Construcción manual de una red entre contenedores

Cloud Computing

Trabajo de Implementación

Introducción

Uno se los propósitos de los contenedores es aislar los entornos de ejecución de servicios diferentes. En particular, es necesario aislar los caminos de comunicación de forma específica para disminuir el grado de vulnerabilidad del sistema resultante frente a ataques intencionados o errores de programación.

Como se ha visto, uno de los mecanismos utilizados por el sistema de contenedores es el de la separación de los espacios de nombres (***namespaces***), de forma que cada contenedor reciba su propio espacio de nombres para cada uno de los recursos nominados a los que tiene aceso en el Sistema Operativo.

De especial relevancia es el espacio de nombres de red, pues no es posible aislar apropiadamente a un contenedor si se permite su comunicación arbitraria con cualquier otro agente en un sistema distribuido.

Los contenedores en Linux utilizan los ***network namespaces*** para establecer un aislamiento apropiado de red, utilizando técnicas basadas en el filtrado de paquetes de red mediante el mecanismos conocido como ***netfilter*** , y que es implementado a través de IPTABLES o, más modernamente, NFTABLES.

Objeto del ejercicio

En un sistema distribuido implementando un servicio en la nube es extremadamente importante entender cómo funciona el sistema de comunicaciones para poder enfocar adecuadamente la resolución de problemas cuando estos surjan.

El presente ejercicio quiere ayudar a entender cómo funcionan los mecanismos subyacentes a los plugins de red utilizados por sistemas como Docker para establecer la comunicación entre contenedores.

Para ello, deberás crear scripts/programas que sean capaces de lanzar contenedores a partir de imágenes Docker, que, inicialmente, no contarán con red (no obtienen una VETH de Docker).

Esos scripts/programs que crees deberán establecer el entorno de red de los contenedores lanzados de forma que:

1. Los contenedores puedan comunicar entre sí mediante protocolos IP
2. Los contenedores puedan comunicar con el HOST
    a. Desde el HOST se pueda comunicar con los contenedores.
3. Los contenedores puedan comunicar con cualquier nodo alcanzable desde el host
    a. Desde nodos que puedan alcanzar al host se pueda establecer algún tipo de comunicación con un contenedor
4. Si los contenedores son desplegados en nodos diferentes, éstos puedan aún comunicarse entre sí como si estuvieran en el mismo segmento de red (protocolo IP).

Los puntos anteriores han sido organizados por nivel de dificultad.

Valoración

La valoración del trabajo se basará principalmente en el nivel de dificultad alcanzado según la progresión establecida anteriormente.

Es importante entender que NO se pretende que la implementación esté lista para producción, pero es importante explicar cómo la aproximación tomada puede llegar a generalizarse. Esto es especialmente relevante para (4).

El código deberá ser entregado en su propio depósito GIT, que deberá poseer uno o varios ficheros Markdown/ASCIIDOC (e.g., README.md) con la explicación del esquema utilizado y su posible generalización.

Observaciones

El trabajo deberá desarrollarse de forma individual.

Para poder llevar a cabo (3) y (4) es necesario usar bien IPTABLES, bien NFTABLES. Ambos sistemas están ampliamente documentados: https://netfilter.org

Para poder llevar a cabo (4) es necesario entender cómo usar enrutamiento estático mediante las facilidades del paquete `iproute2`, en especial, el subcomando `ip route` …