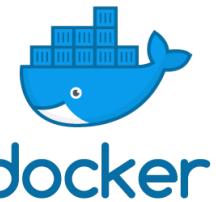




POLITÉCNICA

UNIVERSIDAD
POLITÉCNICA
DE MADRID



Análisis de contenedores Docker

- y sus implicaciones de seguridad

Javier Alonso Silva

Seguridad en Sistemas y Redes

Universidad Politécnica de Madrid

2021



Resumen

TO-DO

Índice

1. Introducción	1
1.1. ¿Qué es Docker?	3
1.2. <i>Real-life usages</i>	7
1.3. <i>Docker rules</i>	10
2. Docker	13
2.1. Estructura de un Docker	13
2.2. Creación de un contenedor	22
2.3. Comunicación entre contenedores	24
2.4. Despliegue de aplicaciones multi-contenedores. docker-compose	24
2.5. “Orquestación” de contenedores	24
2.6. Líneas futuras de desarrollo e innovación	24
3. Seguridad en Docker	24
3.1. Análisis de la pila Docker	25
3.2. Diferencias fundamentales con chroot	25
3.3. Seguridad en las comunicaciones de red – <i>firewall</i>	25
3.4. Seguridad en las comunicaciones inter-contenedores	25
Referencias	25

1. Introducción

La era tecnológica ha avanzado en los últimos años a pasos agigantados, y las demandas del sector han crecido junto a ella. No hace más de 200 años se “descubría” la electricidad; hace 90 años nacía la primera computadora básica capaz de realizar operaciones aritméticas; hace 70 años nacía el transistor que sustituyó las válvulas de vacío (figura 1); y desde entonces, el crecimiento ha sido exponencial [1].



Figura 1: Comparativa de una válvula de vacío (izquierda) frente a un transistor (centro) y un circuito integrado (derecha).

Otro de los ejemplos de tecnologías que han crecido exponencialmente son los dispositivos de almacenamiento, donde no hacía más de 20 años las capacidades máximas se estimaban en torno a los MB (megabytes) y ahora se hablan de EB (exabytes) [2]. Esta evolución es muy representativa también a nivel económico, ya que el coste del almacenamiento ha ido bajando a medida pasaba el tiempo, así como el espacio físico que ocupan los dispositivos (figura 2):

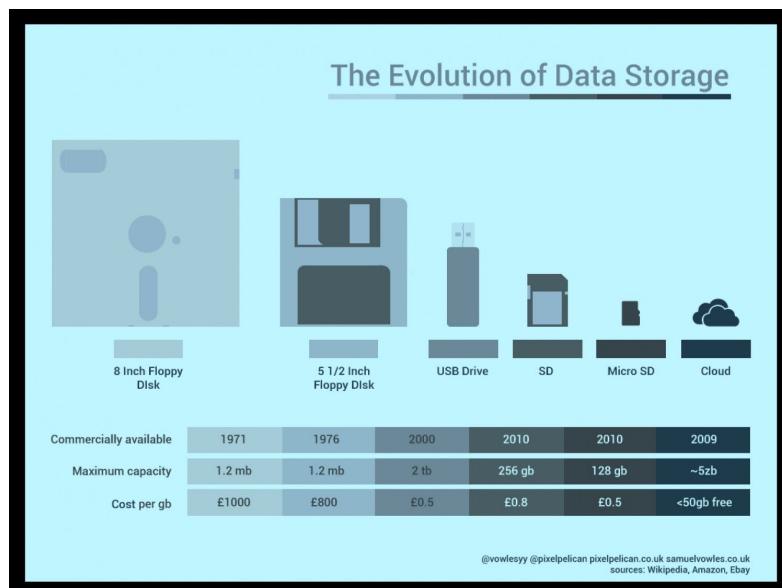


Figura 2: Evolución del espacio de almacenamiento en términos económicos y cuantitativos [3].

Finalmente, el gran salto tecnológico se ha producido con la aparición de Internet y las comunicaciones ya no eran únicamente personales sino entre dispositivos. En relación con el punto anterior, la aparición de Internet ha permitido descentralizar el espacio donde ya el usuario no guarda su información en su equipo personal sino en un clúster de servidores distribuidos a nivel mundial al cual accede, de forma simultánea, desde Internet y desde cualquier dispositivo. Así, lo que comenzó como una red de conexión de unos pocos usuarios ha acabado convirtiéndose en la red global que todos usamos y que conecta más de 4 billones de dispositivos (figura 3).

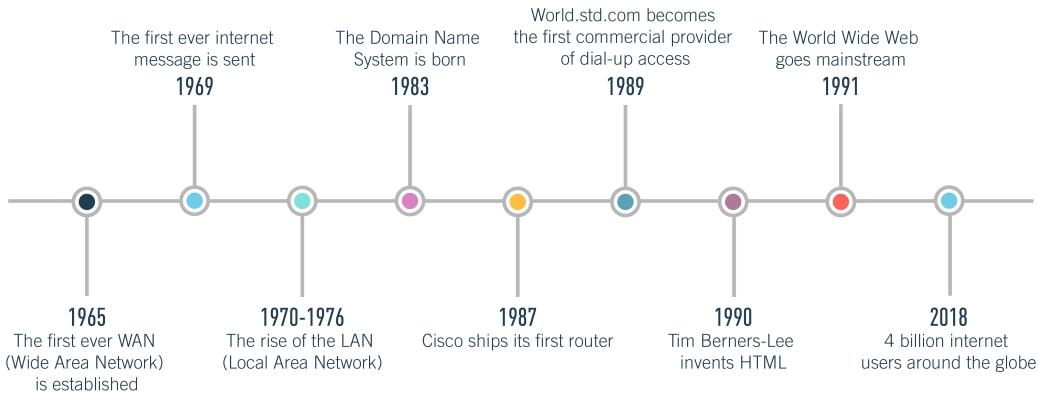


Figura 3: Evolución de Internet a lo largo del tiempo, hasta llegar a hoy [4].

El problema a esto es evidente: con una mayor capacidad de cómputo, con más opciones de comunicación y con más posibilidad de almacenar datos, los requisitos de las aplicaciones van creciendo y creciendo y cada vez son más complejos de satisfacer, no necesariamente a nivel *hardware* (que por lo general suele acompañar) sino a nivel *software*. Como las aplicaciones se orientan a los usuarios es necesario añadir capas de abstracción (como el sistema operativo) para facilitar la labor a la persona. Sin embargo, cada capa nueva que se añade dificulta las tareas de despliegue y mantenimiento dado que existe una gran variedad de combinaciones *hardware* y cada una puede estar con un sistema operativo distinto.

Por otra parte, la extensión de dependencias y posible incompatibilidad entre ellas suele desembocar en el uso de versiones desactualizadas de una librería ya que tendríamos “paquetes rotos”. Esto es tan común que tiene hasta su propio término coloquial “*dependency hell*” [5]. Contar con dependencias obsoletas que ya han cumplido con su ciclo de vida *software* conlleva unas implicaciones de seguridad bastante severas:

- Si un *software* no ha mejorado a lo largo del tiempo, existe una malicia humana que puede aprovecharse de distintos *exploits* existentes y comprometan nuestra aplicación.
- Un *software* no actualizado puede tener implicaciones directas sobre el sistema en que se ejecuta, pudiendo producir fallos en el mismo. Esto se debe principalmente a que el *hardware* sigue mejorando y creciendo y un *software* antiguo puede presentar *bugs* en dispositivos modernos que no presentaría en antiguos.

- Un *software* no actualizado puede comprometer otros elementos del sistema en que se ejecuta. Por ejemplo, una aplicación ‘A’ hace uso de dicho *software* y una aplicación ‘B’ también. Sin embargo, la última aplicación se ha diseñado para trabajar con la última versión del *software* pero la aplicación ‘A’ solo puede funcionar con una versión antigua e insegura. Por consiguiente, pese a que la aplicación ‘B’ funcionaría correctamente el hecho de usar una versión antigua e insegura del *software* compromete directamente al sistema y a la aplicación.

Es por eso que existen alternativas como “*chroot*” y máquinas virtuales para subsanar estos problemas. Sin embargo, en los últimos años ha aparecido una herramienta muy sonada y con gran éxito: Docker y los contenedores.

1.1. ¿Qué es Docker?

Docker es una plataforma abierta diseñada para el desarrollo, despliegue y ejecución de aplicaciones [6]. La idea fundamental que reside detrás de Docker es la de separar la infraestructura de las aplicaciones de manera que se pueda entregar el *software* rápidamente.

Por debajo, Docker ofrece una plataforma que otorga la habilidad de empaquetar y ejecutar las aplicaciones en un entorno aislado llamado “contenedor” (*container*). Entre otras características, un contenedor permite ejecutar una aplicación de forma segura sobre el host en cuestión. La pregunta que surge es, ¿qué es un contenedor?

Contenedores

Un contenedor es una unidad estándar *software* que empaqueta código y todas sus dependencias de manera que la aplicación se ejecuta rápidamente y de forma fiable bajo múltiples entornos de ejecución [7]. Una imagen Docker es un paquete ligero, independiente y ejecutable que incluye absolutamente todo lo necesario para poder ejecutar una aplicación: desde el código en sí hasta el *runtime*, herramientas del sistema, bibliotecas y configuraciones.

