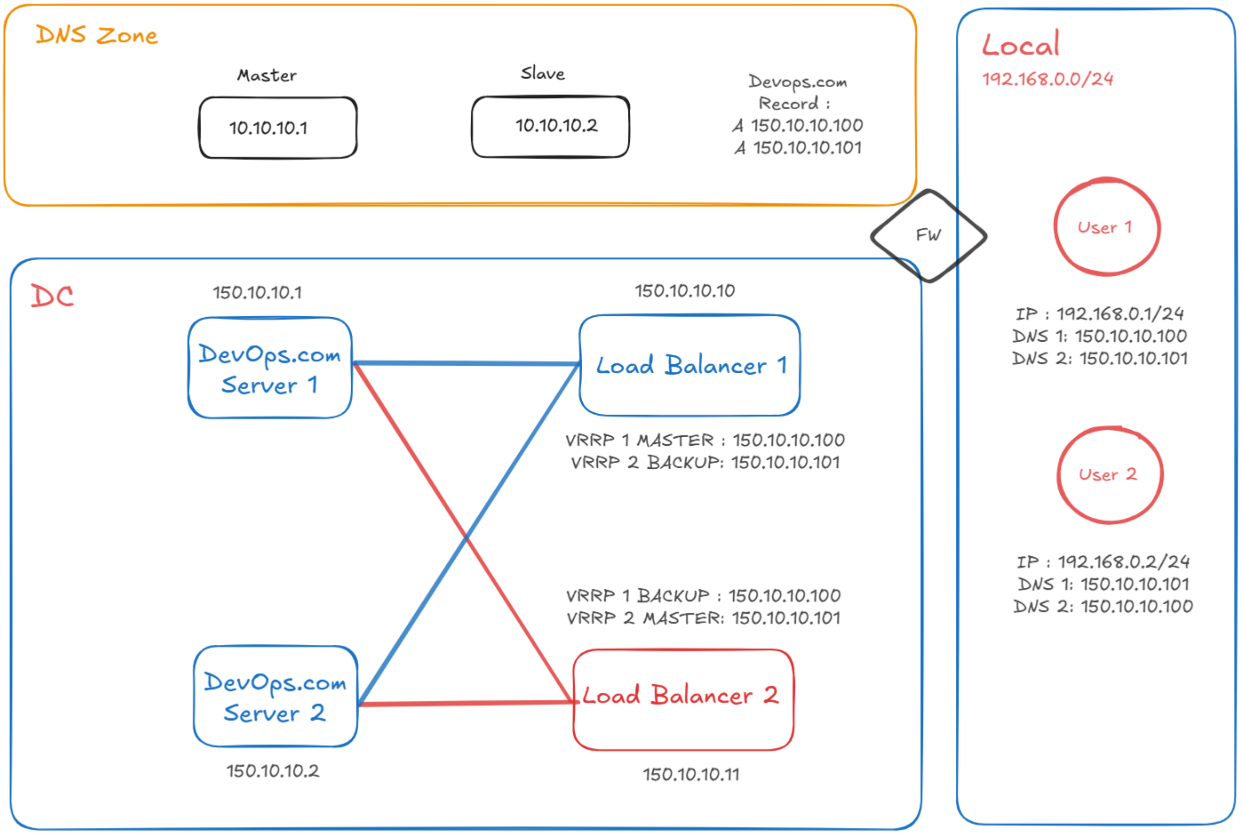
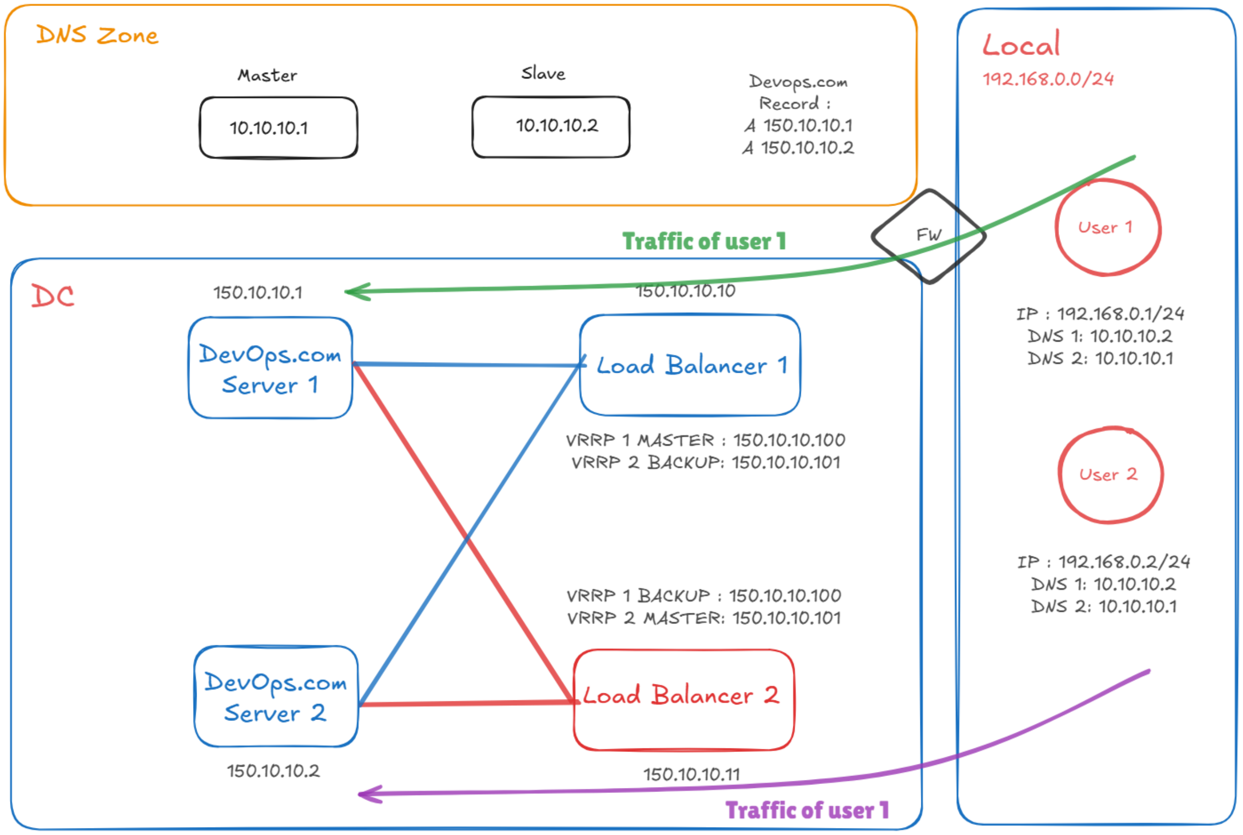
Exercise: Implementing Active/Active Load-Balancer with KEEPALIVED and NGINX servers and use them as SSL termination

