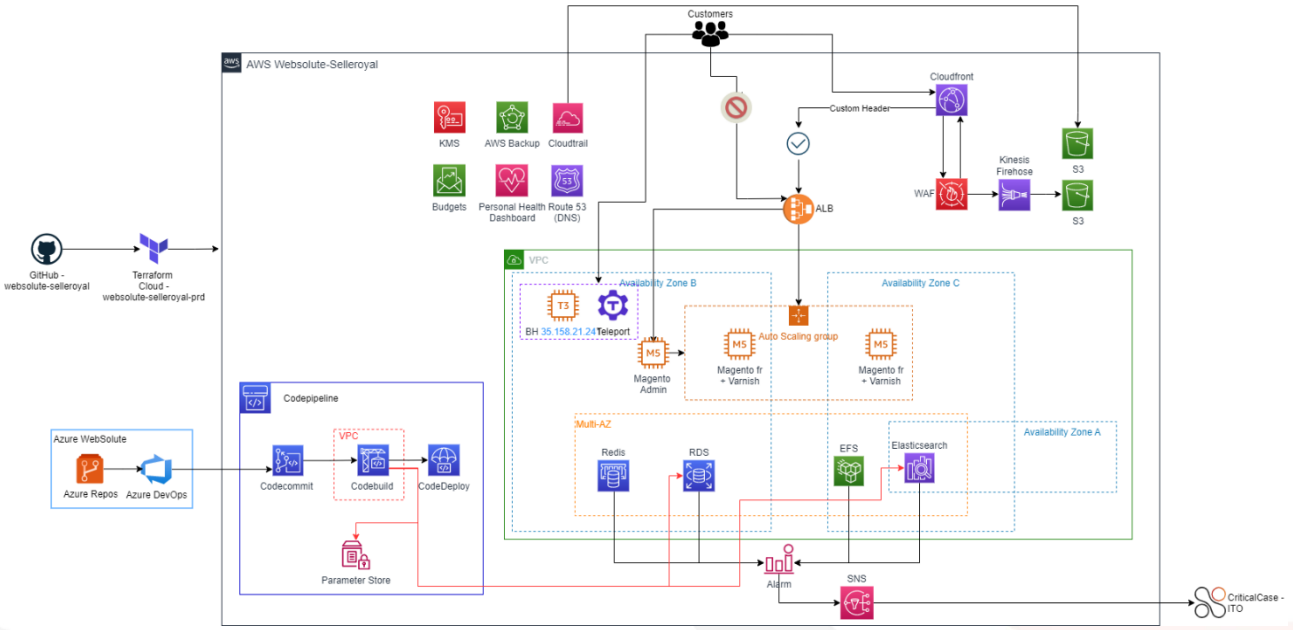
2.3.10 System Manager Parameter Store

Sensitive data used by CodeBuild during the code compilation phase are stored in these encrypted parameters

Name	Tier	Type	Encrypted	Description
/magento/stg/auth.json	Standard	SecureString	Yes	Credentials used to download Magento plugins
/magento/stg/env.php	Standard	SecureString	Yes	PHP file used by Magento to interact with other AWS resources (RDS, EFS, Redis, etc ...)
/magento/stg/rds_database_magento	Standard	SecureString	Yes	Database RDS Magento
/magento/stg/rds_hostname	Standard	SecureString	Yes	Database Hostname Magento
/magento/stg/rds_password_magento	Standard	SecureString	Yes	Database Password Magento
/magento/stg/rds_username_magento	Standard	SecureString	Yes	Database Username Magento

2.4 Production Environment

2.4.1 Architecture



The production environment has been deployed in a two Availability Zone (it is possible to add a third AZ). 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/* and /statics/*. A custom domain with a certificate was chosen: www.selleroyal.com, selleroyal.com

2.4.3 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

2.4.4 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
Magento-prd-alb	eu-central-1b, eu-central-1c	Application	HTTPS	sg-0a74ac5026ec2446a

2.4.5 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.r6g.large	2	16 GB	Aurora MySQL (8.0)	subnet-073871995b4fffcce, subnet-08dc043eac36ecebd	sg-049e19fbf63d86740

2.4.6 EC2

Frontend servers where Magento application is installed is under autoscaling group. The VMs that will be created will have this configuration

Name	Min Size	Max Size	Scaling Policy	Spot instance	Instance Type	CPU	RAM	Engine	Disk	Subnet	Security Group ID
magento-prd	2	6	Yes	Yes	m5.large	2	8 GB	Ubuntu 20.04	100 GB	subnet-073871995b4fffcce, subnet-08dc043eac36ecebd	sg-004df19a2f42cf916

The scaling policy allows you to increase the number of servers in case the CPU usage exceeds 80% usage
The minimum number of servers present in auto scaling are 2 On Demand instances. The servers that are created in the event of peak traffic are spot servers

Admin server is out of the autoscaling group. This is the configuration:

Name	Instance Type	CPU	RAM	Engine	Disk	Subnet	Security Group ID
magento-admin-prd-1	m5.large	2	8 GB	Ubuntu 20.04	50 GB	subnet-08dc043eac36ecebd	sg-0f538f3309178064d

Bastion Host is the only way to reach the internal infrastructure via Teleport. Bastion Host has its own public IP address (3.73.93.198).

