Exam Report

October 20, 2023

Computer Systems Engineering

Cloud Architecture

Prof. Mtro. Rodolfo Luthe Ríos

Marco Ricardo Cordero Hernández

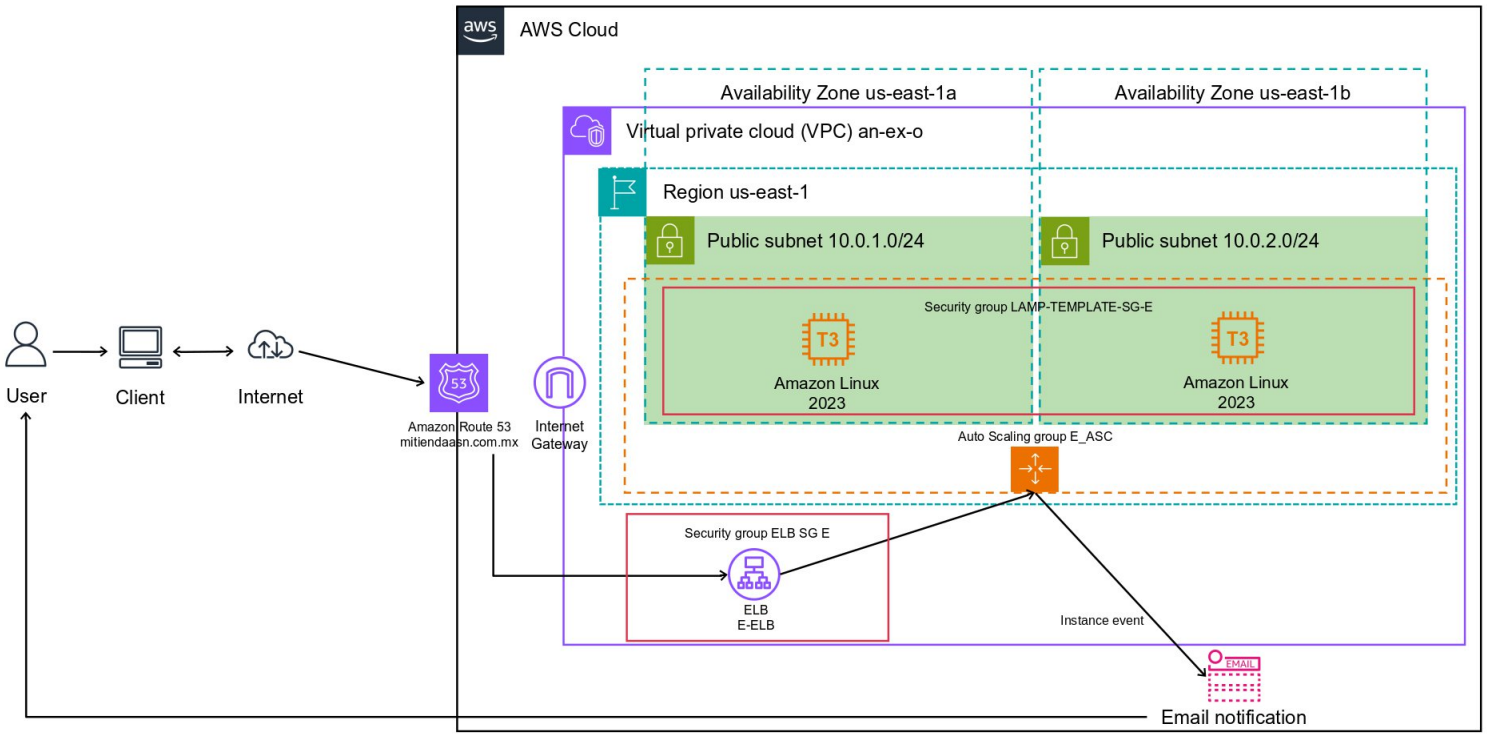
is727272@iteso.mx

ITESO

Universidad Jesuita
de Guadalajara

Diagram

The following architecture it's proposed as a graphic solution for the stated goals.