Durante la ejecución, una imagen se convierte en un contenedor que se ejecuta sobre la máquina Docker (*Docker Engine*), la cual se encuentra disponible en entornos Linux y Windows.

Al fin y al cabo, los contenedores nos aseguran que una aplicación que hemos desarrollado se va a ejecutar de la misma manera en una máquina u otra. El uso del motor Docker permite ejecutar múltiples contenedores sobre un mismo anfitrión sin añadir demasiada carga en el sistema e indiferentemente de la infraestructura que exista por debajo (figura 4):

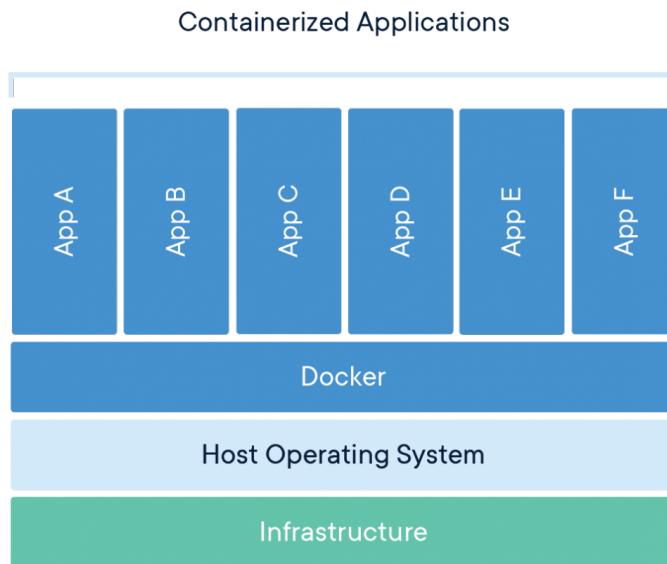


Figura 4: Distribución de los contenedores sobre el motor de ejecución de Docker [7].

La distribución de los contenedores mostrada en la figura 4 puede parecerse mucho a la distribución que tendríamos en una máquina virtual. Sin embargo, hay varias características que lo distinguen principalmente:

1. Un contenedor se ejecuta directamente sobre la máquina anfitriona, mientras que una máquina virtual requiere de un hipervisor.
2. Un contenedor es una abstracción de la capa de aplicación que encapsula el código y las dependencias juntas, mientras que una máquina virtual es una abstracción de una capa física *hardware*.
3. Un contenedor comparte el kernel con el sistema operativo anfitrión, por lo que tiene un gran rendimiento; mientras, una máquina virtual ejecutará su propio kernel sobre el hipervisor del sistema operativo anfitrión.
4. El espacio que necesita un contenedor es muy pequeño en comparación con el de una máquina virtual, que engloba y encapsula un sistema operativo al completo.

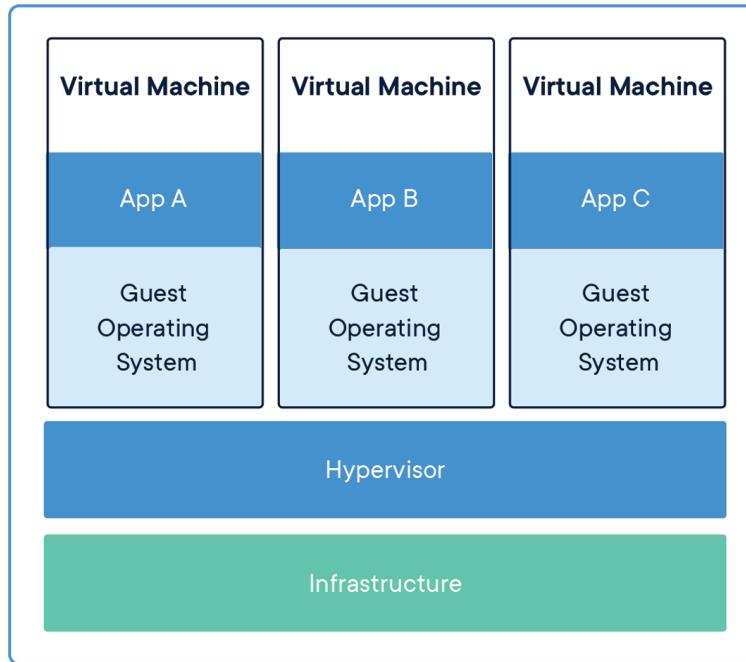


Figura 5: Capas de abstracción de una máquina virtual sobre una máquina anfitriona [7].

En la figura 5 se puede apreciar cómo una máquina virtual añade muchas más capas de abstracción que ralentizan el rendimiento. Sin embargo, esto no quiere decir que sean una mala alternativa: la realidad es que se combinan las dos para obtener una gran flexibilidad para desplegar aplicaciones – contenedores cuando se quiere ejecutar algo directamente sobre el anfitrión; máquinas virtuales para emular *hardware* y que ejecuten en su interior contenedores para ejecutar aplicaciones fácilmente.

La evolución y constante mantenimiento de los contenedores ha generado lo que se conoce como estándar de la industria “*containerd*”. Este estándar define claramente qué arquitectura debe tener un contenedor por debajo y está en constante evolución a medida que la industria crece y madura.

Además, la especificación anterior ha pasado de ser un mero estándar a una aplicación en sí de gestión y orquestación de contenedores, permitiendo que aplicaciones distintas de Docker hagan uso de la arquitectura basada en contenedores aprovechando la OCI: *Open Container Initiative*

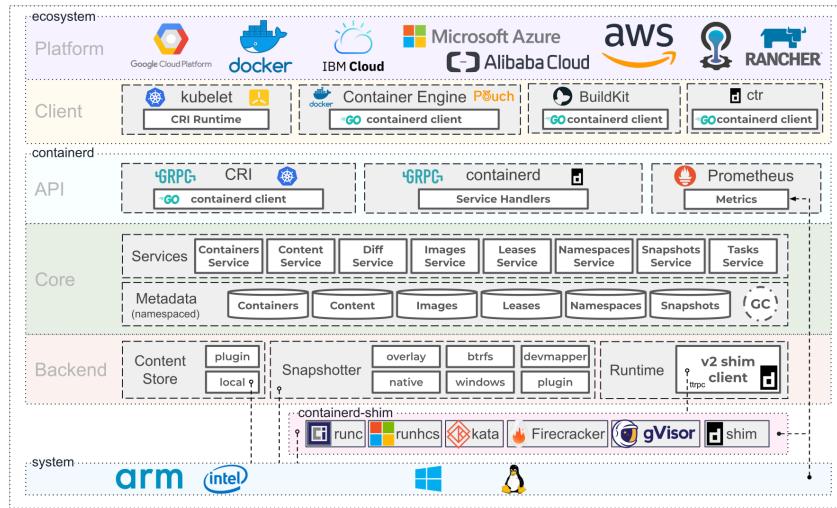


Figura 6: Entorno de ejecución de *containerd* basado en *runC* de la OCI [8].

Docker Engine

El motor de ejecución de Docker establece la arquitectura de ejecución *de facto* que es utilizable desde distintas distribuciones Linux y servidores Windows [9].

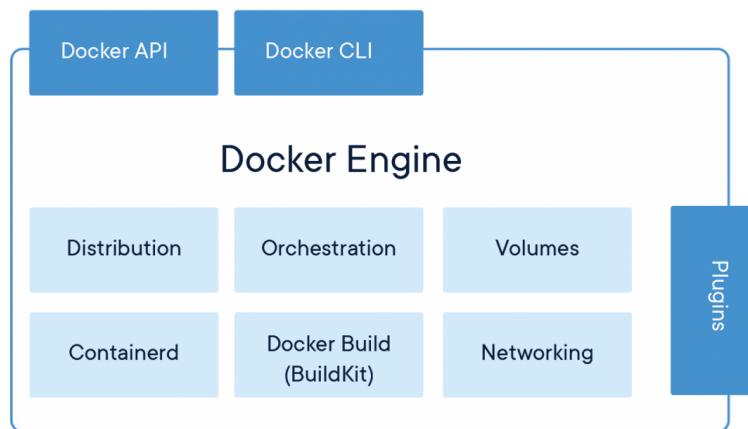


Figura 7: Arquitectura del entorno de ejecución de Docker [9].

El motor de ejecución de Docker se compone de una gran cantidad de elementos que encapsulan de forma uniforme multitud de aptitudes de un sistema operativo o una aplicación (figura 7). Este entorno de ejecución sin embargo es complejo ya que engloba multitud de elementos físicos, como pueden ser las interfaces de red y los volúmenes.

Esto resulta fundamental ya que los contenedores Docker no tienen ni que confiar en la

red del anfitrión: tienen su propio *stack* de red para realizar las comunicaciones que necesiten. Con el motor de ejecución de Docker se busca solventar esos problemas “*dependency hell*” que se han comentado anteriormente y la situación de “en mi equipo funciona”.

