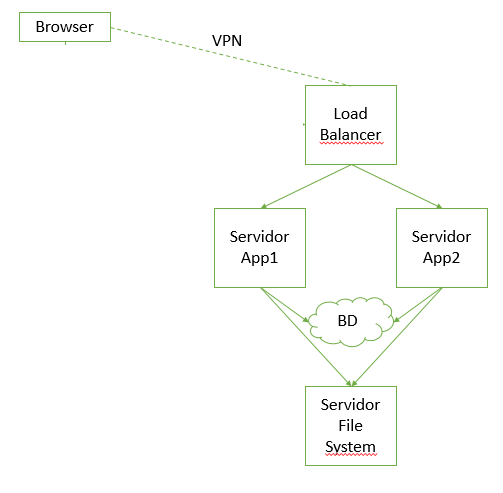
QA Disponibilidad

Arquitectura Base:



HAPROXY:

* Proxy inverso (permite que un browser con conexión a la VPN, pueda ingresar a los servidores AppServer 10.131.137.177 y 10.131.137.179).
* Se utiliza el algoritmo source para disponibilidad en Failover (Un servidor responde a todas las peticiones, y si este se cae el otro se encarga de recibir las peticiones hasta que el servidor1 entre de nuevo en producción)
* Permite recibir comunicaciones seguras (https) con un certificado autofirmado el cual se encuentra en la ruta /etc/ssl/private/mydomain.pem
* Estadisticas de tiempo de estado de vida (UP o DOWN)

NFS:

* Se configura el FileServer con NFS server 10.131.137.194, y se crea una carpeta donde se comparten los recursos en los servidores de aplicación, en esta carpeta es donde se realizan los uploads de la app, las imágenes quedan almacenadas en el fileserver.

Caso de estudio:

HAPROXY (10.131.137.184) con certificado autofirmado

AppServer1 (10.131.137.179)

AppServer2 (10.131.137.177)

BD en Nube (mlab)

File Server (10.131.137.194)

En el AppServer1 hay una app corriendo por el puerto 3006

En el AppServer2 hay otra app corriendo por el puerto 3006

Para comprobar el funcionamiento, en un browser (conectado a la VPN) entre:

<http://10.131.137.179:3006> y <http://10.131.137.177:3006>

Para validar el HAproxy se ingresa por la ruta <http://10.131.137.184>, donde debe responder uno de los dos servidores de aplicación.

Instalación de HAProxy:

En CentOS:

$ sudo yum install haproxy

Configuración en el HAPROXY:

$ sudo vim /etc/haproxy/haproxy.cfg

En el haproxy.cfg, se agregan las siguientes líneas y el certificado auto firmado

*stats enable*

*stats hide-version*

*stats realm HAproxy Statistics*

*stats uri /haproxy?stats*

*stats auth admin:admin*

*#---------------------------------------------------------------------*

*# main frontend which proxys to the backends*

*#---------------------------------------------------------------------*

*frontend http-in*

*bind \*:80*

*default\_backend http\_app*

*frontend https-in*

*bind \*:443 ssl crt /etc/ssl/private/mydomain.pem*

*default\_backend http\_app*

*backend http\_app*

*mode http*

*option httplog*

*# balance leastconn*

*# balance roundrobin*

*balance source*

*server app1 10.131.137.179:80 check*

*server app2 10.131.137.177:80 check*

*backend https\_app*

*mode tcp*

*option http-server-close*

*option forwardfor*

*reqadd X-Forwarded-Proto:\ https*

*reqadd X-Forwarded-Port:\ 443*

*option forwardfor if-none*

*balance roundrobin*

*server app1 10.131.137.177:443 check*

*server app2 10.131.137.179:443 check*

Configuración NFS

<https://www.howtoforge.com/nfs-server-and-client-on-centos-7>

En el servidor NFS se configura la carpeta a compartir en el archivo /etc/exports: /home/nfs \*(rw,sync,no\_root\_squash,no\_all\_squash)

Y en los clientes se conecta la carpeta:

10.131.137.194:/home/nfs /home/app/proyecto01/st0263\_subirImagenesApp/public/uploads/ nfs defaults 0 0