Case Study

Group: RDEnvi

Robertas Asvicas

Dmitry Lvov

**Contents**

[Project definition 3](#_Toc55857907)

[Infrastructure Diagram 3](#_Toc55857908)

[Infrastructure Components 4](#_Toc55857909)

[VPC 4](#_Toc55857910)

[Subnets 4](#_Toc55857911)

[NAT subnets: 4](#_Toc55857912)

[Web/App subnets 4](#_Toc55857913)

[Database subnets: 4](#_Toc55857914)

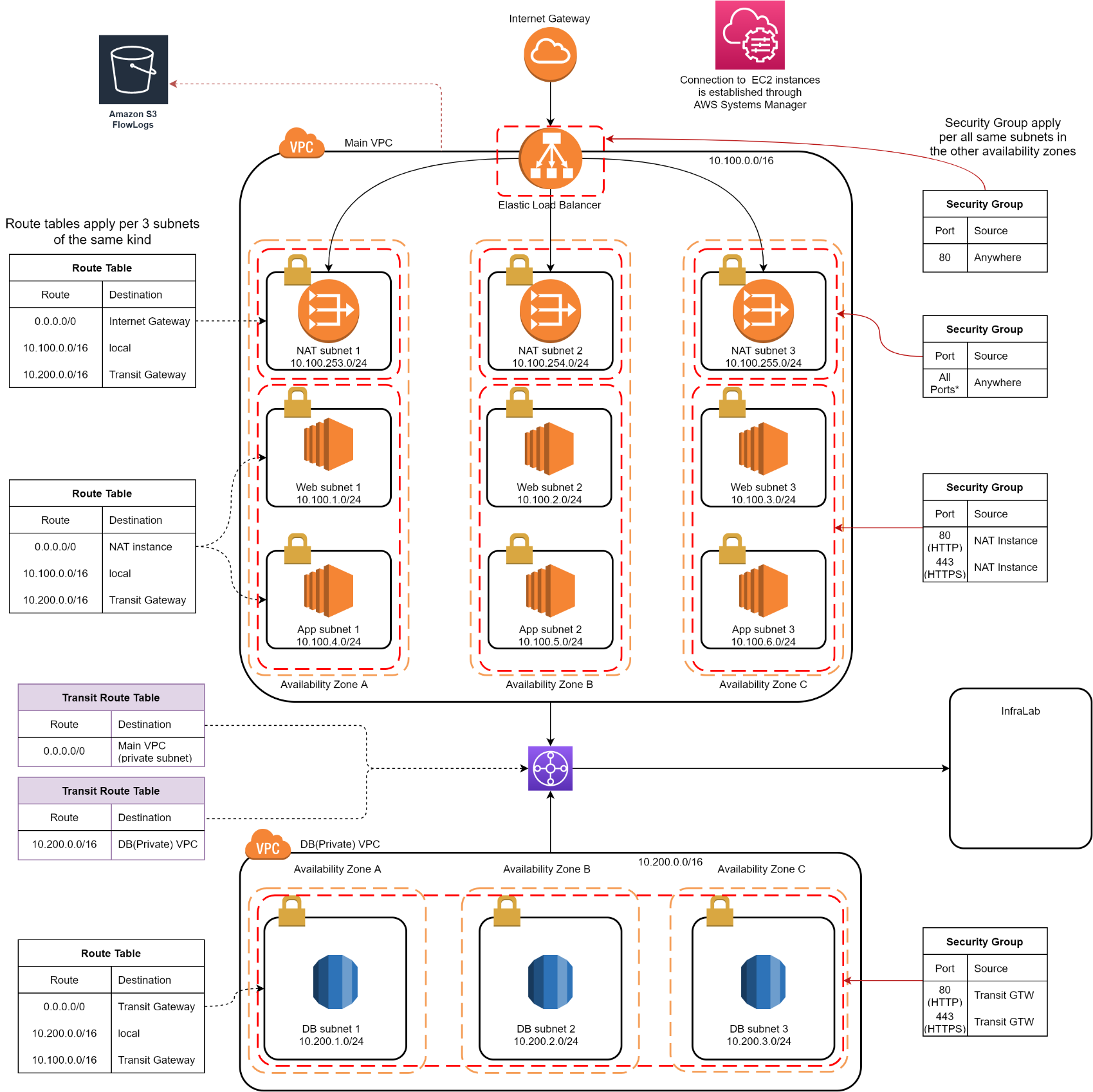
# Project definition

Our main goal in this project was to create suitable infrastructure for software students to host websites, applications. Infrastructure was supposed to be automated, scalable, and secure. We were using Amazon Web Services (further as AWS) for infrastructure creation, Ansible and Terraform for automation and different techniques for security implementations.