De los elementos mostrados en la figura 7, se tiene que son:

- *Distribution*: la distribución Linux en la que se basa el contenedor. Actualmente, Docker solo permite ejecutar contenedores basados en Linux.
- *Orchestration*: cuando hay múltiples contenedores, la orquestación es el proceso por el cual el motor de ejecución de Docker gestiona y maneja qué contenedores se ejecutan, cómo se comunican, cuáles hay que crear nuevos y cuáles eliminar. Es de las partes más complejas que existen en el mundo de los contenedores y ha evolucionado a clústers mucho más completos (y complejos) como Kubernetes o Docker Swarm.
- *Volumes*: los volúmenes (conjuntos de datos) que se manejan en los contenedores. Debido a su arquitectura cerrada, los datos que genera un contenedor solo están visibles para ese contenedor mientras este esté en ejecución. Cuando finalice, todos los datos no persistentes son eliminados.
- *Containerd*: el estándar y cliente de ejecución y manejo de los contenedores a muy bajo nivel.
- *Docker Build (BuildKit)*: herramienta de libre distribución que transforma los ficheros *Dockerfile* en imágenes Docker, listas para ser usadas y distribuidas.
- *Networking*: *stack* de red completo que se pone a disposición de cada contenedor Docker. Cada aplicación puede crear su propio dispositivo de red que cumpla con los requisitos que necesita. Existen varios tipos de adaptadores: *bridge*, *NAT* y *host*. El primero se emplea para realizar comunicaciones a través de red entre distintos contenedores; el segundo para realizar comunicaciones con el exterior mediante una conexión de red completamente independiente a la del anfitrión; la tercera para compartir la interfaz de red del anfitrión con el contenedor, como si fuese una aplicación interna.

Con todo lo anterior, una aplicación puede ejecutarse muy fácilmente en cualquier equipo que integre el motor de ejecución de Docker.

1.2. *Real-life usages*

Desde que nació en 2013, Docker ha ido creciendo y con ello las aplicaciones directas que ha encontrado en el mercado.

Sandboxing

Una de las principales ventajas que otorgó Docker desde su nacimiento fue el de aislar las aplicaciones entre sí y, por consiguiente, ofrecer un entorno de “caja de arena” (*sandbox*) en donde ejecutar nuestras aplicaciones (o aplicaciones inseguras) con cierta confianza [10].

Es cierto que esta característica ya estaba asentada con las máquinas virtuales, y funcionaba correctamente y de forma efectiva. Sin embargo, el tiempo de despliegue y lentitud de una máquina virtual hacía que usarlas para este propósito fuese costoso y no resultase interesante.

Con los contenedores se puede tener un entorno aislado que funciona igual de rápido que una aplicación nativa con unos tiempos de despliegue y uso de recursos limitado. Como se ha visto anteriormente, el motor de ejecución de Docker tiene el control sobre un montón de componentes virtuales y reales que permiten, entre otros, limitar y restringir el acceso a los recursos *hardware* del dispositivo. Bajo esta premisa, un contenedor puede usar solo cierta cantidad de CPU, RAM o red y que cambie en tiempo de ejecución.

Portabilidad

Otra de las características fundamentales de los contenedores es la capacidad de encapsular un *software* y todas sus dependencias. Esto convierte a los contenedores en una gran solución portable: sabemos que si una aplicación funciona en Docker en un equipo Linux, funcionará en Docker de otro equipo Linux exactamente igual, sin necesidad de realizar ningún cambio e indiferentemente de la distribución.

Con la llegada de WSL2, el kernel de Linux se introdujo al completo dentro de las máquinas Windows 10, permitiendo que Docker se pudiera ejecutar de “forma nativa”[11]. Con esto, la limitación anterior se elimina y los contenedores diseñados para Linux funcionarán también en Windows.

Esto ha tenido una repercusión directa con el auge de los sistemas basados en la nube, los cuales a veces resultaban complejos y tediosos. Con los contenedores, una aplicación que un desarrollador ejecuta *on-premise* en su equipo puede ser fácilmente desplegada a un entorno *cloud* sin necesidad de preocuparse si cumple los requisitos o instala las dependencias. La única restricción es que el entorno *cloud* al que se mueva soporte Docker.

Arquitectura de composición

Una gran mayoría de aplicaciones que se ejecutan actualmente están ejecutándose sobre una pila de aplicaciones: servidor web, base de datos, caché en memoria, gestión de logs, etc. La pregunta es, ¿qué sucedería si se encapsula cada una de esas aplicaciones en un contenedor?

Así nace la arquitectura de microservicios, tan popular y estandarizada hoy en día. Un microservicio define un elemento único de una aplicación (que puede ser usado entre 1...n veces) el cual acelera y facilita las labores de desarrollo de una aplicación. Entre otras ventajas, un microservicio puede ser actualizado, reemplazado, eliminado o modificado sin afectar al resto de microservicios que componen una aplicación. Esta alternativa se ha asentado como la solución ideal a las aplicaciones monolíticas monstruosas, que lo engloban todo (como XAMPP) ya que han demostrado ser mucho más fáciles de mantener y desarrollar.

Escalado y orquestación

Aprovechando la arquitectura de microservicios y contenedores, existen técnicas de escalado y orquestación automáticas basadas en Docker y contenedores.

De esta manera, en picos de conexión se despliegan automáticamente más contenedores que gestionan entre ellos las peticiones entrantes y salientes. Cuando las solicitudes bajan, los contenedores en desuso desaparecen para dejar de usar recursos.

Entre las herramientas más sonadas para la gestión de contenedores está Kubernetes, desarrollado por Google. La idea de orquestación nace a raíz de esta empresa que empieza a invertir cantidades millonarias de dinero en contenedores porque le ve un nuevo potencial: las comunicaciones vía Internet de los contenedores. Hasta ahora solo hemos visto un modelo de arquitectura: un cliente Docker que ejecuta uno o varios contenedores. Sin embargo, con la aparición de los microservicios y la orquestación, y dadas las características de red de los contenedores, se abre la posibilidad de que múltiples clientes Docker en máquinas físicamente distintas puedan estar ejecutándose de forma simultánea y compartiendo datos entre ellos fácilmente.

Debido a las capas de aislamiento de Docker, esta comunicación no es sencilla: no sirve con comunicar dos direcciones IP. Sin embargo, utilizando un motor de Docker distribuído se pueden realizar las conexiones como si de una LAN se tratase, cuando en realidad se está usando una red *overlay*. Esto se muestra en la figura 8:

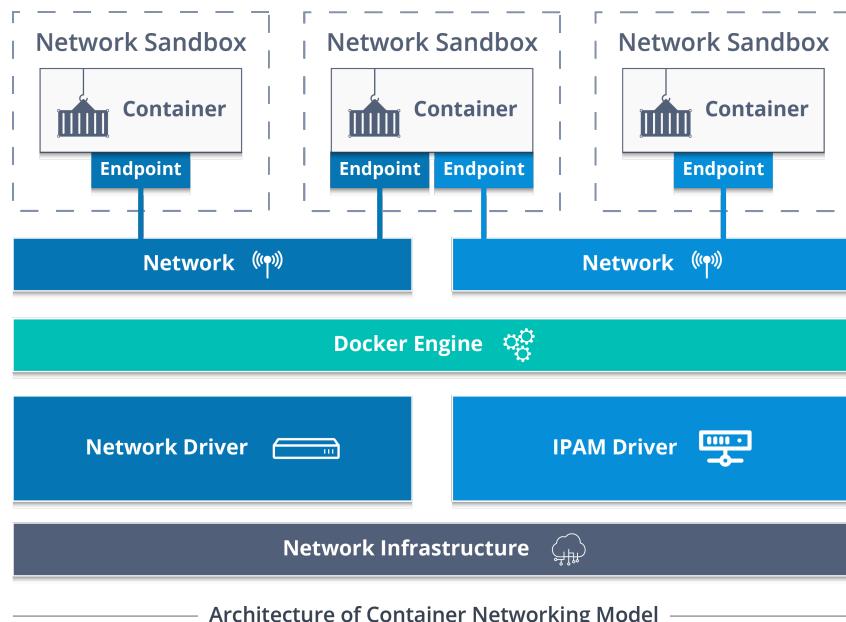


Figura 8: Comunicación entre contenedores usando el motor de Docker [12].

Con todas estas ideas en mente, es evidente que Docker ofrece soluciones fáciles y sencillas para escalar automáticamente aplicaciones alrededor de un clúster de nodos distribuído por el mundo.

Muchas de las aplicaciones de Docker surgen en el mundo DevOps, en donde la mayoría de herramientas de integración continua (CI) y despliegue continuo (CD) han migrado sus infraestructuras hacia Docker. Con esto se consigue que los tests y las compilaciones se hagan de forma sencilla con contenedores de un solo uso.

Otra aplicación directa son las arquitecturas *cloud*, en donde antes había que configurar cientos de parámetros para desplegar una aplicación web basada en PHP y MySQL y ahora

basta con usar uno o varios contenedores que agrupen las funcionalidades que necesitamos.

Por otra parte, gracias a los contenedores los tiempos de desarrollo se han agilizado mucho. Antes, por ejemplo, una aplicación requería de compilar ciertos paquetes y realizar ciertas instalaciones que llevaban mucho tiempo. Con Docker, se exponen las librerías necesarias y se trabaja directamente con aquello que se necesita, sin necesidad de dedicar tiempo a esas tareas.

