

ICT & Infra S3 Monitoring & Supporting Services, week 5

Class:	CB01
Student number:	4961854
Student name:	Heiko Morales

Introduction

In this practice I am going to create a load balancer with the nginx software. This load balancer will distribute the workload between two different web servers. In addition, it will also act as a proxy manager and host the SSL certificates.

Assignment. Nginx load balancer

First we will connect to the machine and install nginx

```
sudo apt-get install epel-release -y
```

```
sudo apt-get install nginx -y
```

Once installed we must go to the configuration file in "/etc/nginx/nginx.conf".

in the server section we put the servers that are going to need port 80 redirection to port 433 to have SSL encryption adding https instead of http. On the other hand, in the upstream section we will add the servers that will share the load.

```
server{
    listen 80 default_server;
    listen [::]:80 default_server;
    server_name firepassLB;
    root /usr/share/nginx/html;

    #Load configuration files for the default server block.
    include /etc/nginx/default.d/*.conf;
    location /{

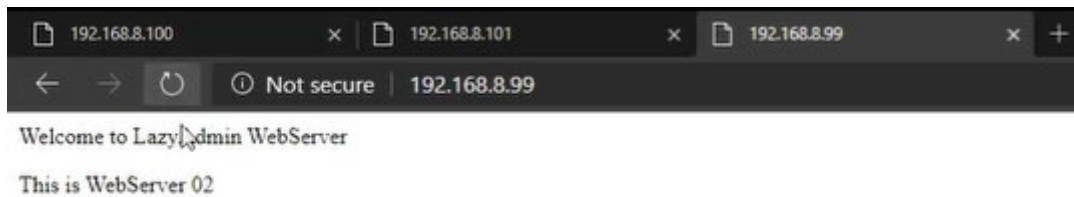
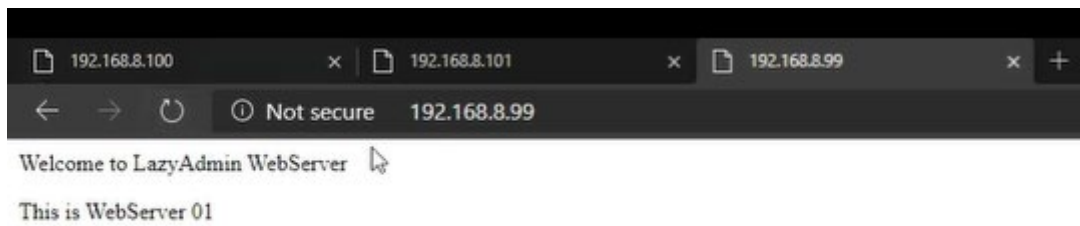
    }
    error_page 404 /404.html;

    location = /40x.html {
        proxy_pass https://192.168.8.100;
        proxy_pass https://192.168.8.101;
        proxy_pass https://x.x.x.x;
    }

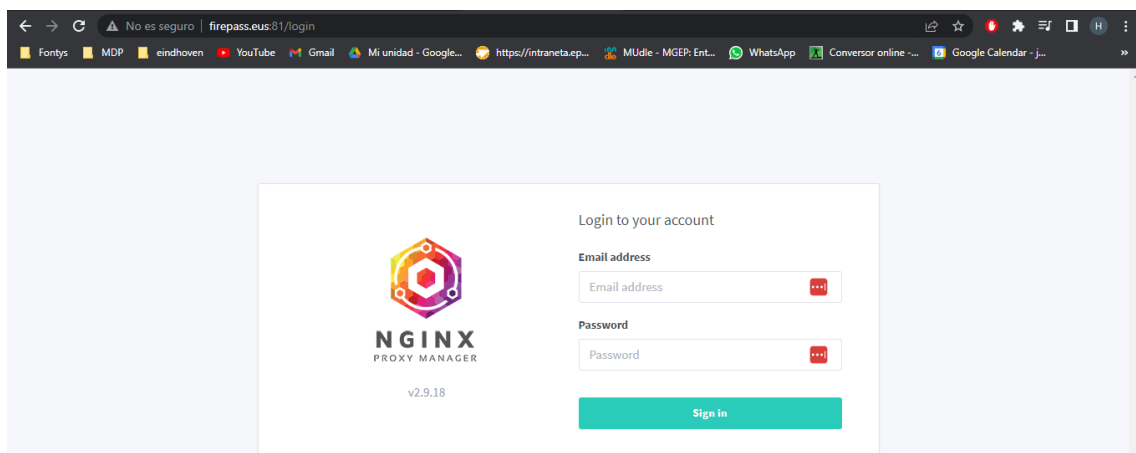
    error_page 500 502 503 504 /50x.html;
    location = /50x.html {

    }
}

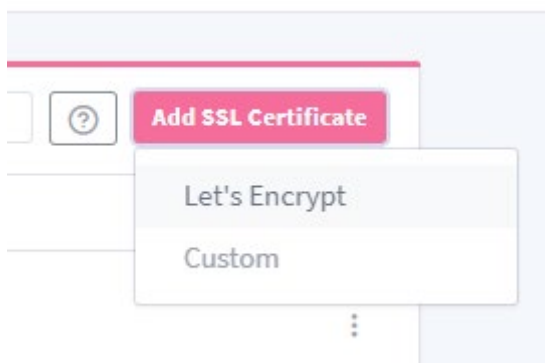
upstream backend {
    server 192.168.8.100;
    server 192.168.8.101;
}
```