# Requirements

* Network Infrastructure on AWS
  + Secure – usage of private subnets, private VPCs, NAT instances, configured Security Groups
  + Scalable – usage of Autoscaling Groups, Availability Zones
  + Resilient – usage of Elastic Load balancer, Availability Zones
  + Automated – deployment is automated via Ansible, Terraform
* Isolated Database
* Automation – Ansible:
  + Apache deployment
  + Flask deployment
* Automation – Terraform

Infrastructure Diagram



Infrastructure Components

## VPC

Infrastructure is made out of 2 VPCs:

|  |  |
| --- | --- |
| Main VPC | Private VPC |
| CIDR block: 10.100.0.0/16 | CIDR block: 10.200.0.0/16 |
| Used to host everything BUT databases | Used to host ONLY databases |
| NAT subnets can be accessed from WAN | Can NOT be accessed from WAN |
| Has Internet Access | No Internet Access (only through Transit Gateway) |
| EC2 instances can be accessed only through SSM | EC2 instances can be accessed only through SSM |
| Has 3 Availability Zones | Has 3 Availability Zones |

## Subnets

There are 4 types of subnets in our infrastructure:

* NAT subnets
* Web subnets
* App subnets
* Database subnets

### NAT subnets:

Is hosting **NAT** **instances** which serve as a **middleman** between **Private** **subnet** and **Internet**. **Route Table** is configured that NAT subnet instances see Internet Gateway (further as IGW) – route to the Internet, Transit Gateway (further as TGW) – route to Database and local VPC Instances. Has its own **Security Group**, which allows all traffic Inbound into NAT subnet to all ports. **IP** addresses **range** varies **from 10.100.253.0/24 to 10.100.255.0/24**. Is deployed in all **3 Availability Zones** (further as AZ).

Web/App subnets:

Web and App subnets have **same configuration**. Are hosting **websites** (Apache, Nginx, Flask, etc.). **Route Table** is configured that it sees TGW – route to DB, NAT instance – route to IGW and local VPC instances. Has its own **Security Group**, which allows port **80** and port **443** (HTTP and HTTPS) traffic from NAT instances. **IP** addresses **range** varies **from 10.100.1.0/24 to 10.100.6.0/24.** Is deployed in all **3** **AZ**s.

### Database subnets:

Database subnets are hosting **database instances**. **Route Table** is configure that it sees TGW (route to Main VPC and IGW) and local VPC instances. Has its own **Security Group**, which allows port **80** and port **443** traffic **from** **TGW**. **IP addresses** range varies **from 10.200.1.0/24 to 10.200.3.0/24**. Is deployed in all **3 AZ**s.

## Transit Gateway

Transit Gateway connects 2 VPCs and our InfraLab (server on-premises) through VPN connection (which is not complete yet). It provides one-way internet connection for Private VPC. Has its own Route Tables (see diagram above). Therefor for our infrastructure TGW is configured differently with no default propagation and unified route table.

## VPC Flow Logs

All traffic that is going through Main VPC is registered by Flow Logs (both, accepted and rejected traffic). Logs are stored in S3 bucket called flow-log-bucket-rdenvi. AWS is automatically sorting everyday traffic throughout different folders.

## Elastic Load Balancer

Elastic load balancer is responsible for managing the traffic load that will be generated by the users among 3 availability zones for much faster accessibility. Has its own **Security Group** which allows port **80** so that the users can only connect through ELB without violating the privacy of the infrastructure. **WEBLB-885405402.eu-central-1.elb.amazonaws.com**

# Billing

Whenever budget exceeds 4.00USD an alarm message is sent to root account e-mail (r.asvicas@student.fontys.nl).