Docker

Álvaro González Sotillo

22 de enero de 2024

Índice

1. Qué es una máquina virtual

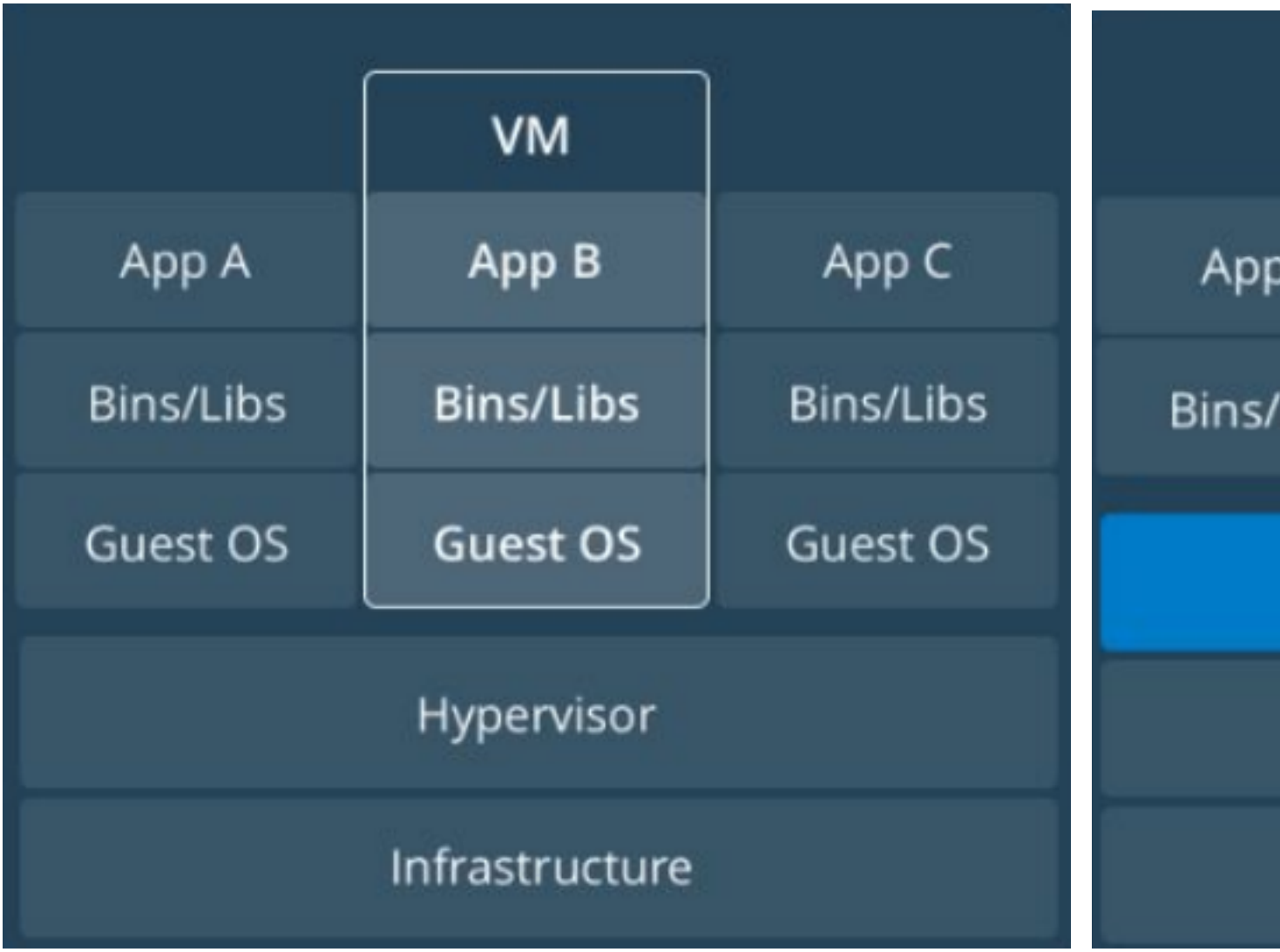
- Un proceso implementa todo el *hardware* de un PC
  - Representa los discos como ficheros
  - La tarjeta de vídeo utiliza una ventana en vez de un monitor
  - La tarjeta de red real se comparte, utilizando redes virtuales
- La BIOS/UEFI consigue arrancar normalmente, y ejecuta un sistema operativo
- Conclusión:
  - Un proceso en una máquina virtual no sabe que es *virtual*
  - Los procesos de la máquina virtual están **aislados** de la máquina real

2. Qué es Docker

- Docker integra diversas capacidades de aislamiento entre procesos que tiene Linux
  - chroot
  - cgroups
  - namespaces
- Usa además
  - mount points, para la comunicación entre *containers*
  - overlayfs, para construir containers acumulando *capas*
  - iptables/netfilter, para simular tarjetas de red
- Conclusión
  - Se pueden crear containers sin usar Docker
  - Docker también aisla procesos entre sí

3. Máquina virtual *vs* Docker

3.1. Comparación gráfica



3.2. Tabla comparativa

	Docker	Máquina Virtual
SO	SO compartido entre contenedores	Nuevo SO para cada VM
Seguridad	Menos seguro, se comparte el kernel	Más seguro, no se comparte nada
Rendimiento	Rendimiento rápido	La virtualización es más lenta
Tiempo de arranque	Rápido (segundos)	Lento (minutos)
Necesidades de memoria	Ligera	Requiere mucha memoria
Necesidades de almacenamiento	Normalmente megabytes	Normalmente gigabytes
Portabilidad	En cualquier linux moderno	El hardware emulado puede diferir entre diferentes s