1.3. Docker rules

Desde su nacimiento en 2013 hasta su expansión mundial hace poco más de 4 años, en 2017/18, los contenedores se han convertido en el *modus operandi* de muchas empresas, que han visto en la tecnología de contenedores una gran ventaja y forma de despegar y aumentar su producción.

Desde entonces, diversos estudios como el llevado a cabo por Portworx cada año brindan la oportunidad de ver qué tecnologías dominan el mercado y cómo va evolucionando el mundo de los contenedores.

De entre los datos obtenidos, es destacable la adopción de contenedores en las empresas tecnológicas: un 87 % de los encuestados (2019) afirman usar contenedores en comparación con el 55 % registrado en 2017. Es más, el 90 % de las aplicaciones que ejecutan en esos contenedores están en entornos de producción, una gran diferencia con 2018 (84 %) y 2017 (67 %) [13].

Estos datos radican en la inversión económica que las empresas realizan en labores de “contenerización”, invirtiendo entre \$500 000 y \$1 000 000 [13]. De entre todos los motivos que mueven a las empresas a realizar esas inversiones, prima la seguridad de los datos sobre los demás.

Parece ser que una de las principales labores de los contenedores en estas decisiones es la de proteger la información (61 %), gestionar las vulnerabilidades fácilmente (43 %) y proteger el sistema en tiempo de ejecución (34 %). Estos datos van directamente ligados con las medidas de seguridad que las compañías adoptan al usar contenedores:

- Cifrar los datos (64 %).
- Monitorización en tiempo de ejecución (49 %).
- Escaneo de vulnerabilidades en los registros de contenedores (49 %).
- Escaneo de vulnerabilidades en las operaciones de CI/CD (49 %).
- Bloquear anomalías mediante la protección en tiempo de ejecución (48 %).

El siguiente motivo de la gran adopción de contenedores es que agiliza mucho la velocidad en el desarrollo y la eficiencia. Por otra parte, la portabilidad de los contenedores permite a las empresas poder mover sus entornos de producción y desarrollo entre una y otra plataforma de nube públicas, de entre las cuales las más usadas (12 % de la muestra) son AWS, Azure y Google Cloud [13].

En particular, se observa cómo AWS (la plataforma de Amazon) es la dominante en este sector, llevándose el 78 % del sector; la siguiente, Azure con el 39 %; y finalmente, GCP (*Google Cloud Platform*) con el 35 % y subiendo rápidamente [14]. Destaca el crecimiento de Google ya que es quien empezó a invertir mucho dinero en contenedores desde su nacimiento y el creador de Kubernetes, la tecnología de orquestación más usada a nivel mundial.

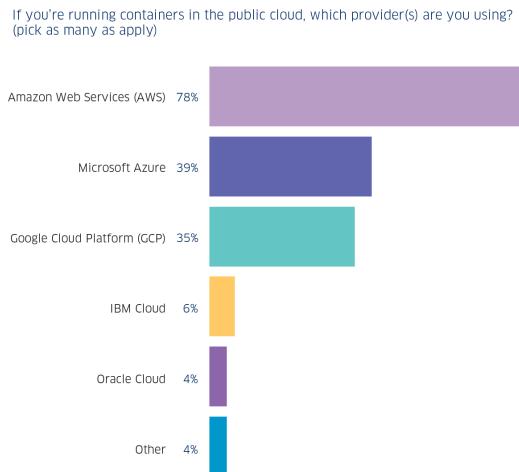


Figura 9: Uso de contenedores según la plataforma *cloud* [14].

La situación mencionada anteriormente se ve directamente reflejada en la “contenerización” de aplicaciones en según que plataforma. De los usuarios de Azure, solo el 20 % ha creado un contenedor para más de la mitad de sus aplicaciones, significativamente más bajo que el 33 % de los no usuarios. Esto se ve drásticamente reducido cuando se hablan de aplicaciones en entorno de producción [14].

Por el contrario, casi un tercio de los usuarios de GCP (31 %) han creado un contenedor para más de la mitad de sus aplicaciones, relativamente superior al 27 % de los no usuarios. Este mismo efecto se produce con respecto a las aplicaciones en producción desplegadas en GCP [14].

Esto se ve reflejado en el gráfico de la figura 10:

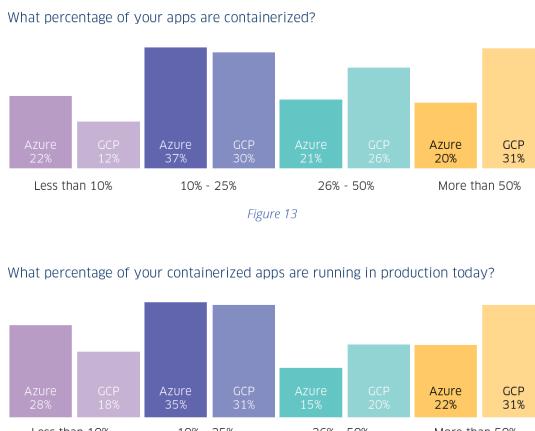


Figura 10: Porcentaje de las aplicaciones desplegadas en contenedores en según qué plataformas [14].

En un estudio más moderno, se estima en el año 2020 ha supuesto un mayor auge en las tecnologías de “contenerización”, en donde los responsables de IT han priorizado la creación de contenedores para aplicaciones ya existentes, migrar toda la infraestructura a la nube y hacer un mejor uso de las plataformas en la nube. De entre todos los problemas, el principal es cumplir con los requisitos legales, de rendimiento y regulatorios vigentes según las necesidades de la industria; y la portabilidad de las aplicaciones, las cuales estaban confinadas y diseñadas para sistemas en particular y ahora se quieren desplegar en la nube en general [15].

Esto se ve en la infografía diseñada por Forrester (figura 11):

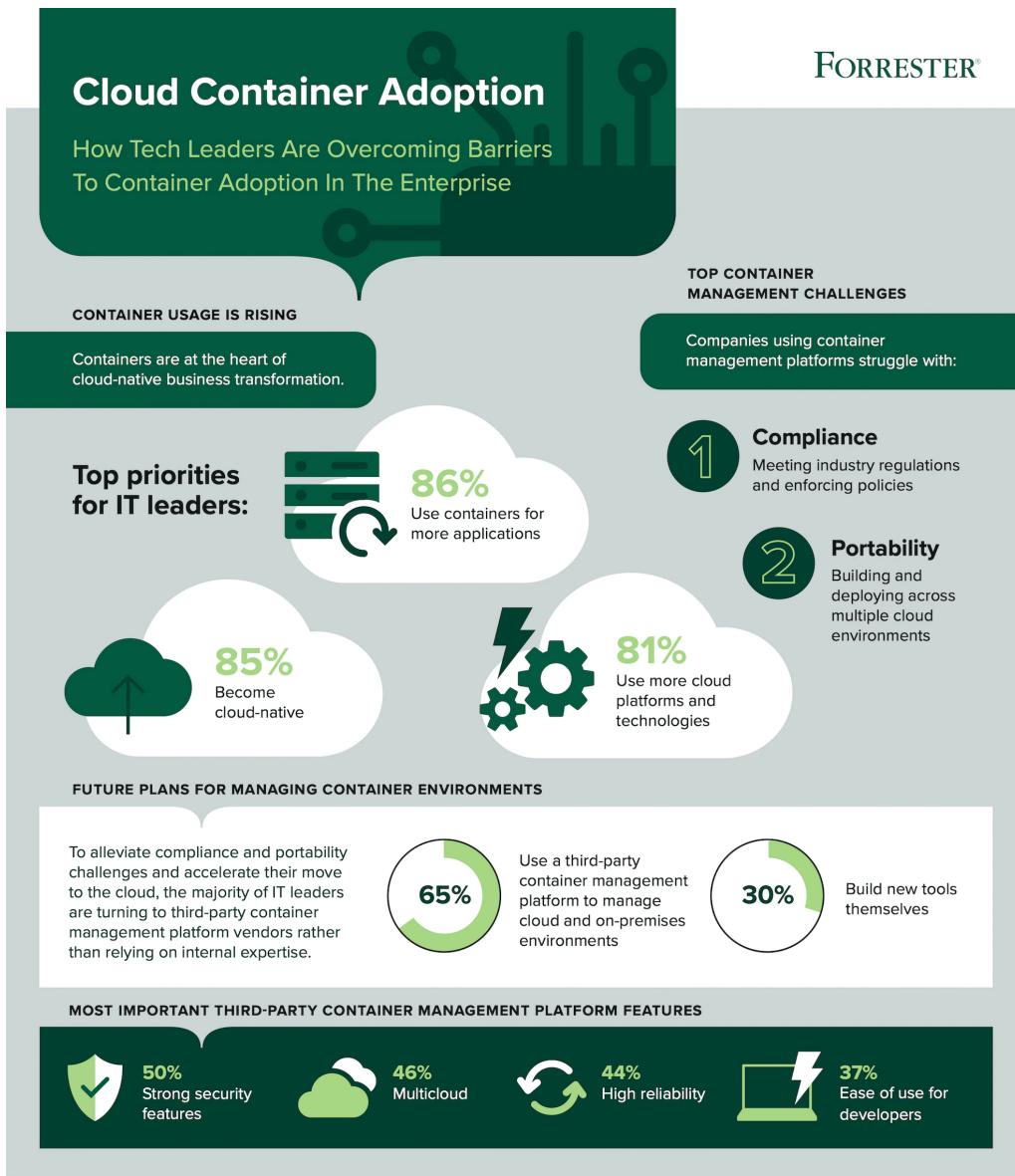


Figura 11: Estadísticas de adopción de tecnologías basadas en contenedores en la nube, 2020 [15].