Name	EIP	Instance Type	CPU	RAM	Engine	Disk	Subnet	Security Group ID
bastion-host-1	3.73.93.198	t3.medium	2	4 GB	Ubuntu 20.04	20 GB	subnet-0c0b028e8aa96f0c3	sg-0f965f0d0c230d7f5

2.4.7 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, eu-central-1c	cache.m5.large	2	6,38GB	Redis 6.2.6	subnet-08dc043eac36ecebd, subnet-073871995b4fffcce	sg-0b8f2f5825c7b0349

2.4.8 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, eu-central-1c, eu-central-1a	m5.large.search	2	8 GB	7.10	50 GB	subnet-04f9996420520afe3, subnet-073871995b4fffcce, subnet-08dc043eac36ecebd	sg-093f3fe1ddd400d20

2.4.9 EFS

It is used to share magento upload/media between Magento instances

Name	File System ID	Availability Zone	Subnet	Security Group
magento-prd-efs	fs-001cf65a0cda11c62	eu-central-1b, eu-central-1c	subnet-08dc043eac36ecebd, subnet-073871995b4fffcce	sg-0d4774095c350197c

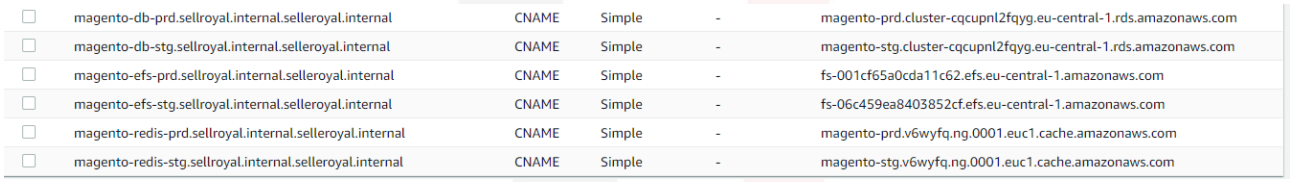
2.4.10 System Manager Parameter Store

Sensitive data used by CodeBuild during the code compilation phase are stored in these encrypted parameters

Name	Tier	Type	Encrypted	Description
/magento/prd/auth.json	Standard	SecureString	Yes	Credentials used to download Magento plugins
/magento/prd/env.php	Advanced	SecureString	Yes	PHP file used by Magento to interact with other AWS resources (RDS, EFS, Redis, etc ...)
/magento/prd/rds_database_magento	Standard	SecureString	Yes	Database RDS Magento
/magento/prd/rds_hostname	Standard	SecureString	Yes	Database Hostname Magento
/magento/prd/rds_password_magento	Standard	SecureString	Yes	Database Password Magento
/magento/prd/rds_username_magento	Standard	SecureString	Yes	Database Username Magento

2.5 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 selleroyal.internal domain with the following records:



magento-db-prd.sellroyal.internal.selleroyal.internal	CNAME	Simple	-	magento-prd.cluster-cqcupnl2fqyg.eu-central-1.rds.amazonaws.com
magento-db-stg.sellroyal.internal.selleroyal.internal	CNAME	Simple	-	magento-stg.cluster-cqcupnl2fqyg.eu-central-1.rds.amazonaws.com
magento-efs-prd.sellroyal.internal.selleroyal.internal	CNAME	Simple	-	fs-001cf65a0cda11c62.efs.eu-central-1.amazonaws.com
magento-efs-stg.sellroyal.internal.selleroyal.internal	CNAME	Simple	-	fs-06c459ea8403852cf.efs.eu-central-1.amazonaws.com
magento-redis-prd.sellroyal.internal.selleroyal.internal	CNAME	Simple	-	magento-prd.v6wyfq.ng.0001.euc1.cache.amazonaws.com
magento-redis-stg.sellroyal.internal.selleroyal.internal	CNAME	Simple	-	magento-stg.v6wyfq.ng.0001.euc1.cache.amazonaws.com

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

stage-m2.selleroyal.com	CNAME	d1b1vy67oemtjr.cloudfront.net
selleroyal.com, www.selleroyal.com	CNAME	ds3lu3cfgznbc.cloudfront.net