Once everything is done, we will be able to see that in the browser we have the two different servers running. But there is no HTTPS. This is because we haven't configured it yet. By accessing port 81, a UI will be displayed to facilitate the task.



Once inside we will go to the SSL certificates section and in the add button we will select the first one.



we will add the data and hit save

Add Let's Encrypt Certificate ✕

Domain Names *

*.firepass.eus

Add *.firepass.eus...

Test Server Reachability

ⓘ Test whether the domains are reachable from the public internet using Site24x7. This is not necessary when using the DNS Challenge.

Email Address for Let's Encrypt *

heiko.morales@alumni.mondragon.edu

⋮


☐ Use a DNS Challenge

☒ I Agree to the [Let's Encrypt Terms of Service](#) *

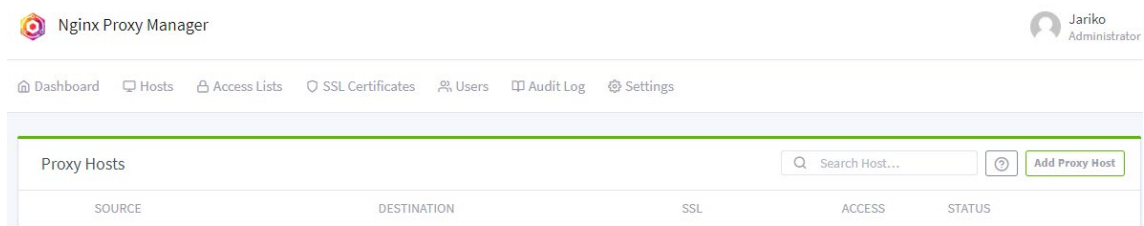
Cancel

Save

a new record will be created for us

	<div>firepass.eus</div> <div>Created: 5th October 2022</div>	Let's Encrypt	4th March 2023, 8:50 am
---	--	---------------	-------------------------

later we go to the proxy section and click on add proxy host.



We will fill in the form and click on SSL.

This screenshot shows the 'New Proxy Host' form with the 'Details' tab selected. The form includes the following fields and options:

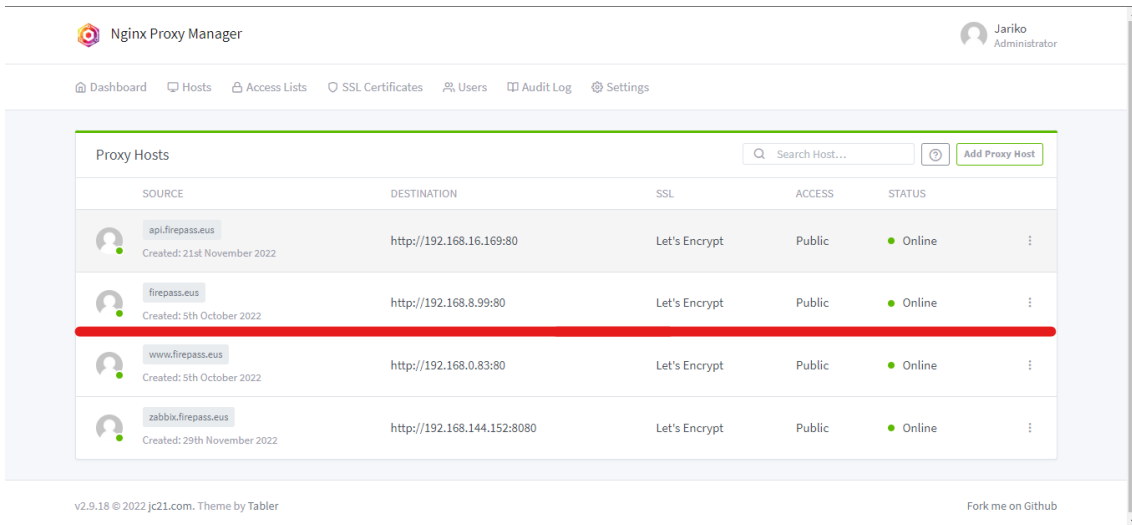
- Domain Names ***: A text input field containing 'firepass.eus'.
- Scheme ***: A dropdown menu set to 'http'.
- Forward Hostname / IP ***: A text input field containing '192.168.8.99'.
- Forward Port ***: A text input field containing '80'.
- Cache Assets**: A toggle switch that is turned on.
- Block Common Exploits**: A toggle switch that is turned on.
- Websockets Support**: A toggle switch that is turned on.
- Access List**: A text input field containing 'Publicly Accessible'.
- At the bottom right, there are 'Cancel' and 'Save' buttons.

in SSL we will add the previously requested certificate and save.

This screenshot shows the 'New Proxy Host' form with the 'SSL' tab selected. The form includes the following fields and options:

- SSL Certificate**: A text input field containing 'firepass.eus'.
- Force SSL**: A toggle switch that is turned on.
- HTTP/2 Support**: A toggle switch that is turned on.
- HSTS Enabled ?**: A toggle switch that is turned on.
- HSTS Subdomains**: A toggle switch that is turned on.
- At the bottom right, there are 'Cancel' and 'Save' buttons.

And we will see how the new registry has been created.

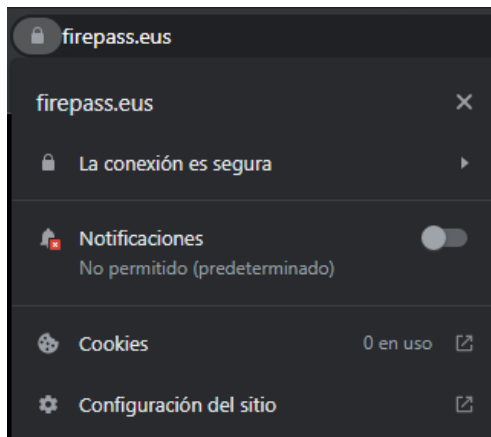


The screenshot shows the Nginx Proxy Manager web interface. At the top, there's a navigation bar with links to Dashboard, Hosts, Access Lists, SSL Certificates, Users, Audit Log, and Settings. The user 'Jariko Administrator' is logged in. The main section is titled 'Proxy Hosts' and contains a table with the following data:

SOURCE	DESTINATION	SSL	ACCESS	STATUS
api.firepass.eus <small>Created: 21st November 2022</small>	http://192.168.16.169:80	Let's Encrypt	Public	Online
firepass.eus <small>Created: 5th October 2022</small>	http://192.168.8.99:80	Let's Encrypt	Public	Online
www.firepass.eus <small>Created: 5th October 2022</small>	http://192.168.0.83:80	Let's Encrypt	Public	Online
zabbix.firepass.eus <small>Created: 29th November 2022</small>	http://192.168.144.152:8080	Let's Encrypt	Public	Online

At the bottom of the interface, it says 'v2.9.18 © 2022 jc21.com. Theme by Tabler' and 'Fork me on Github'.

if we check it, we can see that it works perfectly



```
C:\Users\heiko>nslookup
Servidor predeterminado: dns.google
Address: 8.8.8.8

> firepass.eus
Servidor: dns.google
Address: 8.8.8.8

Respuesta no autoritativa:
Nombre: firepass.eus
Address: 3.74.73.9
```