De entre todos los datos anteriores, es destacable el gran uso de Docker y Kubernetes para gestionar toda esta infraestructura. En 2017, Docker representaba un 99 % de los contenedores en uso. Sin embargo, con la compra de CoreOS por RedHat y el lanzamiento de la OCI ha promovido el nacimiento y establecimiento de nuevas tecnologías de contenedores que le han quitado cuota de mercado a Docker [16]. Actualmente, la distribución queda (figura 12):



Figura 12: Usos de tecnologías de contenedores: Docker domina, seguido por rkt y Mesos [16].

Todo esto nos lleva a ver que si bien aparecen alternativas nuevas Docker sigue siendo la tecnología dominante y la que más adopción está teniendo. Esta competitividad es muy buena ya que permite a Docker y a otras tecnologías de contenedores, como rtk de RedHat (CoreOS), evolucionar, seguir avanzando y mejorando. Lo interesante no es ya usar Docker, rtk o LXC sino que se ha establecido un estándar de contenedores abierto (OCI) y que pone las bases a lo que es una tecnología revolucionaria.

2. Docker

Ahora que ya se han introducido los contenedores, las tecnologías de virtualización y tendencias de uso, se va a explicar cómo funciona Docker en profundidad. Por una parte, se va a ver cómo es la estructura de un contenedor Docker, cómo se comunica con el kernel de Linux, cómo se aísla del resto del sistema y cómo funciona a nivel de discos virtuales, interfaces de red y gestión de recursos.

Por otra parte, se comentarán diversos ejemplos y estructuras básicas que permiten la creación de un contenedor aislado, la comunicación de varios contenedores y el despliegue de una aplicación basada en múltiples contenedores funcionando simultáneamente.

Finalmente, se comentarán tecnologías de orquestación de contenedores, como son los clústers de Kubernetes y Docker Swarm y qué planes hay previstos de cara al desarrollo e innovación de Docker como cliente y gestor de contenedores, para dar pie a un análisis de la seguridad real de los contenedores, en el punto 3.

2.1. Estructura de un Docker

Docker ofrece un mecanismo de comunicación con un entorno aislado llamado contenedor, que ha sido introducido anteriormente. Los contenedores por defecto están aislados, son seguros y empaquetan todo lo necesario para funcionar, por lo que no necesitan nada del sistema que está por debajo.

Internamente, Docker utiliza la arquitectura “cliente–servidor” para gestionar tanto las comunicaciones y contenedores. Por una parte, el cliente de Docker se comunica con el *daemon*,

el cual es el encargado de realizar las tareas pesadas: construir (*build*), levantar (*run*) y distribuir (*distribute*) los contenedores Docker.

Lo interesante del servicio en ejecución de Docker es que puede funcionar o bien en la misma máquina que el cliente o bien sobre otra máquina diferente. Esto es gracias a que la comunicación del cliente con el servicio se realiza mediante *sockets* de UNIX, que proveen de una alta velocidad; o bien mediante interfaces de red, haciendo uso de la API REST de Docker.

La arquitectura Docker

Toda la arquitectura de Docker se puede resumir en la siguiente figura (figura 13):

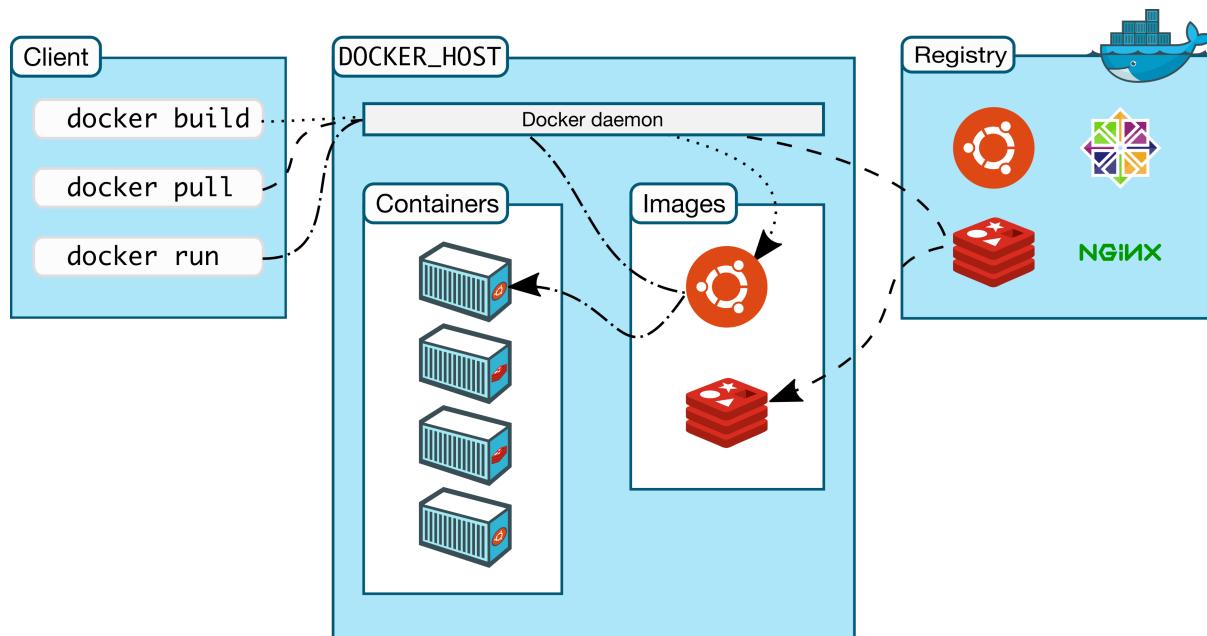


Figura 13: Arquitectura cliente–servidor de Docker [6].

De la imagen anterior destacan tres bloques principales: el cliente, el servidor (*docker host*) y el registro (*registry*). Por una parte, el cliente es la principal forma de comunicarse con el servicio de Docker. Ejecutando comandos como `docker run` se envían al servicio peticiones mediante la API REST interna que gestionan los contenedores.

Por su lado, el servicio está gestionado por el *Docker daemon*, llamado `dockerd`. Dicho servicio escucha de forma activa las peticiones API entrantes y gestiona los objetos de Docker, como las imágenes, contenedores, interfaces de red y volúmenes. Además, un servicio puede comunicarse con otros servicios para gestionar a su vez otros contenedores.

Finalmente, los registros de Docker (no confundir con los *logs*, que también se traduce como “registro”) son un repositorio en donde se almacenan imágenes Docker. Por defecto, se hace uso de Docker Hub, que es el registro principal y al cual el servicio de Docker solicita imágenes cuando no las encuentra, y en donde cualquier usuario puede publicar la imagen que quiera. Pero, además, una persona puede hospedar su propio registro privado (al igual que si se desplegase un servidor Nexus).

Uno de los conceptos fundamentales que se han mencionado anteriormente son los “objetos

Docker". Esa nomenclatura se usa para agrupar y mencionar a todo aquello que se crea y genera cuando se trabaja con el servicio de Docker: imágenes, contenedores, interfaces de red, *plugins*, volúmenes y demás.

Imágenes

Una imagen conforma una plantilla de solo lectura la cual contiene instrucciones para crear un contenedor Docker. Por lo general, las imágenes se basan en otras ya existentes con configuraciones adicionales.