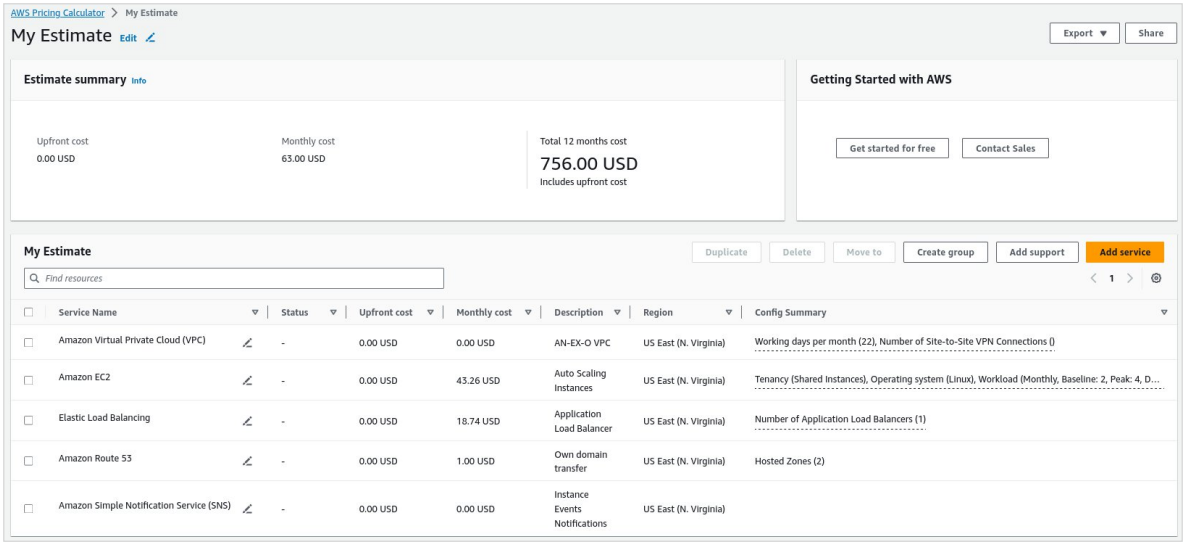


Solution justification

- VPC features: These core configurations include privacy clauses enforcement, access to internet.
- Route 53: This service allows users to bring their own pre-registered domain, allowing the customer previous resource usage with no additional charges for new DNS registration.
- EC2 instances: The default service for cloud computing would be used to run the previously developed LAMP stack application.
- Auto scaling group with launch templates through AMIs: These AWS tools would handle scalability, resiliency, availability and QoS trough automatic instance deployment when usage of the main instance it's surpassed. Within this same tool, email notifications can be configured to notify the customer and the engineer that would manage this architecture at the same time.
- Application load balancer and target groups: Along with the previous tool, this combination of AWS services will ensure correct user traffic distribution for high throughput desirable seasons like end of year sales and such events.

Budget Justification

The estimated budget would be the following:



This estimate takes into account from 2 to 4 instances with a monthly peak of 7 days. In this case, the recommendation would be a monthly payments, as is not assured that every operative month will have traffic peaks like at the end of year.

Development

The first approach to this implantation it's to create an Amazon Machine Image from a instance. For this matter, the following features will be assigned to this disposable helper instance:

- Name: LAMP E AMI
- Operating system: Amazon Linux 2023 or newest version
- Instance type: t3.small
- Auto-assign public IP
- New *LAMP-TEMPLATE-SG-E* security group
    - Accept port 22 (SSH), port 80 (HTTP) and port 443 (HTTPS) connections from the internet (0.0.0.0/0)

Name	AMI ID	AMI name	Source	Owner	Visibility
E AMI	ami-00d0e6aec8d3bf1f8	LAMP E AMI	042979533702/LAMP E AMI	042979533702	Private

Instance remote connection through SSH has to be made to install corresponding LAMP stack dependencies and general configurations with these commands:

```
sudo dnf update -y

sudo dnf install -y httpd wget php-fpm php-mysqli php-json php php-devel
```

```
sudo dnf install mariadb105-server

sudo systemctl start httpd

sudo systemctl enable httpd

sudo systemctl is-enabled httpd

# Omitted application enabling related steps
```

With this template instance already configured, VPC related components such as subnets and the VPC itself will be created.

- VPC Name: an-ex-o
- CIDR block: 10.0.0.0/16
- Availability zones: 2 (us-east-1a, us-east-1b)
- Public/Private subnets: 2
- CIDR blocks:
    - Public subnets
        - A: 10.0.1.0/24
        - B: 10.0.2.0/24

Name	VPC ID	State	IPv4 CIDR
an-ex-o-vpc	vpc-06dca8aad1be9e375	Available	10.0.0.0/16

Once the VPC has been properly created, a launch template for app environment instances it's created with these features:

- Name: LAMP-TEMPLATE-E
- Image: LAMP E AMI
- Instance type: t3.small
- Login: vockey
- Utilize *LAMP-TEMPLATE-SG-E* security group
    - Add network interface
        - Public IP assignation enabled
        - Delete interface on termination
- 30GB volume size (gp3)

Launch Template ID	Launch Template Name	Default Version	Latest Version	Create Time
lt-0e46386a574b59f65	LAMP-TEMPLATE-E	1	1	2023-10-21T03:10:20.000Z

