

Índice

Prólogo	13
Capítulo I	
Introducción a Docker	15
1. Nacimiento y evolución de los contenedores	15
2. Contenedores Docker vs. Máquinas virtuales (VM)	16
2.1. ¿Qué es Docker?	16
2.2. Diferencias entre Máquinas Virtuales y contenedores Docker	17
3. Docker frente a sus competidores	18
3.1. Rocket	18
3.2. Original Mesos Container y Universal Container Runtime (UCR)	18
3.3. CRI-O	19
3.4. Unikernels	19
4. Estandarización de la tecnología de contenedores	19
4.1. Image-spec	20
4.2. Runtime-spec	21
5. Introducción a Docker	22
5.1. Componentes Docker	22
5.2. Diferencias entre imagen y contenedor Docker	24
5.3. El demonio Docker (o Docker Engine)	24
5.4. Instalación de Docker	26
5.4.1. Windows	26
5.4.2. Mac	26
5.4.3. Linux	27
5.5. Primeros pasos con Docker	28
Capítulo II	
Dockerfile	39
1. Dockerfile	39

1.1. Formato	42
1.2. Directivas	42
1.3. escape	42
1.4. Variables de entorno	43
1.5. Fichero .dockerignore	44
1.6. FROM	46
1.7. RUN	51
1.8. CMD	52
1.9. ENTRYPOINT	53
1.10. LABEL	56
1.11. EXPOSE	56
1.12. ENV	57
1.13. ADD	58
1.14. COPY	59
1.15. VOLUME	60
1.16. USER	62
1.17. WORKDIR	63
1.18. ARG	64
1.19. ONBUILD	66
1.20. STOPSIGNAL	67
1.21. HEALTHCHECK	68
1.22. SHELL	69

Capítulo III

Imágenes71

1. Capas	71
2. Manejo de imágenes	74
2.1. Descarga de Imágenes	75
2.2. Publicación de Imágenes	76
2.3. Registro	78
2.4. Limpieza de Imágenes	80
2.5. Buenas Prácticas Creando imágenes	83

Capítulo IV

Contenedores87

1. Ciclo de Vida de un Contenedor	88
2. Configuración de un Contenedor	93
2.1. Creando Contenedores más amigables	93
2.2. Publicación de Puertos	96
2.3. Restricción de Recursos	97

2.3.1. Memoria.....	98
2.3.2. CPU.....	99
3. Información de Contenedores	100
4. Interactuando con Contenedores	101
5. Persistencia de Datos y Volúmenes	102
5.1. Persistencia de Datos.....	103
5.2. Sistema de Ficheros del Host.....	105
5.3. Memoria.....	106
5.4. Volúmenes.....	106
6. Limpieza.....	107
6.1. Contenedores.....	108
6.2. Volúmenes.....	108
7. Compose	109
7.1. Variables de Entorno	113
7.2. Compartiendo la Configuración de Compose	115
7.2.1. Multiple Ficheros Compose.....	115
7.2.2. Añadiendo y Reemplazando la Configuración	117
7.2.3. Redes en Compose.....	118
7.2.4. Sincronizando el Arranque	120
 Capítulo V	
Redes	123
1. Conceptos básicos de redes en Docker.....	123
2. Tipos de redes Docker	127
2.1. Bridge.....	128
2.2. Host	130
2.3. Overlay.....	131
2.4. MacVLAN.....	132
3. Creación y gestión de redes Docker	133
4. Enlazando contenedores (link)	135
 Capítulo VI	
Introducción a Docker Swarm.....	137
1. Conceptos Básicos	137
1.1. Swarm	137
1.2. Nodos	138
1.3. Servicios/Tareas	138
1.4. Balanceador de Carga	138

2. Creando un Swarm	138
3. Manejando Servicios	140
4. Manejando Nodos.....	142
5. Stacks.....	143
6. Configuraciones y Secretos	147
7. Limpieza.....	149

Capítulo VII

Buenas Prácticas de Seguridad.....151

1. Configuración del host	151
1.1. Creación de particiones separadas para los contenedores.....	151
1.2. Limitar los usuarios que pueden controlar el demonio de Docker.....	152
1.3. Auditar los ficheros y directorios de Docker.....	153
2. Configuración del demonio de Docker	154
2.1. Restringir el tráfico de red entre contenedores.....	155
2.2. Autorización habilitada para el CLI de Docker.....	155
2.3. Gestión centralizada/remota de log.....	157
2.4. Recuperación en vuelo de los contenedores.....	159
2.5. Permisos en los ficheros de configuración del demonio de Docker.....	159
3. Configuración de la imagen y fichero Dockerfile.....	160
3.1. Ejecución de contenedores con usuario no root.....	160
3.2. Content Trust de docker	161
3.3. Eliminación de los permisos de setuid y setgid	162
3.4. COPY en vez de ADD en el Dockerfile	162
3.5. No almacenar secretos en el Dockerfile.....	163
4. Runtime de contenedores.....	164
4.1. Habilitar SELinux/AppArmor.....	164
4.2. Capabilities de Linux restringidas dentro de los contenedores.....	165
4.3. No permitir la ejecución de contenedores privilegiados.....	166
4.4. SSH no permitido dentro de los contenedores.....	167
4.5. No mapear puertos privilegiados dentro de los contenedores.....	167
4.6. Asegurar que el namespace de red host no es compartido.....	168
5. Otras buenas prácticas.....	169
5.1. Docker bench security.....	170

Capítulo VIII

SecDevOps175

1. Filosofía DevOps	175
1.1. Entornos de CI/CD.....	176
1.2. Añadiendo “Sec” al “DevOps”.....	180
2. Análisis estático de vulnerabilidades	182
2.1. OpenSCAP/oscap-docker.....	183
2.2. CoreOS/Clair.....	185
2.3. Anchore.....	187
2.4. Dagda.....	190
3. Firma de imágenes	193
3.1. Notary.....	194
4. Publicación de imágenes	198
4.1. Registry.....	199
Capítulo IX	
Moby Project	203
1. Introducción	203
2. InfraKit	205
3. LinuxKit	210
4. BuildKit	215
5. Containerd	219
6. SwarmKit	223
Índice alfabético	229
Índice de imágenes	231