Un caso habitual es una imagen basada en `ubuntu-server` sobre la cual se instala un servidor Apache y la aplicación NodeJS que hemos desarrollado. Con esto, tendríamos una imagen la cual se basa en Ubuntu, que ejecuta un servidor Apache y que tiene una aplicación NodeJS, junto con los ajustes pertinentes para un correcto funcionamiento, definiendo así una imagen nueva (figura 14):

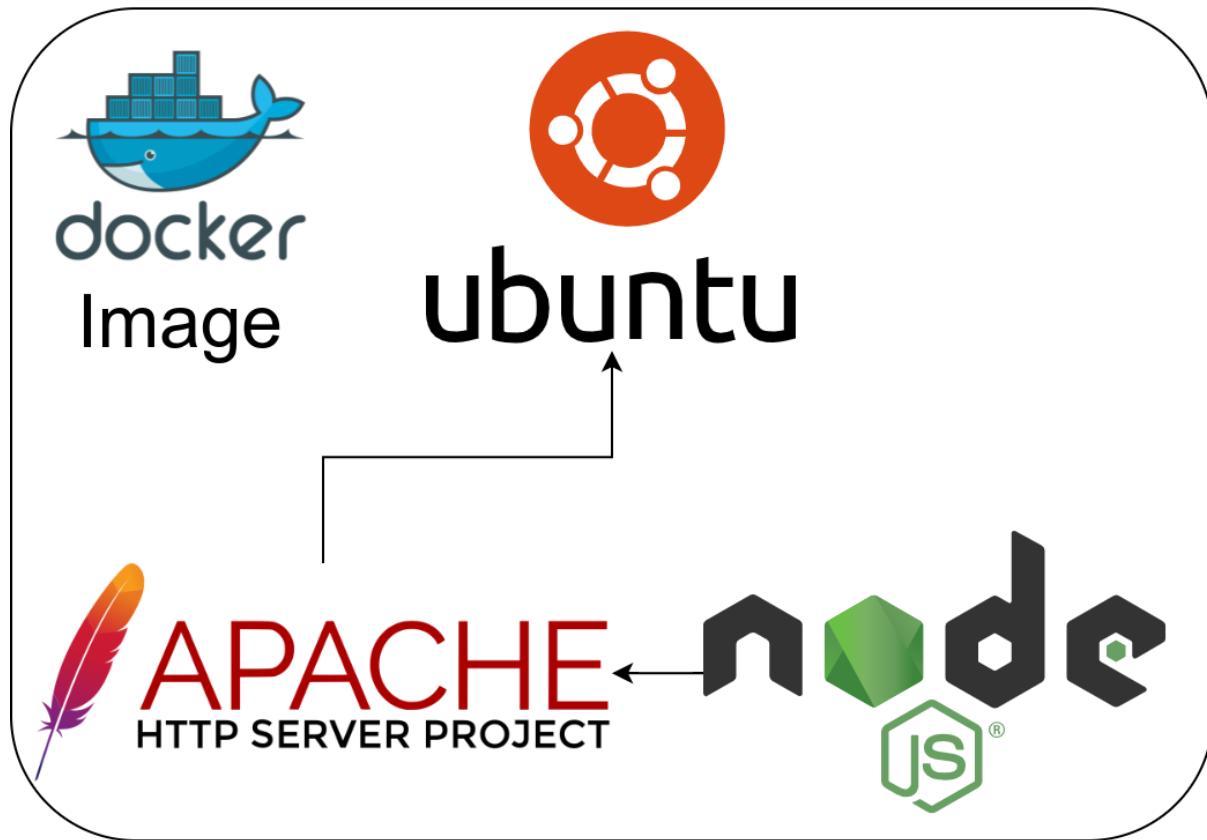


Figura 14: La nueva imagen que habríamos definido basándose en las premisas anteriores.

Cuando se quiere crear una nueva imagen se utiliza un fichero `Dockerfile` el cual incluye las directivas necesarias para construir una imagen desde cero (o basándose en una ya existente). Además, el funcionamiento de este tipo de ficheros es muy similar a los `Makefile` en tanto que, cuando se realiza algún cambio sobre el mismo, solo se reconstruyen en aquellas imágenes que hayan cambiado las capas modificadas. Esto se traduce en imágenes mucho más pequeñas, ligeras y rápidas en comparación, por ejemplo, a las máquinas virtuales.

Contenedores

Un contenedor es una instancia de una imagen que puede ser ejecutada. Las operaciones básicas sobre contenedores son: crear, iniciar, parar, mover o eliminar. Además, se pueden conectar una o varias redes, volúmenes de datos o inclusive definir y crear una nueva imagen a partir del estado actual.

Por defecto, un contenedor está bastante bien aislado del resto de contenedores en la máquina anfitriona. Sin embargo, se puede definir y controlar cómo de aislada está una red, un almacenamiento o los subsistemas que están por debajo.

Es fundamental tener en cuenta que un contenedor está directamente definido por la imagen que lo crea y por las configuraciones iniciales que se le dan en el momento de la creación. Sin embargo, todos los cambios efectuados durante su ciclo de vida que no sean de imagen o de configuración desaparecerán una vez el contenedor se detenga y se elimine (esto incluye todo el sistema de ficheros que hay por debajo).

Almacenamiento

Dada la situación anterior, es necesario buscar alguna manera de persistir la información de los contenedores. Por defecto, los datos que se generan y gestionan en un contenedor de Docker son directamente gestionados por el servicio de Docker y se trabaja con ellos sobre una capa escribible asociada al contenedor [17]. Esto se traduce en:

- Los datos no son persistentes, por lo que eliminar el contenedor eliminará la información.
- La capa escribible de un contenedor está asociada a dicho contenedor, por lo que resulta complejo para otros procesos extraer información de ella.
- Además, dicha capa está directamente asociada a la máquina anfitriona en donde el contenedor está ejecutándose, por lo que es muy complejo mover los datos de un sitio a otro.
- Realizar escrituras sobre la capa escribible de un contenedor necesita de un driver que gestione el sistema de ficheros. Usando el kernel de Linux, este driver ofrece una sistema de ficheros UnionFS, configurado a partir de la unión de varios sistemas de ficheros [18]. Esto conlleva una penalización en rendimiento en comparación con el uso de volúmenes de datos, que trabajan directamente sobre el sistema de ficheros del anfitrión.

Por defecto, existen dos formas de persistir los datos de un contenedor: mediante el uso de volúmenes o mediante *bind mounts*, es decir, asociar un directorio en el host con un directorio en el contenedor.

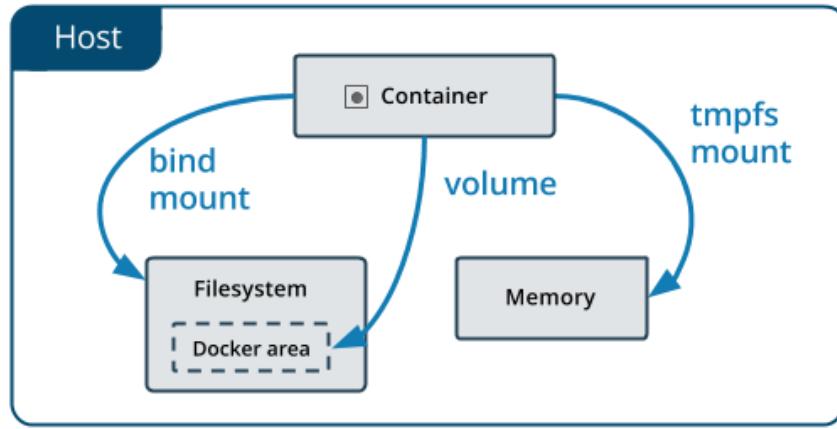


Figura 15: Posibles ubicaciones en donde se almacena la información en contenedores Docker [17].

— Volúmenes

Los volúmenes ofrecen un almacenamiento persistente completamente gestionado por Docker, por lo que hay que crearlos de forma explícita con “`docker volume create`”.

Cuando se crea un volumen, los datos se alojan directamente en la máquina anfitriona. Si se asocia a un contenedor, el volumen monta como un directorio dentro del mismo, mostrando un funcionamiento similar a *bind mounts*. La principal diferencia es que los volúmenes ofrecen un entorno completamente aislado de almacenamiento, gestionado por Docker y portable.

Aprovechando lo anterior, es posible montar un volumen en varios contenedores abriendo la posibilidad de que compartan datos entre ellos. Además, los volúmenes son independientes de los contenedores que los usan: si ningún contenedor usa un volumen, este sigue existiendo hasta que se elimine manualmente (“`docker volume prune`”).

Por otra parte, como los volúmenes son gestionados por Docker permite disponer de *volume drivers* para almacenar datos en equipos remotos.

Para resumir, se indican las características principales de los volúmenes [19]:

- Son fáciles de manejar, hacer copias de seguridad y de migrar a otros servidores.
- Se pueden gestionar completamente desde la interfaz de línea de comandos de Docker.
- Funcionan tanto en Windows como en Linux.
- Están diseñados para que puedan ser compartidos por varios contenedores de forma segura.
- Se pueden almacenar los datos en equipos remotos o proveedores de servicios en la nube.
- El rendimiento en plataformas paganas (MacOS y Windows) es mejor que con *bind mounts*.
- No incrementan el tamaño del contenedor sino del volumen en sí.

Los volúmenes se almacenan en el área de Docker, aislados del sistema dentro del sistema (figura 16):

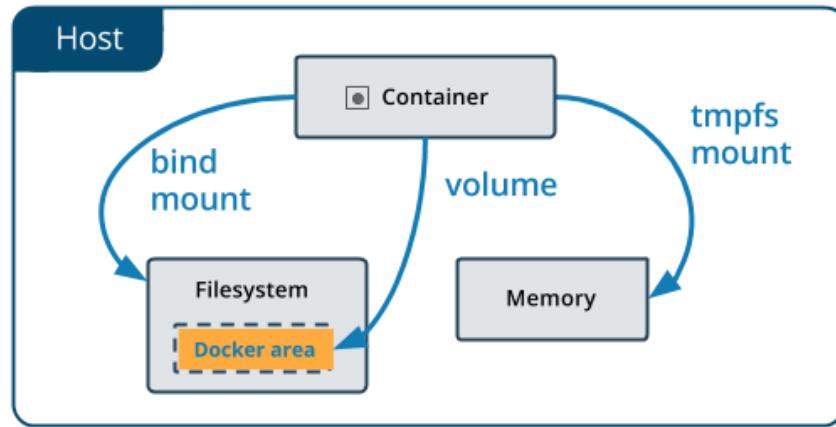


Figura 16: Ubicación del almacenamiento de los volúmenes en Docker [19].