2.6 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

2.7 Cloudwatch

2.7.1 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

Name Alarm	Resource type	Description
magento-prd-2-rds-cpu-utilization-SELLEROYAL-564037702494-AWS	RDS	Usage of the RDS CPU
magento-prd-1-rds-cpu-utilization-SELLEROYAL-564037702494-AWS	RDS	Usage of the RDS CPU
magento-prd-1-rds-free-memory-SELLEROYAL-564037702494-AWS	RDS	Available RDS memory
magento-prd-2-rds-free-memory-SELLEROYAL-564037702494-AWS	RDS	Available RDS memory
magento-prd-1-rds-max-connections-SELLEROYAL-564037702494-AWS	RDS	Maximum connections that RDS can accept
magento-prd-2-rds-max-connections-SELLEROYAL-564037702494-AWS	RDS	Maximum connections that RDS can accept
status-check-failed-instance-i-0eb76f5fc158cdff6-selleroyal-web-564037702494	EC2	Check that the instance works from a hardware and os point of view
status-check-failed-instance-i-05b2dbec84b83bdb2-selleroyal-web-564037702494	EC2	Check that the instance works from a hardware and os point of view
TARGETGROUP-Magento-prd-magento-LOADBALANCER-Magento-prd-alb-UnHealthy-selleroyal-web-564037702494	Loadbalancer	Availability of instances attached to the balancer
TARGETGROUP-Magento-prd-admin-LOADBALANCER-Magento-prd-alb-UnHealthy-selleroyal-web-564037702494	Loadbalancer	Availability of instances attached to the balancer
magento-prd-efs-permitted-throughput-SELLEROYAL-564037702494-AWS	EFS	EFS permitted throughput
status-check-failed-system-i-0eb76f5fc158cdff6-selleroyal-web-564037702494	EC2	Check that the instance works from a hardware point of view
status-check-failed-system-i-05b2dbec84b83bdb2-selleroyal-web-564037702494	EC2	Check that the instance works from an os point of view
magento-prd-elasticSearch-free-storage-space-SELLEROYAL-564037702494-AWS	Elasticsearch	Available Elasticsearch storage

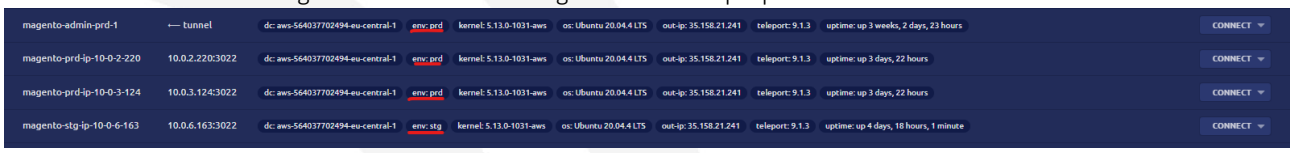
magento-prd-elasticSearch-jvm-memory-pressure-SELLEROYAL-564037702494-AWS	Elasticsearch	Available Elasticsearch JVM memory
magento-prd-elasticSearch-automated-snapshot-failure-SELLEROYAL-564037702494-AWS	Elasticsearch	Elasticsearch snapshots failed
magento-prd-elasticSearch-cpu-utilization-SELLEROYAL-564037702494-AWS	Elasticsearch	Usage of the Elasticsearch CPU
magento-prd-elasticSearch-red-status-SELLEROYAL-564037702494-AWS	Elasticsearch	Red state of Elasticsearch
magento-prd-elasticSearch-ClusterIndexWritesBlocked-SELLEROYAL-564037702494-AWS	Elasticsearch	Cluster Index Writes Blocked
magento-prd-Redis_DatabaseMemoryUsagePercentage-Node-1-SELLEROYAL-564037702494-AWS	Redis	Database Memory Usage Percentage
magento-prd-Redis_CurrConnections-node-1-SELLEROYAL-564037702494-AWS	Redis	Maximum connections that Redis can accept
magento-prd-Redis_CurrConnections-node-2-SELLEROYAL-564037702494-AWS	Redis	Maximum connections that Redis can accept
magento-prd-Redis_EngineCPUUtilization-Node1-SELLEROYAL-564037702494-AWS	Redis	CPU Utilization
magento-prd-Redis_EngineCPUUtilization-Node2-SELLEROYAL-564037702494-AWS	Redis	CPU Utilization
magento-prd-Redis_DatabaseMemoryUsagePercentage-Node-2-SELLEROYAL-564037702494-AWS	Redis	Database Memory Usage Percentage

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.websolute-selleroyal.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 "**selleroyal**", 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 Prod and dev environment the following users:

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

3.2 Pipeline

For the automatic deployment of the code on the Magento servers, the AWS CodePipeline service was used. The code is located inside an Azure Repos owned by Websolute. When a push occurs on the staging or master branches (in the case of production), an Azure DevOps pipeline takes care of cloning the code to the CodeCommit repository by starting the pipeline in AWS. The next stage is CodeBuild in VPC which has the task of running the Magento code, downloading external plugins and interacting with other services such as RDS. The credentials and sensitive data are encrypted and stored within the Parameter Store. When the Build phase is finished, CodeDeploy takes care of releasing the code on the servers.