Administración de Sistemas y Redes

Curso 2022-23 - Práctica 9

Balanceo de carga con HAProxy (cluster de alta disponibilidad) y SAN (Storage Area Network)

OPCIONAL

Balanceo de carga con HAProxy

Harán falta tres máquinas con Linux que llamaremos balanceador, web1 y web2 aunque podrían ser más de dos los servidores web y no necesariamente Linux. Inicialmente estarán conectadas a Internet vía NAT con el adaptador por defecto.

Se pueden hacer tres instalaciones limpias o partir de una y clonarla dos veces más. Si se hace una clonación, en la política de dirección MAC debe estar activa la opción "Incluir solo dirección MAC de adaptador de red NAT" o bien "Generar nuevas direcciones MAC para todos los adaptadores de red" antes de empezar a clonar. Como es lógico no se puede tener tres máquinas en una misma red con una misma MAC.

Instalar el servidor web en los nodos web1 y web2 y haproxy en el nodo balanceador. Por comodidad se puede tener todo en las tres máquinas y luego se clonan. También se instalará el php.

```
# dnf install httpd haproxy php
```

Apagar ahora la máquina virtual y cambiar su adaptador de NAT a red sólo anfitrión. Si nuestro anfitrión anda escaso de memoria podemos rebajar la RAM a 1,5 GB en las máquinas virtuales.

Hacer dos clones más, serán necesarios tres equipos.

En las preferencias globales de red VirtualBox deshabilitar el servidor DHCP para la red de solo anfitrión.

Iniciar las tres máquinas. Con la orden # ip addr hay que mirar qué adaptador de red está activo. Si las máquinas proceden de instalaciones limpias probablemente será enp0s3.

En el balanceador modificar la configuración de `enp0s3` para que tenga una dirección IP 192.168.56.20 estática.

```
# nmcli connection modify enp0s3 ipv4.method manual ipv4.address
192.168.56.20/24
```

Reiniciar el equipo (o la red: `# nmcli con reload; nmcli net off; nmcli net on`) y comprobar con la orden # `ip addr` que el adaptador tiene la dirección IP correcta.

Repetir los pasos anteriores con los equipos web1 y web2 pero poniendo las direcciones IP respectivas 192.168.56.21 y 192.168.56.22.

Con las tres máquinas iniciadas se puede comprobar que hay conectividad entre ellas con la orden ping, bien desde una de ellas o bien desde el anfitrión:

```
C:\> ping 192.168.56.20
C:\> ping 192.168.56.21
C:\> ping 192.168.56.22
```

El siguiente paso es activar los servidores web. En web1 y web2 crear el archivo `/var/www/html/index.html` con:

```
<html>
<head>
    <title>Servidor web 1</title>
</head>
<body>
    <h1>Servidor web 1</h1>
</body>
</html>
```

Hay que acordarse de poner "Servidor web 2" en web2.

Abrir el cortafuegos para tráfico web en las tres máquinas:

```
# firewall-cmd --add-service http
# firewall-cmd --add-service http --permanent
```

En web1 y web2 iniciar el servicio httpd:

```
# systemctl start httpd.service
# systemctl enable httpd.service
```

Desde el anfitrión con Windows comprobar con cualquier navegador que se puede acceder a ambos servidores web: http://192.168.56.21/ y http://192.168.56.22/

En este punto ya tenemos dos servidores web activos y corriendo, se pueden minimizar ambas máquinas virtuales. El siguiente paso es configurar el balanceador de carga.

En el equipo balanceador hay un archivo llamado `/etc/haproxy/haproxy.cfg`, hay que cambiar las siguientes líneas para que escuche en el puerto 80 y balancee entre los dos servidores web recién instalados:

```
frontend main
    # bind *:5000
    bind *:80

[...]

backend app
#    server app1 127.0.0.1:5001 check
#    server app2 127.0.0.1:5002 check
#    server app3 127.0.0.1:5003 check
#    server app4 127.0.0.1:5004 check
    server web1 192.168.56.21:80 check
    server web2 192.168.56.22:80 check
```

Hay que iniciar ahora servicio de balanceo de carga

```
# systemctl start haproxy.service
# systemctl enable haproxy.service
```

También se puede minimizar ahora esta máquina virtual.