– **Bind mounts**

Los montajes de sistema de ficheros dentro de los contenedores llevan existiendo desde el lanzamiento inicial de Docker. Su funcionamiento es simple: utilizando los mecanismos de los sistemas operativos anfitriones, un directorio (o fichero) en el equipo anfitrión se monta dentro del contenedor en una ruta en específico. Si el fichero o directorio no existe, se crea bajo demanda en el momento de la creación del contenedor.

Es importante tener en cuenta que este tipo de sistema de ficheros está mucho más limitado que un volumen y pueden suponer un gran fallo de seguridad en tanto a que es posible acceder a ficheros sensibles del sistema.

Hay que tener en cuenta que los contenedores Docker siempre se ejecutan como super usuario (administrador), por lo que un proceso malicioso podría editar, modificar, leer y eliminar ficheros fundamentales del sistema anfitrión si no se ha tenido cuidado con el directorio a montar.

Sin embargo, es una opción muy interesante para almacenar datos que son modificados con cierta regularidad o que no interesa “persistirlos”. Por ejemplo, ficheros de configuración (para cambiarla bajo demanda), directorios que contengan logs, etc.

Los *bind mounts* se almacenan en el sistema de ficheros anfitrión (figura 17):

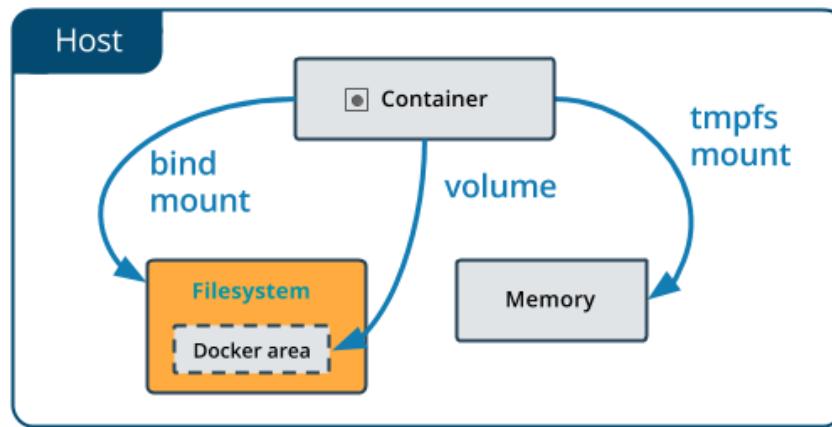


Figura 17: Ubicación del almacenamiento de los *bind mounts* en Docker [20].

– *¿Cuándo usar volúmenes o bind mounts?*

Basándose en la documentación oficial de Docker [17], hay unos casos para unos o para otros, según se requiera (tabla 1):

	Compartir datos entre contenedores	Gestionar ajustes	Estructura del FS	Copias de seguridad	Datos en la nube	Alto rendimiento	Versiones del código fuente
Volúmenes	✓	✗	✓	✓	✓(nativo)	✓(en Docker Desktop)	✗
Bind mounts	✗	✓	✗	✗	✓(usando un sistema de ficheros en la nube, como SAMBA)	✓(depende del sistema de ficheros del anfitrión)	✓

Cuadro 1: Cuándo usar un tipo de almacenamiento persistente u otro, de elaboración propia basándose en la documentación [17].

Interfaces de red

Docker ofrece un potente mecanismo de gestión de redes para permitir la comunicación entre contenedores y con elementos externos. Una de las motivaciones principales detrás de la gestión propia de la red por parte de Docker es la de que las aplicaciones no sepan si están dentro de un contenedor o si tienen que comunicarse con el exterior o con una carga de trabajo externa a Docker, sino que van a comunicarse directamente sin necesidad de ninguna configuración externa.

Indiferentemente de si el servicio se está ejecutando en una máquina Linux y otro en una máquina Windows, la comunicación entre ellas se va a realizar completamente independiente a la plataforma.

La gestión de las redes y aislamiento de las mismas se realiza mediante una manipulación directa de *iptables*. Esto se hace así porque el *firewall* nativo de Linux tiene una grandísima potencia, es muy configurable y se ejecuta directamente a nivel de kernel, lo cual reduce el *overhead* que pudiera presentar si fuese una aplicación a nivel de usuario.

Esto conlleva que las rutas del *firewall* que se hubiesen creado previamente deben aparecer antes de las creadas por Docker (para que tengan mayor peso) y permiten llevar la ejecución de contenedores Docker a distintos tipos de *hardware*: servidores, routers (en donde Docker actúa como router) y equipos embebidos.

Por defecto, Docker expone los siguientes drivers [21]:

- **bridge**: el driver que se usa por defecto, si no se especifica ninguno. Se destina este tipo de driver cuando las aplicaciones se ejecutan de forma aislada y solo necesitan comunicarse con el exterior o, si por el contrario, hace falta que múltiples contenedores se comuniquen entre sí.
- **host**: elimina el aislamiento de red con el sistema anfitrión, usando la interfaz del sistema (por lo que se debe ajustar el *firewall* y la red, si necesita alguna característica especial).
- **overlay**: interconecta múltiples servicios de Docker (que pueden estar en máquinas distintas) para facilitar la comunicación entre clústers de Docker Swarm o contenedores entre sí.
- **macvlan**: asigna una dirección MAC al contenedor de forma que parezca que es una máquina física, por lo que se realiza el enrutamiento según las direcciones MAC.
- **none**: deshabilita todas las comunicaciones de red para el contenedor, se suele usar conjunto a un driver personalizado.
- **Network plugins**: cada persona puede desarrollar su propio driver de red para que cumpla con una función específica.

Interfaz a bajo nivel

Docker, para funcionar, necesita del kernel de Linux por debajo. ¿Por qué esta caracterización? Todo se debe a medidas de seguridad.

Por lo general, un contenedor de Docker se asemeja mucho a los contenedores LXC de Linux nativos, incluyendo entre otros características de seguridad. Si observamos los requisitos de la interfaz Docker (figura 18) vemos que inclusive hace uso de la librería de LXC:

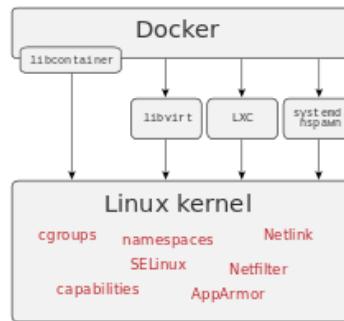


Figura 18: Interfaz de Docker con respecto al kernel de Linux. Fuente: Wikipedia [22].

El principal mecanismo de aislamiento son los *Linux kernel namespaces*, consistentes en una “venda en los ojos” hacia los procesos que se ejecutan dentro de un contenedor.

Lo siguiente que entra en juego son los *control groups* (*cgroups*), necesarios para limitar el acceso a los recursos del sistema.

Todas estas capas se analizarán en mayor profundidad más adelante, en el punto 3.

2.2. Creación de un contenedor

La creación de un contenedor siempre se realiza de la misma manera: mediante un fichero *Dockerfile*. Los *Dockerfile* son ficheros del estilo de los *Makefile* que contienen unas reglas básicas que definen lo que será una imagen de un contenedor.

El comando que crea una imagen es `docker build`, el cual toma las instrucciones que aparecen en el fichero y las va ejecutando una a una hasta que se produce un error o finaliza correctamente.

Un fichero *Dockerfile* cuenta con multitud de directivas que permiten personalizar y configurar cómo va a funcionar [23]. Aquí se van a introducir algunas de las más importantes (o las más usadas) [24]:

- **FROM:** define una imagen base de partida sobre la que construir.
- **ADD:** copia ficheros y directorios dentro de la imagen del contenedor. Además, acepta URLs como parámetro y las descarga directamente dentro.
- **RUN:** añade capas a la imagen base, instalando aplicaciones, librerías y componentes.
- **CMD:** especifica qué comandos se deben ejecutar al iniciarse el contenedor. Es importante tener en cuenta que solo puede existir una instrucción CMD en el fichero *Dockerfile* (si no, se usa solo el último que aparezca). Su funcionalidad principal es la de establecer los valores por defecto de un contenedor en ejecución.

- ENTRYPPOINT: es la instrucción “principal” de un Dockerfile. Especifica el punto de entrada de un contenedor que se quiere que funcione como un ejecutable. Por ejemplo, el siguiente comando “`docker run -it --rm -p 80:80 nginx`” ejecuta un servidor NGINX de forma interactiva, publica el puerto 80 y, cuando finaliza su ejecución, se elimina.
- ENV: define las variables del entorno del contenedor que se usarán en tiempo de ejecución.
- COPY: con una funcionalidad similar a ADD pero con más limitaciones.
- EXPOSE: define en qué puertos la aplicación estará escuchando.
- USER: especifica el UID (o el nombre del usuario) que se usará internamente en el contenedor para ejecutar las aplicaciones.
- VOLUME: define volúmenes de datos a crear o un punto de montaje del contenedor en tiempo de ejecución.
- WORKDIR: especifica la ubicación en donde se ejecutará el comando en tiempo de ejecución.
- LABEL: especifica etiquetas del contenedor en forma de metadatos. Se conforman de parejas clave–valor que especifican información relativa a la imagen dentro del contenedor como, por ejemplo, la versión, el nombre del paquete, etc.