Khaloakbari@gmail.com

Physical Topology



Traffic Flow :



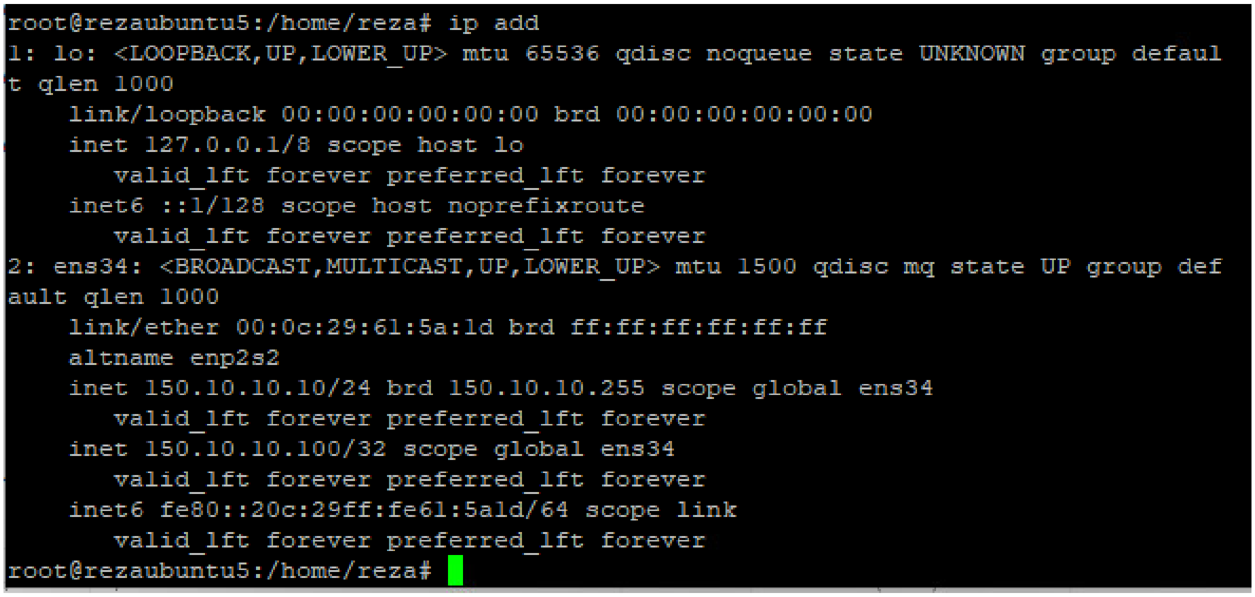
Step-by-Step Process:

1. **Client Request to Access devops.com**
   - A client initiates a request to access the website **devops.com** by entering the URL in their browser or through another application.
   - The browser first needs to resolve the domain name **devops.com** into an IP address. For this purpose, it sends a DNS query to the configured DNS resolver.
2. **DNS Resolution**
   - The DNS server associated with **devops.com** has two IP addresses registered for the domain. These IP addresses correspond to the load balancers that manage traffic for the website.
   - To distribute traffic evenly, the DNS server uses the **Round Robin** method to return one of the two IP addresses.
   - In this instance, the DNS server returns the first IP address, which is the **virtual IP (VIP)** of the primary load balancer configured using the **VRRP (Virtual Router Redundancy Protocol)**.

3. **Client Traffic to the Load Balancer**
   - The client sends its request to the IP address provided by DNS. This address belongs to the **primary load balancer**, which is designated as the **master** in the VRRP configuration.
   - The load balancer receives the client's HTTPS request for **https://devops.com**.
4. **Load Balancer Handling the Request**
   - Based on its configuration, the load balancer decides which backend web server will handle the client's request. This decision might be based on algorithms like **Round Robin**, **Least Connections**, or **Weighted Distribution**.
   - The selected web server's IP address is retrieved, and the request is forwarded.
5. **Protocol Translation (HTTPS to HTTP)**
   - The client's traffic from the client to the load balancer is secured using **HTTPS** (encrypted communication).
   - Once the load balancer processes the request, it forwards it to the backend web server using **HTTP** (unencrypted communication). This configuration helps offload the SSL/TLS encryption process from the web servers to the load balancer.
6. **Web Server Response**
   - The web server processes the request and generates a response (e.g., the requested webpage or data).
   - The response is sent back to the load balancer over **HTTP**.
7. **Response to the Client**
   - The load balancer receives the response from the web server.
   - Before sending the response back to the client, the load balancer re-encrypts the communication using **HTTPS** to maintain security.
   - Finally, the response is delivered to the client, and the website content (e.g., **devops.com**) is displayed in the browser.

LB1

IP address on First LB when running VRRP with keepalived in active/active mode



```
root@rezaubuntu5:/home/reza# ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: ens34: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group def
ault qlen 1000
    link/ether 00:0c:29:61:5a:1d brd ff:ff:ff:ff:ff:ff
    altname enp2s2
    inet 150.10.10.10/24 brd 150.10.10.255 scope global ens34
       valid_lft forever preferred_lft forever
    inet 150.10.10.100/32 scope global ens34
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe61:5a1d/64 scope link
       valid_lft forever preferred_lft forever
root@rezaubuntu5:/home/reza#
```