En el navegador del anfitrión ir a http://192.168.56.20/ ¿qué aparece?
Tras refrescar la página varias veces ¿qué aparece?

Si se detiene ahora uno de los servidores web (web1 o web2) con `# systemctl stop httpd.service` (o bien se apaga la máquina) y se refresca de nuevo la página ¿qué aparece?

Al detener el servicio httpd o apagar también el otro servidor web y refrescar de nuevo la página ¿qué aparece?

Elimine los ficheros index.html y en su lugar ponga estos ficheros index.php en ambos servidores web.

```
<html>
    <script type="text/javascript">
    // muestra las cookies que hay en el navegador
    function MuestraCookies() {
    var todas=document.cookie;

    // array de pares nombre - valor
    en_array=todas.split(';');

    // muestra cada par
    for (var i=0; i<en_array.length; i++) {
      nombre=en_array[i].split('=')[0];
      valor=en_array[i].split('=')[1];
      document.write("cookie "+nombre+" = "+valor+"<br>\n\r");
    }
  }
</script>
<script type="text/javascript">
  MuestraCookies();
</script>
<body>
<?php
  // añade una cookie de sesión
  session_start();
  // muestra el servidor que atiende la petición
  $server_ip=$_SERVER['SERVER_ADDR'];
  echo "petición servida por: ".$server_ip."<br>".PHP_EOL;
?>
</body>
</html>
```

¿Cambia la cookie de sesión? Experimente modificando haproxy.cfg con este contenido que permite hacer sesiones "pegajosas". Borre de vez en cuando las cookies del navegador en la última hora para hacer pruebas y añada capturas de pantalla.

```
balance roundrobin
   cookie mi_cookie insert indirect nocache
   server web1 192.168.56.21:80 check cookie valor1
   server web2 192.168.56.22:80 check cookie valor2
```

¿Cuál sería la utilidad de estas sesiones pegajosas frente a las de servidor alternante?

SAN (Storage Area Network)

Los servidores NAS ya conocidos permiten proporcionar y compartir carpetas y ficheros ya sea vía protocolo SAMBA/CIFS o vía NFS sobre sistemas de ficheros muy habituales como son NTFS, ext4 o xfs.

Los servidores SAN en cambio proporcionan bloques a otros equipos desde los cuales estos bloques se ven como discos externos. Para estos servidores SAN se emplean conexiones basadas en canal de fibra (FC) con el protocolo FCP que permite velocidades de hasta 16Gb/s aunque también se pueden emplear protocolos sobre Ethernet siendo el iSCSI (Internet Small Computer System Interface) el más frecuente.

A diferencia de los NAS no es posible compartir un disco SAN excepto si se emplea algún tipo de sistema de ficheros de cluster diseñado específicamente para esto como puedan ser GFS2 (RedHat), CSV (Microsoft), GPFS (IBM) o Xsan (Apple).

Para esta práctica se van a emplear dos equipos, uno que hará de servidor (llamado "objetivo/target" de ahora en adelante) y proporcionará los bloques de un disco completo y los de una imagen de disco. El otro hará de cliente (llamado "iniciador/initiator" de ahora en adelante) que montará los dos discos de red proporcionados por el servidor/objetivo. Este iniciador o cliente verá tales recursos como discos internos.

Ambas máquinas virtuales tendrán un adaptador de red conectado a NAT para descargar el software necesario y otro conectado a una red interna que se empleará exclusivamente para el tráfico iSCSI.

Las operaciones a realizar son a partir de dos Linux mínimos o con GUI: primero añadir un segundo adaptador de red interna a ambas máquinas virtuales y además al equipo que actuará como servidor añadirle un segundo disco.