4. Componentes Docker

- **Cliente**: Usa el *socket* de Docker para controlar el servidor
- **Servidor** (demonio): Gestiona las imágenes contenedores
- **Imagen**:
  - Personalizadas: con un *dockerfile*
  - Del registro: Imágenes prediseñadas (equivalentes a un fichero **OVA** para máquinas virtuales)
- **Contenedor** Una imagen en ejecución
- **Registro**: Almacén público de imágenes

5. Portabilidad de Docker

- ¿Hay Docker para Windows?
  - Respuesta corta: No
  - Respuesta larga:
    - Hay un *cliente* Docker para Windows
    - Se instala una máquina virtual con Linux
    - El cliente Docker se conecta al servidor Docker de la máquina virtual
    - También hay *containers* para Windows, solo instalables en Windows

6. Instalación de Docker

- Página oficial
- Para Debian/Ubuntu:
  - Desinstalar las versiones instaladas con `apt-get`

```
for pkg in docker.io docker-doc docker-compose podman-docker containerd runc
do
    sudo apt-get remove $pkg
done
```

  - Usar el *script* (no recomendado en producción)

```
curl https://get.docker.com/ | sh
```

6.1. Prueba de instalación

- Solo `root` y el grupo `docker` pueden usar el servidor Docker

```
docker run hello-world
```

7. Imágenes y *containers*

7.1. Conceptos básicos

- Una imagen se ejecuta en un *container*. La misma imagen se puede ejecutar en varios *containers*
- Una imagen provee un programa a ejecutar cuando se ejecuta con `run`
  - Cuando ese programa termina, el *container* se destruye
  - Se puede especificar otro programa a ejecutar
  - Se puede conectar la consola a dicho programa

```
docker run debian # crea un container y termina inmediatamente, bash no tiene entrada
docker run -it debian # crea un container y conecta la consola al programa por defecto
docker run debian /bin/bash -c "echo Un mensaje y termino"
```

7.2. Lista de containers e imágenes

```
docker images
docker ps # containers en ejecucion
docker ps -a # todos los containers
```

- Conclusión: `run` no ejecuta *containers*, sino que crea y ejecuta *containers*
  - `run` = `create` + `start`
- Los "parámetros"de un *container* se especifican en su creación. No se pueden cambiar al ejecutarlos.
- Los *container* tienen un nombre. Si no se especifica, Docker inventa uno.

8. Volúmenes

- Los *containers* son inmutables.
  - Los datos modificados en el *container* son una capa adicional (overlayfs)
  - Desaparecen al apagar el *container*
- La persistencia se puede conseguir con
  - volúmenes
  - *mounts*

8.1. *mounts*

- Equivalente a un `mount --bind`

```
docker run -it --mount type=bind,src="$(pwd)",target=/src debian bash
```

8.2. Volúmenes

- Puntos de montaje definidos al crear la imagen
- Suelen ser directorios importantes para la aplicación *containerizada*

```
docker run -dit --name my-apache-app -p 8080:80 -v $HOME:/usr/local/apache2/htdocs/ httpd:2.4
```

  - `-dit` : **i** nteractive, **t** ty, **d** etached
  - `-p 8080:80` : El puerto `8080` de la dirección `0.0.0.0` se conecta a la *ip* del *container*, puerto `80`
  - `-v` : El volumen `/usr/local/apache2/htdocs` será el directorio *home*
  - Resultado: Apache corriendo en el puerto 8080 sirviendo los ficheros del directorio *home*

9. .Entrar.en un *container*

- Se pueden ejecutar comandos en un *container* en ejecución

```
docker exec -it my-apache-app bash
```

  - **-i**: Ejecutar de forma interactiva (redirigir entrada y salida estándar)
  - **-t**: Ejecutar en un TTY (una consola)

10. Usuarios

- Los usuarios en Linux se identifican por un número
  - Docker comparte el *kernel* con el sistema operativo
  - Por tanto, los usuarios de los *containers* son los del Linux real
- Conclusiones
  - Se comparten los identificadores, no los nombres
  - El usuario *root* es el mismo en todos los *containers* y en el Linux real
  - Cuidado con la seguridad!

11. *Docker registry*

- Las imágenes se almacenan en registros
  - El registro por defecto es https://registry.hub.docker.com
  - Los siguientes comandos son equivalentes

```
docker run hello-world
docker run registry.hub.docker.com/hello-world
```

- Oracle tiene un registro para sus imágenes
  - https://container-registry.oracle.com/
  - Se necesita registro (gratis) en Oracle
  - La contraseña del registro no es la de la cuenta de Oracle, sino el *Auth token*

```
docker login container-registry.oracle.com/
```

11.1. *Cache* en el instituto

`10.1.33.201:8090`

- Es un *registry* inseguro (sin https).
- Para poder usarse hay que modificar/crear el fichero `/etc/docker/daemon.json`

```
{
    "insecure-registries":["10.1.33.201:8090"]
}
```

12. Práctica: Instalar webmin

- Es un sistema para manejar servidores Linux mediante con una interfaz web
- Comprueba qué se ha instalado en el *container* y lanza una *shell* desde la web

```
sudo docker run -p 10000:10000 10.1.33.201:8090/johanp/webmin
```

13. Referencias

- Formatos:
  - Transparencias
  - PDF
  - EPUB
- Creado con:
  - Emacs
  - org-re-reveal
  - Latex
- Alojado en Github