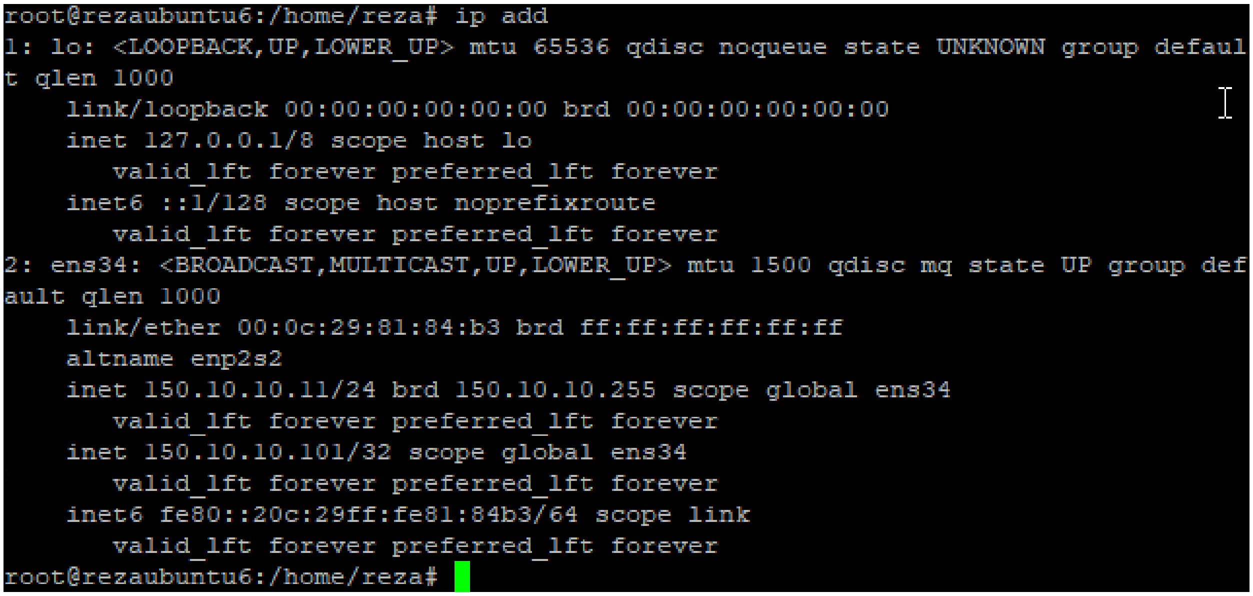
Configuration on LB 1

```
vrrp_instance VI_1 {

state MASTER # Change to BACKUP on the other server

interface ens34 # Replace with your network interface name

virtual_router_id 51

priority 100 # Set to 50 on the other server

advert_int 1

}

virtual_ipaddress {

150.10.10.100 # Replace with your desired virtual IP address

}
```

```
vrrp_instance VI_2 {

state BACKUP # Change to MASTER on the other server

interface ens34 # Replace with your network interface name

virtual_router_id 52

priority 50 # Set to 100 on the other server

advert_int 1

}

virtual_ipaddress {

150.10.10.101 # Replace with your desired virtual IP address

}
```