Puestos en marcha ambos sistemas, la configuración de los adaptadores de red interna pueden hacerse con las órdenes nmcli ya conocidas aplicándolas al adaptador enp0s8 de manera que el servidor (objetivo/target) tenga la dirección IP 192.168.222.1 y el cliente (iniciador) la 192.168.222.2 quedando este adaptador en la zona `"internal"` del cortafuegos. Reiniciar la red y comprobar con la orden ping que ambos equipos se ven entre sí. Verificar también que cada adaptador está en la zona correspondiente:

```
# firewall-cmd --get-active-zones
```

En el objetivo comprobar que aparece el disco nuevo y crear un fichero de 1 GB que se exportará como otro disco.

```
# fallocate --length 1G fichero.dsk
```

A continuación instalar el software, poner en marcha el servicio y abrir el puerto TCP 3260.

```
# dnf -y install targetcli
# systemctl enable --now target
# firewall-cmd --add-service=iscsi-target --zone=internal --permanent
# firewall-cmd --add-service=iscsi-target --zone=internal
```

Antes de configurar el objetivo y el iniciador debemos definir dos IQN. IQN son las iniciales de iSCSI Qualified Name y deben ser únicos. El formato que se emplea (RFC 3720) es iqn.aaaa-mm.mi.dominio:algo, por ejemplo iqn.2023-02.mi.dominio:c3po. Usaremos para el objetivo iqn.2023-02.as.servidor:1111 y para el iniciador iqn.2023-02.as.cliente:2222, nótese que no es necesario que existan los dominios de Internet que se indican, es solo un convenio. A continuación de los ":" puede ponerse cualquier cosa, un número de serie, un nombre de equipo o incluso nada eliminando los dos puntos.

En el servidor hay que crear al menos un IQN objetivo, dos objetos para los almacenes de bloques y dos LUN (logical unit number). Opcionalmente pueden definirse más cosas.

```
# targetcli
/> ls
/> cd iscsi
/iscsi> create iqn.2023-02.as.servidor:1111
/iscsi> ls
/iscsi> cd /backstores/block
```

Suponemos que el disco nuevo es /dev/sdb y el fichero imagen de disco es fichero.dsk, se crea cada elemento y se verifica que se ha creado satisfactoriamente.

```
/backstores/block> create name=mi_disco_sdb dev=/dev/sdb
/backstores/block> ls
/backstores/block> cd /backstores/fileio
/backstores/fileio> create name=mi_fichero file_or_dev=fichero.dsk
/backstores/fileio> ls
```

Si el servidor tiene varios interfaces, debería especificarse ahora la dirección IP del adaptador por donde se desea escuchar, de lo contrario el servidor escuchará por todos los adaptadores. Vamos a saltar este paso pero en la vida real habría que borrar antes el acceso por defecto y añadir un acceso exclusivo para la dirección IP del adaptador de red a emplear. En este caso el servidor debería escuchar solo por el adaptador de red interna que tiene de dirección IP 192.168.222.1.

```
/backstores/fileio> cd /iscsi/iqn.2023-02.as.servidor:1111/tpg1/portals
/iscsi/iqn.20...servidor:1111/tpgi/portals> delete 0.0.0.0 3260
/iscsi/iqn.20...servidor:1111/tpgi/portals> create 192.168.222.1
```

Creación de las dos LUNs y de un ACL sin restricciones para el iniciador.

```
/backstores/fileio> cd /iscsi/iqn.2023-02.as.servidor:1111/tpg1/luns
/iscsi/iqn.20...111/tpg1/luns> create /backstores/block/mi_disco_sdb
/iscsi/iqn.20...111/tpg1/luns> create /backstores/fileio/mi_fichero
/iscsi/iqn.20...111/tpg1/luns> ls
/iscsi/iqn.20...111/tpg1/luns> cd ../acls
/iscsi/iqn.20...111/tpg1/acls> create iqn.2023-02.as.cliente:2222
/iscsi/iqn.20...111/tpg1/acls> ls
/iscsi/iqn.20...111/tpg1/acls> exit
```

Si todo ha ido correctamente se habrá guardado la configuración en `/etc/target/saveconfig.json`

En el iniciador, instalar el software.

```
# dnf -y install iscsi-initiator-utils
```

Editar el nombre del iniciador.

```
# vi /etc/iscsi/initiatorname.iscsi
InitiatorName=iqn.2023-02.as.cliente:2222
```

Verificar si ve al servidor.

```
# iscsiadm --mode=discovery --type=sendtargets --portal=192.168.222.1
```

Si todo es correcto se verá como respuesta la dirección IP del servidor y su IQN.