With the previous launch template, the auto scaling group also has to be created with this requirements:

- Name: E-ASC
- Both *public* subnets created before (A, B)
- New *application* load balancer

    - Name: E-ELB
    - Internet-facing scheme
    - Target group name: E-ELB
- Default lattice integration and health checks settings
- Group size
    - Desired capacity: 2
    - Minimum capacity: 2
    - Maximum capacity: 4
- Deploy new instance on 60% of usage with 180 seconds of warmup
- Notifications
    - Notification 1
        - Name: Mi-Tienda-ASN-Instance-Event-Developer
        - Recipients: is727272@iteso.mx
        - All event types
    - Notification 2
        - Name: Mi-Tienda-ASN-Instance-Event-Customer
        - Recipients: customer.mail@exam.an (demonstrative non-valid name)
        - All event types

Name	Launch template/configuration	Instances	Status	Desired capacity	Min	Max	Availability Zones
E_ASC	LAMP-TEMPLATE-E | Version Default	2	-	2	2	4	us-east-1a, us-east-1b

Both developer and customer mails have been included in this case, however, one of them could be omitted. Developer mail could be omitted to only attend customer calls when needed, and customer mail could be omitted to relieve them from technical events that would be directly targeted to the implementers. The first option would be more realistic.

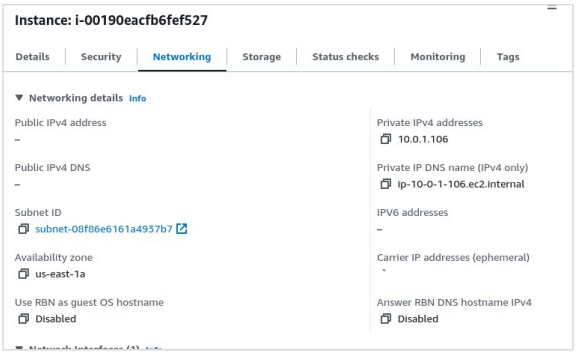
Right after this auto scaling group it's created, the previously created security group will be modified to ensure that new instances won't be accessible from outside of the VPC. For this, an additional security group for load balancing has to be created with these requirements:

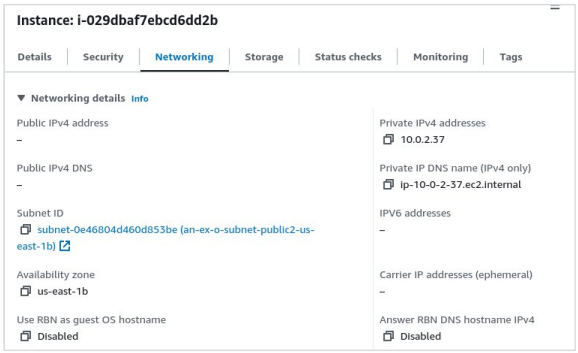
- Name: ELB SG E
- VPC: an-ex-o
- Inbound rules
    - 0.0.0.0/0 to HTTP and HTTPS ports
- Outbound rules
    - All traffic

The previously created security group (LAMP-TEMPLATE-SG-E) will be modified to only accept HTTP/S inbound traffic from the newly created security group. For this, previously created rules have to be deleted before the association is made, otherwise, completion impeding warnings will arise. SSH is intentionally left open for all traffic, however, a real implementation would make use of a set of strictly defined IP's or an administrative bastion instance to access these groups.

Security group rule ID	IP version	Type	Protocol	Port range	Source
sgr-046009392ed92e5ab	–	HTTP	TCP	80	sg-00f67c21f888f41a7 / ELB SG E
sgr-0d0cfabf10a958e4e	IPv4	SSH	TCP	22	0.0.0.0/0
sgr-059bcf51ace28e9be	–	HTTPS	TCP	443	sg-00f67c21f888f41a7 / ELB SG E

A final modification has to be made inside the load balancer to remove the previously assigned security group and replace it with the ELB SG E security group. Once this alteration it's made, the architecture instances won't be publicly accessible through web browser, but the load balancer will still be.





Additional notes

Although Route 53 service was proposed in the initial architecture, the account used for this proposal is restricted to only some AWS services and features, unfortunately, the former is not included in its allowed usage. However, the steps to reproduce this additional migration are as simple as going in the mentioned service, search for registered domains section and transfer in the previously owned domain. This case doesn't states which DNS registrar service provides the domain, but a general/common set of steps have to be followed in order for the domain to be transferred to AWS. After this process is conducted, DNS name provided by AWS for the load balancer would be replaced with the provided mitiendaasn.com.mx domain.