LB 2

IP address on second LB when running VRRP with keepalived in active/active mode



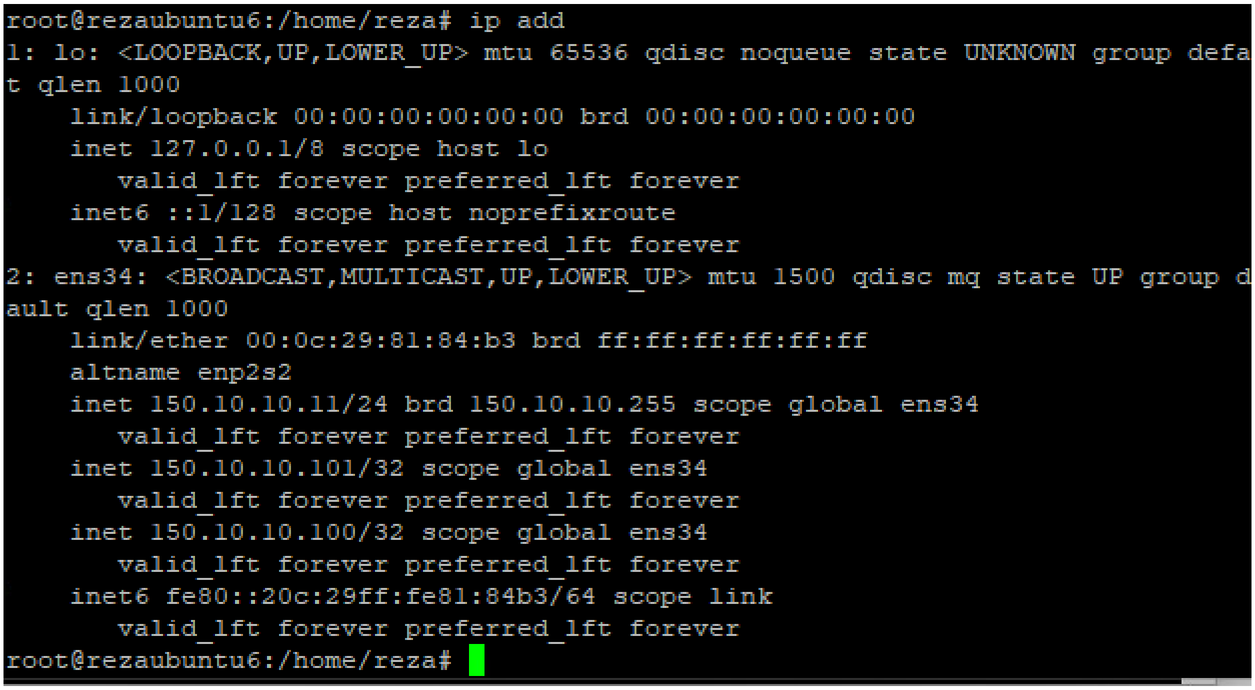
```
root@rezaubuntu6:/home/reza# ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defaul
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: ens34: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group def
ault qlen 1000
    link/ether 00:0c:29:81:84:b3 brd ff:ff:ff:ff:ff:ff
    altname enp2s2
    inet 150.10.10.11/24 brd 150.10.10.255 scope global ens34
       valid_lft forever preferred_lft forever
    inet 150.10.10.101/32 scope global ens34
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe81:84b3/64 scope link
       valid_lft forever preferred_lft forever
root@rezaubuntu6:/home/reza#
```

```
vrrp_instance VI_1 {

state BACKUP # Set the state to BACKUP on the slave server

interface ens34 # Replace with your network interface name

virtual_router_id 51

priority 50 # Set a lower priority than the master server

advert_int 1

virtual_ipaddress {

150.10.10.100

}
```

```
vrrp_instance VI_2 {

state MASTER # Set the state to BACKUP on the slave server

interface ens34 # Replace with your network interface name

virtual_router_id 52

priority 100 # Set a lower priority than the master server

advert_int 1

virtual_ipaddress {

150.10.10.101

}
```

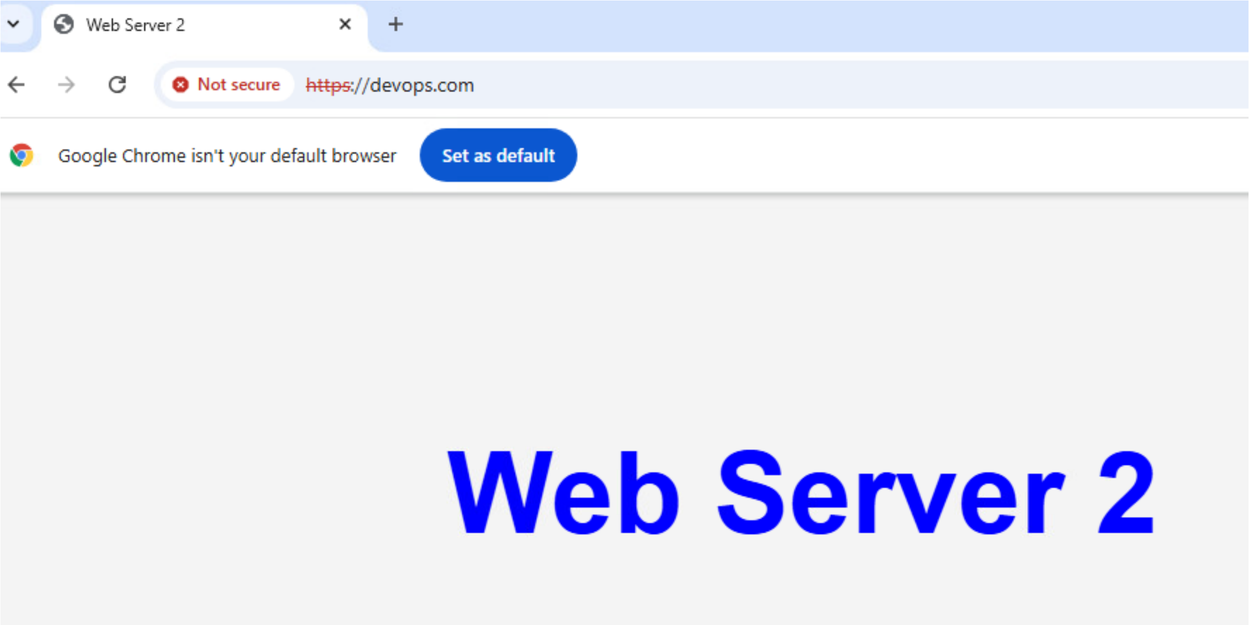
Test :