Se puede hacer ahora un login interactivo (--logout para salir)

```
# iscsiadm --mode=node --targetname=iqn.2023-02.as.servidor:1111 --
portal=192.168.222.1 --login
```

A partir de este momento con `# lsblk` deben aparecer en el iniciador dos nuevos discos sdb y sdc si no había previamente otros. También pueden verse con # cat /proc/scsi/scsi

Estos dos discos ya se pueden particionar, formatear y montar. Como no se sabe si van a ser sdb1 o sdd1 o cualquier otra cosa, es conveniente en el `/etc/fstab` montarlos por UUID en vez de por nombre. Es decir en vez de algo como esto:

```
/dev/sdb1 /mnt/disco ext4 _netdev 0 0
```

obtener el UUID con `# blkid /dev/sdb1` y poner en fstab

```
UUID="0fc99ba2-912f-4519-ab6d-04c76608c303" /mnt/disco ext4 _netdev 0 0
```

De esta forma siempre se montará en /mnt/disco con independencia de que sea vea con cualquier nombre. La opción _netdev garantiza que se espera a que se inicie primero la red.

En vez de ext4 puede emplearse ext2, ext3, xfs o cualquier otro sistema de ficheros que se desee.

Hágalo así con ambas particiones y reinicie el sistema. Compruebe que se realiza todo de forma automática en el iniciador y que ha arrancado correctamente el demonio iscsi con:

```
# systemctl status iscsi
```

Añada una captura de pantalla de la orden `# df` y de la `# cat /proc/scsi/scsi`

Consideraciones de seguridad: aunque no entra en el ámbito de esta asignatura debería permitirse el acceso con `# targetcli` solo a la dirección IP del servidor deseada y se debería poner una ACL con las especificaciones necesarias. También debería abrirse el cortafuegos solo para el iniciador y debería añadirse un nombre de usuario CHAP y contraseña, tanto en el servidor como en el iniciador.

A título informativo, las acciones a realizar para dotar de usuario y contraseña a la conexión serían las que siguen.

En el cliente, lo primero cerrar la conexión actual desmontando antes las unidades si fuera necesario.

```
# iscsiadm --mode node --targetname iqn.2023-02.as.servidor:1111 --
portal 192.168.222.1 --logout
```

En el servidor, indicar que se necesita autentificación (en el tpg) e indicar el usuario y clave en la acl del iniciador.

```
# targetcli
/> cd /iscsi/iqn.2023-02.as.servidor:1111/tpg1
/iscsi/iqn.20...dor:1111/tpg1> set attribute authentication=1
/iscsi/iqn.20...dor:1111/tpg1> cd /iscsi/iqn.2023-
02.as.servidor:1111/tpg1/acls/iqn.2023-02.as.cliente:2222
/iscsi/iqn.20....cliente:2222> set auth userid=mi_usuario
/iscsi/iqn.20....cliente:2222> set auth password=mi_clave
```

De nuevo en el cliente editar el fichero donde se especifican los parámetros de conexión cambiando lo siguiente.

```
# vi iscsid.conf
node.session.auth.authmethod = CHAP
node.session.auth.username = mi_usuario
node.session.auth.password = mi_clave
```

Borrar los datos de contacto anteriores, muy importante.

```
# iscsiadm --mode node --targetname iqn.2023-02.as.servidor:1111 --
portal 192.168.222.1 --op delete
```

Verificar de nuevo al servidor.

```
# iscsiadm --mode=discovery --type=sendtargets --portal=192.168.222.1
```

E iniciar sesión.

```
# iscsiadm --mode=node --targetname=iqn.2023-02.as.servidor:1111 --
portal=192.168.222.1 --login
```