Departamento de
Automática y Computación
Automatika eta
Konputazio Saila

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

Linux network namespaces

1. Introducción y objetivos

El objetivo de esta actividad es profundizar un poco más en el uso de *network namespaces*, en concreto en el contexto de LXD.

Llegaremos a crear un escenario de networking entre contenedores donde habrá routers implementados con contendores.

2. Network namespaces

En esta actividad necesitará un simple host con sistema operativo Linux. Esto puede ser la instalación del PC que esté empleando o puede ser una máquina virtual. En el caso de llevar a cabo la actividad en el laboratorio deberá hacerlo en una máquina virtual. Se recomienda por ejemplo una instalación de Ubuntu Server.

Emplee el siguiente comando para ver el listado de procesos corriendo en Linux:

 # ps faxu

Se muestran los procesos en forma de árbol, donde puede ver qué procesos son descendientes de otros.

En el directorio /proc se mapean variables del kernel. Debería tener un directorio dentro de /proc para cada proceso, con nombre el identificador numérico del proceso (PID = Process ID). Dentro de ese directorio hay otro, llamado ns, dentro del cual habrá links que hacen referencia por ejemplo a los diferentes namespaces. En concreto /proc/<PID>/ns/net hace referencia al *network namespace* del proceso (netns a partir de ahora para abreviar), donde <PID> es el identificador numérico del proceso. En este momento todos los procesos deberían estar haciendo referencia al mismo netns.

A continuación cree un contenedor y repita el listado de procesos. Verá ahora también los procesos del contenedor, todos ellos descendientes de un nuevo proceso init. Si mira el netns de uno cualquiera de los procesos del contenedor debería hacer referencia a un valor distinto.

Muchos comandos requieren el nombre del netns para hacerle referencia pero LXD los crea sin asignarles nombre. Esto se puede resolver con sencillez. Para ello necesita que exista el directorio /var/run/netns (créelo si no existe) y dentro de él debe crear un link a cada netns al que quiera hacer referencia, de forma que a partir de ahora lo podremos referenciar por el nombre de este fichero. Por ejemplo[1], suponiendo que el PID del proceso init del contenedor recién creado es 1995 :

 # mkdir –p /var/run/netns

 # ln -sf /proc/1995/ns/net /var/run/netns/net-contenedor1

A partir de ahí podremos hacer referencia al *network namespace* con el nombre net-contenedor1

Puede averiguar también el PID del proceso init de un contenedor con el comando:

 # lxc info <nombre-contenedor>

[1] Más sobre cómo crear link en el manual en línea (*man ln*)

Campus de Arrosadía
Arrosadiko Campusa
31006 Pamplona - *Iruñea*
Tfno. 948 169113, Fax. 948 168924
Email: ayc@unavarra.es

Puede ejecutar un proceso que corra en un netns concreto empleando opciones del comando ip. Por ejemplo[2], para lanzar ifconfig en el namespace anterior podríamos hacer:

 # ip netns exec net-contenedor1 ifconfig -a

3. Virtual Ethernet devices

Lo que emplea LXD para comunicar a los contendores con el host son Virtual Ethernet devices, o veth. Puede leer sobre ellos en el manual en línea[3].

Los veth se crean por pares y lo que se envía por uno se lee por el otro. Veamos cómo usarlos creando un link entre dos contenedores.

Lance 2 contenedores, que llamaremos contenedor1 y contenedor2.

Enlace el netns de cada contenedor a /var/run/netns siguiendo el procedimiento de la sección anterior, con nombres net-contenedor1 y net-contenedor2

Cree un par de veths con el siguiente comando:

 # ip link add v-1a type veth peer name v-1b

Hemos indicado los nombres de ambos extremos, que serán v-1a y v-1b.

Puede borrar la pareja borrando uno cualquiera de ellos, por ejemplo con:

 # ip link del v-1a

Podrá ver ambos interfaces en el namespace del host (es decir, haciendo ifconfig -a en el host). A continuación asignaremos cada veth a uno de los dos contenedores:

 # ip link set dev v-1a netns net-contenedor1

 # ip link set dev v-1b netns net-contenedor2

Dejará de ver los interfaces en el host y los verá en cada contenedor. Ahora simplemente configure dirección IP a cada uno de esos interfaces (desde una Shell en el contenedor o como se ha comentado en la sección anterior usando ip netns exec) y compruebe que los contenedores tienen comunicación entre ellos a través de esos interfaces.

4. Actividad

Cree la topología de la Figura 1 empleando contenedores. Esto quiere decir que todos los equipos que se muestran son en realidad contenedores en el mismo host. Esto incluye a los equipos representados con un símbolo de router IP. En los router IP tendrá que activar el reenvío de paquetes (es un flag del kernel local a cada netns que puede modificar con sysctl). Los links que aparecen en la figura son todos parejas de veth.

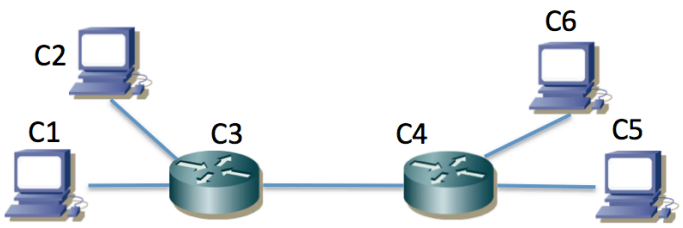

Figura 1 - Topología a crear mediante contenedores

[2] De nuevo más sobre esto en el manual en línea (*man ip-netns*)

[3] *man veth*