If we stop the First LB1 ‘s NGINX service, the second LB2 ‘s IP address is as following :



```
root@rezaubuntu6:/home/reza# ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group defa
t qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: ens34: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq state UP group d
ault qlen 1000
    link/ether 00:0c:29:81:84:b3 brd ff:ff:ff:ff:ff:ff
    altname enp2s2
    inet 150.10.10.11/24 brd 150.10.10.255 scope global ens34
       valid_lft forever preferred_lft forever
    inet 150.10.10.101/32 scope global ens34
       valid_lft forever preferred_lft forever
    inet 150.10.10.100/32 scope global ens34
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe81:84b3/64 scope link
       valid_lft forever preferred_lft forever
root@rezaubuntu6:/home/reza#
```

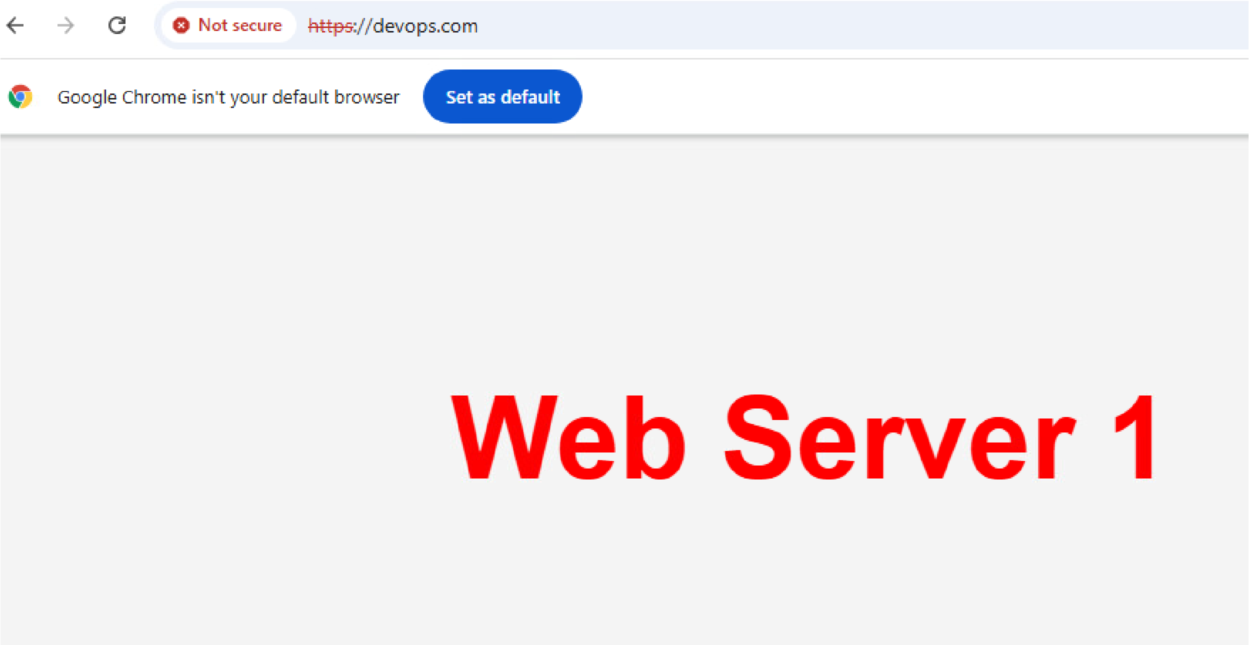
WEB Server 1 :



Google Chrome isn't your default browser

Web Server 2

WEB Server 2



Google Chrome isn't your default browser

Web Server 1