Por lo general, un Dockerfile comienza con la especificación de una imagen de partida (ya que no es habitual crear una imagen desde cero) y, a continuación, se procede a instalar diversos paquetes y capas que puedan ser necesarias para nuestra aplicación. A continuación se copian los paquetes y requisitos de la aplicación dentro de la imagen y se ejecuta la compilación o preparación del paquete, si fuera necesario. Finalmente, se especifica el punto de entrada del contenedor y los argumentos que recibirá, si recibe. Además, si es necesario se añaden los puertos expuestos y volúmenes necesarios para el funcionamiento.

En el código 1 se tiene un ejemplo de un Dockerfile completo [25]:

```
1 # syntax=docker/dockerfile:1
2 FROM golang:1.16-alpine AS build
3
4 # Install tools required for project
5 # Run `docker build --no-cache .` to update dependencies
6 RUN apk add --no-cache git
7 RUN go get github.com/golang/dep/cmd/dep
8
9 # List project dependencies with Gopkg.toml and Gopkg.lock
10 # These layers are only re-built when Gopkg files are updated
11 COPY Gopkg.lock Gopkg.toml /go/src/project/
12 WORKDIR /go/src/project/
13 # Install library dependencies
14 RUN dep ensure -vendor-only
15
16 # Copy the entire project and build it
17 # This layer is rebuilt when a file changes in the project directory
18 COPY . /go/src/project/
19 RUN go build -o /bin/project
20
21 # This results in a single layer image
```

```
22 FROM scratch
23 COPY --from=build /bin/project /bin/project
24 ENTRYPOINT [ "/bin/project" ]
25 CMD [ "--help" ]
```

Listing 1: Ejemplo de Dockerfile para una aplicación Go [25].

En el fichero anterior se establece una imagen de partida `golang:1.16-alpine` que contiene los binarios de Go en una distribución de muy poco peso (proyecto Linux Alpine). Esta imagen se obtiene desde Docker Hub.

A continuación, instala el paquete `git` y el gestor de dependencias de Go. Después, copia el proyecto en sí e instala las dependencias en la ruta `/go/src/project`. Finalmente, copia el directorio actual en dicha ruta y define una nueva imagen partiendo de la de Golang en donde se ejecuta el proyecto compilado con las opciones `--help` por defecto.

Cuando se define un contenedor es recomendable instalar solo aquellas dependencias que sean necesarias. Esto permite una mayor y mejor mantenibilidad, reduce la complejidad y el tiempo de construcción de la imagen.

Por otra parte, se recomienda encarecidamente desacoplar la aplicación: por ejemplo, un servidor web posiblemente requiera de varias aplicaciones en ejecución. Es recomendable separarlas en contenedores y habilitar la comunicación entre ellos a encapsularlo todo en un único contenedor. Esto facilita, entre otros, un escalado horizontal en donde si se requieren de más imágenes se crean.

Además, el número de capas se debe mantener lo más pequeño posible: las instrucciones `RUN`, `COPY` y `ADD` crean capas, mientras que otras instrucciones solo crean imágenes intermedias.

Finalmente, es importante construir el Dockerfile teniendo en cuenta que Docker usa una caché interna. Si se quiere deshabilitar se puede hacer con la opción `--no-cache=true` en el comando `docker build`. Sin embargo, es recomendable hacer uso de la caché interna de Docker ya que agiliza el proceso de construcción.

2.3. Comunicación entre contenedores

2.4. Despliegue de aplicaciones multi-contenedores. docker-compose

2.5. “Orquestación” de contenedores

2.6. Líneas futuras de desarrollo e innovación

3. Seguridad en Docker

3.1. Análisis de la pila Docker

3.2. Diferencias fundamentales con chroot

3.3. Seguridad en las comunicaciones de red – *firewall*

3.4. Seguridad en las comunicaciones inter-contenedores

Referencias

- [1] «History of Technology Timeline,» Encyclopedia Britannica. (), dirección: <https://www.britannica.com/story/history-of-technology-timeline> (visitado 07-05-2021).
- [2] «Evolution of Data Storage Timeline,» The Gateway. (), dirección: </gateway/data-storage-timeline/> (visitado 07-05-2021).
- [3] WeComputingTech. «Storage devices london | We Computing Blog.» (), dirección: <http://www.wecomputing.com/blog/tag/storage-devices-london/> (visitado 07-05-2021).
- [4] «How To Become A Web Developer in 2021 — Everything You Need To Know.» (), dirección: <https://careercity.com/en/blog/web-development/what-does-it-take-to-become-a-web-developer-everything-you-need-to-know-before-getting-started/> (visitado 07-05-2021).
- [5] *Dependency hell*, en Wikipedia, 29 de mayo de 2021. dirección: https://en.wikipedia.org/w/index.php?title=Dependency_hell&oldid=1025704309 (visitado 03-06-2021).
- [6] «Docker overview,» Docker Documentation. (2 de jun. de 2021), dirección: <https://docs.docker.com/get-started/overview/> (visitado 03-06-2021).
- [7] «What is a Container? | App Containerization | Docker.» (), dirección: <https://www.docker.com/resources/what-container> (visitado 03-06-2021).
- [8] «Containerd.» (), dirección: <https://containerd.io/> (visitado 03-06-2021).
- [9] «Container Runtime with Docker Engine | Docker.» (), dirección: <https://www.docker.com/products/container-runtime> (visitado 03-06-2021).
- [10] S. Yegulalp. «What is Docker? The spark for the container revolution,» InfoWorld. (), dirección: <https://www.infoworld.com/article/3204171/what-is-docker-the-spark-for-the-container-revolution.html> (visitado 03-06-2021).
- [11] «Docker Desktop WSL 2 backend,» Docker Documentation. (2 de jun. de 2021), dirección: <https://docs.docker.com/docker-for-windows/wsl/> (visitado 03-06-2021).
- [12] S. Kulshrestha. «Docker Networking – Explore How Containers Communicate With Each Other,» Medium. (10 de sep. de 2020), dirección: <https://medium.com/edureka/docker-networking-1a7d65e89013> (visitado 03-06-2021).
- [13] S. Watts. «The State of Containers Today: A Report Summary,» BMC Blogs. (), dirección: <https://www.bmc.com/blogs/state-of-containers/> (visitado 04-06-2021).
- [14] «6 Container Adoption Trends of 2020,» StackRox: Kubernetes and container security solution. (), dirección: <https://www.stackrox.com/post/2020/03/6-container-adoption-trends-of-2020/> (visitado 04-06-2021).

- [15] «Container Adoption Statistics: The Future of the Container Market,» Capital One. (), dirección: <https://www.capitalone.com/tech/cloud/container-adoption-statistics/> (visitado 04-06-2021).
- [16] «Download the 2018 Docker Usage Report,» Sysdig. (29 de mayo de 2018), dirección: <https://sysdig.com/blog/2018-docker-usage-report/> (visitado 04-06-2021).
- [17] «Manage data in Docker,» Docker Documentation. (2 de jun. de 2021), dirección: <https://docs.docker.com/storage/> (visitado 04-06-2021).
- [18] *UnionFS*, en *Wikipedia, la enciclopedia libre*, 2 de jul. de 2020. dirección: <https://es.wikipedia.org/w/index.php?title=UnionFS&oldid=127421790> (visitado 04-06-2021).
- [19] «Use volumes,» Docker Documentation. (2 de jun. de 2021), dirección: <https://docs.docker.com/storage/volumes/> (visitado 04-06-2021).
- [20] «Use bind mounts,» Docker Documentation. (2 de jun. de 2021), dirección: <https://docs.docker.com/storage/bind-mounts/> (visitado 04-06-2021).
- [21] «Networking overview,» Docker Documentation. (2 de jun. de 2021), dirección: <https://docs.docker.com/network/> (visitado 04-06-2021).
- [22] *Docker (software)*, en *Wikipedia*, 6 de jun. de 2021. dirección: [https://en.wikipedia.org/w/index.php?title=Docker_\(software\)&oldid=1027143347](https://en.wikipedia.org/w/index.php?title=Docker_(software)&oldid=1027143347) (visitado 09-06-2021).
- [23] «Dockerfile reference,» Docker Documentation. (9 de jun. de 2021), dirección: <https://docs.docker.com/engine/reference/builder/> (visitado 09-06-2021).
- [24] H. Jethva. «How Dockerfile Works? – Linux Hint.», (), dirección: https://linuxhint.com/dockerfile_beginner_guide/ (visitado 10-06-2021).
- [25] «Best practices for writing Dockerfiles,» Docker Documentation. (9 de jun. de 2021), dirección: <https://docs.docker.com/develop/develop-images/dockerfile-best-practices/> (visitado 10-06-2021).