

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
-----------------------	----

4.3. 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
----------------------------------	----

5.5. 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	52
1.8 CMD	53
1.9 ENTRYPOINT	54
1.10 LABEL	57
1.11 EXPOSE	57
1.12 ENV	58
1.13 ADD	59
1.14 COPY	60
1.15 VOLUME	62
1.16 USER	63
1.17 WORKDIR	65
1.18 ARG	65
1.19 ONBUILD	68
1.20 STOPSIGNAL	68
1.21 HEALTHCHECK	69
1.22 SHELL	70

Capítulo III

Imágenes73

1. Capas73

2.2. Manejo de imágenes76

2.1. Descarga de Imágenes	77
2.2. Publicación de Imágenes	78
2.3. Registro	80
2.4. Limpieza de Imágenes	82
2.4. Buenas Prácticas Creando imágenes	86

Capítulo IV

Contenedores89

1. Ciclo de Vida de un Contenedor90

2. Configuración un Contenedor95

2.1 Creando Contenedores más amigables	96
2.2 Publicación de Puertos	98
2.3 Restricción de Recursos	99

3. Información de Contenedores106

4. Interactuando con Contenedores107

4.1 Contextos.....	108
5. Persistencia de Datos y Volúmenes	111
5.1 Persistencia de Datos.....	111
5.2 Sistema de Ficheros del Host.....	113
5.3 Memoria.....	114
5.4 Volúmenes	115
6. Limpieza	116
6.1 Contenedores.....	116
6.2 Volúmenes	117
7. Compose	118
7.1 Variables de Entorno	123
7.2 Compartiendo la Configuración de Compose	125
7.3 Redes en Compose	128
7.4 Sincronizando el Arranque.....	130
7.5 Perfiles.....	131
7.6 GPU.....	132
 Capítulo V	
Redes	133
1. Conceptos básicos de redes en Docker.....	133
2. Tipos de redes Docker	137
2.1. Bridge.....	138
2.2. Host.....	140
2.3. Overlay.....	141
2.3. MacVLAN.....	142
3. Creación y gestión de redes Docker	143
4. Enlazando contenedores (link)	145
 Capítulo VI	
Introducción a Docker Swarm.....	147
1. Conceptos Básicos	147
1.1 Swarm	147
1.2 Nodos	148
1.3 Servicios/Tareas	148
1.4 Balanceador de Carga	148
2. Creando un Swarm	148
3. Manejando Servicios	150

4. Manejando Nodos.....	152
5. Stacks.....	153
6. Configuraciones y Secretos	157
7. Limpieza.....	158

Capítulo VII

Buenas Prácticas de Seguridad.....161

1. Configuración del host	161
Creación de particiones separadas para los contenedores.....	161
Limitar los usuarios que pueden controlar el demonio de Docker.....	162
Auditar los ficheros y directorios de Docker.....	163
2. Configuración del demonio de Docker	164
Restringir el tráfico de red entre contenedores.....	165
Autorización habilitada para el CLI de Docker	165
Gestión centralizada/remota de log	167
Recuperación en vuelo de los contenedores.....	169
Permisos en los ficheros de configuración del demonio de Docker.....	169
3. Configuración de la imagen y fichero Dockerfile.....	170
Ejecución de contenedores con usuario no root.....	171
Content Trust de Docker	171
Eliminación de los permisos de setuid y setgid	172
COPY en vez de ADD en el Dockerfile	173
No almacenar secretos en el Dockerfile.....	173
4. Runtime de contenedores.....	174
Habilitar SELinux/AppArmor.....	175
Capabilities de Linux restringidas dentro de los contenedores.....	176
No permitir la ejecución de contenedores privilegiados	177
SSH no permitido dentro de los contenedores	177
No mapear puertos privilegiados dentro de los contenedores.....	178
Asegurar que el namespace de red host no es compartido.....	178
Limitar uso de recursos como la memoria y la CPU	179
5. Otras buenas prácticas.....	180
Docker bench security.....	180

Capítulo VIII

SecDevOps185

1. Filosofía DevOps.....	185
Entornos de CI/CD.....	186

Añadiendo “Sec” al “DevOps”	190
2. Análisis estático de vulnerabilidades	192
OpenSCAP/oscap-Docker	193
Quay/Clair	194
Anchore	196
Dagda	198
Docker Scan	201
Trivy	203
3. Firma de imágenes.....	205
Notary	205
4. Publicación de imágenes	210
Registry	211
5. Montando un servidor de integración continua en contenedores	213
 Capítulo IX	
Moby Project	225
1. Introducción.....	225
2. InfraKit.....	227
3. LinuxKit	232
4. BuildKit	237
5. Containerd	241
6. SwarmKit	245
 Índice de imágenes	249
Índice alfabético	251
Otros libros publicados.....	253

