

Prólogo

Capítulo 1
Introducción a Linux

- 1. Los orígenes de Linux 9
- 2. Las distintas distribuciones de Linux 12
 - 2.1 Slackware 13
 - 2.2 Debian 14
 - 2.3 Red Hat Enterprise Linux (RHEL) 15
 - 2.4 Fedora 17
 - 2.5 Ubuntu 18
 - 2.6 Arch Linux. 20

Capítulo 2
La línea de comandos

- 1. Comandos básicos de Linux. 23
- 2. Permisos, seguridad y ACL. 26
 - 2.1 Permisos 26
 - 2.1.1 Aspectos generales 26
 - 2.1.2 Gestión de permisos y propietarios
de archivos/carpetas 31
 - 2.2 Niveles de seguridad 33
 - 2.2.1 SELinux 33
 - 2.2.2 AppArmor 35
 - 2.3 ACL 39

Capítulo 3**Configuración del sistema**

1. Configuración de la red	43
1.1 ifconfig	45
1.2 ip	47
1.3 netstat	49
1.4 ss	51
1.5 ping	53
1.6 traceroute	54
2. Gestión de usuarios y grupos	54
2.1 Gestión de usuarios	56
2.2 Gestión del grupo	56

Capítulo 4**Administración del sistema**

1. Gestión de paquetes y actualizaciones	59
1.1 Debian y el sistema APT	60
1.1.1 Gestión de paquetes	60
1.1.2 Actualización	62
1.1.3 Investigación e información	63
1.2 Fedora y el sistema DNF	64
1.2.1 Gestión de paquetes	64
1.2.2 Gestión del grupo	66
1.2.3 Actualización	67
1.2.4 Investigación e información	67
2. Gestión de los servicios del sistema	68
2.1 Comandos systemctl básicos	68
2.2 Controles adicionales	70
3. Gestión de tareas y procesos	70
3.1 Gestión de tareas con cron y crontab	70
3.2 Gestión de los procesos	71

Capítulo 5
Administración avanzada

- 1. Herramientas de control y diagnóstico 73
 - 1.1 top - Supervisión de procesos en tiempo real 73
 - 1.2 htop, una alternativa coloreada 76
 - 1.3 free, la herramienta para gestionar la RAM 78
 - 1.4 Nagios 79
 - 1.5 Zabbix 85
 - 1.6 ¿Cuál es la mejor solución? 92
 - 1.6.1 Nagios 92
 - 1.6.2 Zabbix 93
- 2. Copias de seguridad y restauración 94
 - 2.1 ¿Por qué hacer copias de seguridad? 94
 - 2.2 ¿Por qué restaurar? 94
 - 2.3 Copias de seguridad 95
 - 2.4 Restauración 95
- 3. Virtualización y contenedores 96
 - 3.1 Virtualización 97
 - 3.2 Contenedorización 98

Capítulo 6
Despliegue y gestión de servidores

- 1. Configuración de un servidor LAMP 101
 - 1.1 ¿Cómo funcionan los módulos de Apache? 108
 - 1.2 Activación de los módulos de Apache 109
- 2. Gestión de un servidor de archivos 111
- 3. Gestión de servidores con SSH 115

Capítulo 7

Redes avanzadas con Linux

1. Introducción a las redes avanzadas	121
2. Configuración de redes VLAN y VPN	124
2.1 VLAN	125
2.2 VPNs	133
3. Uso de servidores proxy	145
3.1 Squid: optimización y control	146
3.2 Privoxy: confidencialidad y filtrado	146
3.3 Implementación y gestión	146
3.4 Ventajas adicionales	147
3.5 Aspectos a tener en cuenta	147
4. Configuración de servidores DNS	148
5. Uso de servidores DHCP	152
6. Configuración del cortafuegos	154
6.1 Configuración básica	156
6.2 Ir más allá	158

Capítulo 8

Automatización con Docker

1. Conceptos básicos de Docker y microservicios	167
1.1 Los orígenes de Docker: un cambio de paradigma en la contenedorización	169
1.2 El despegue de Docker y la adopción por la comunidad	169
1.3 La creciente influencia de Docker en el desarrollo de software	170
2. Configuración de microservicios con Docker	170
2.1 Contenedores en Docker	170
2.2 Dockerfiles: script de construcción de imágenes	171
2.3 Dockerfile para una aplicación web básica en Node.js	171
2.4 Dockerfile para una aplicación Python/Flask	172

- 2.5 Dockerfile para una aplicación Java con Maven 172
- 2.6 Dockerfile para una base de datos MySQL 173
- 2.7 Dockerfile para una aplicación Go 173
- 2.8 La importancia crucial de los registros de Docker en la contenedorización 174
- 2.9 Docker Hub: un pilar de la comunidad Docker 174
- 2.10 Uso de Docker Hub: prácticas y consideraciones 175
- 2.11 Instalación de Docker 176
- 2.12 Crear una cuenta en Docker Hub 178
- 2.13 Opciones actuales 186
- 3. Gestión de microservicios con Docker 186
 - 3.1 Comandos populares de Docker 186
 - 3.2 Comandos adicionales para gestionar volúmenes 192
 - 3.3 Orquestación con Docker Compose 194
 - 3.4 Estructura básica 195
 - 3.5 Aspectos clave 196
 - 3.6 Explicaciones de nuestro archivo 198

Capítulo 9

Automatización con Puppet y Ansible

- 1. Los principios básicos de la automatización con Puppet 203
 - 1.1 Ventajas de Puppet 204
 - 1.2 Inconvenientes de Puppet 205
 - 1.3 Arquitectura maestro-agente (master-slave) 206
 - 1.4 Intercambio de certificados 206
 - 1.5 Creación de manifiestos y compilación en catálogos 207
 - 1.6 Ejecución del catálogo en el cliente 208
 - 1.7 Instalación y configuración de Puppet 209
 - 1.8 Generar y firmar el certificado del agente 212
 - 1.9 Escribir y desplegar los manifiestos 213

2.	Los principios básicos de la automatización con Ansible.	217
2.1	Arquitectura sin agentes	218
2.2	Módulos	218
2.3	Playbooks	220
2.3.1	Instalación e inicio de un servidor web Apache	220
2.3.2	Creación de usuarios	221
2.3.3	Actualización de todos los paquetes en servidores Debian	221
2.3.4	Aplicar un playbook.	222
2.4	Inventario	224
2.4.1	Ejemplo en formato INI.	224
2.4.2	Ejemplo en formato YAML	225
2.5	Variables	225
2.5.1	Variables definidas en un playbook.	226
2.5.2	Variables en los archivos de inventario.	226
2.5.3	Variables en archivos de variables independientes.	226
2.5.4	Pasar variables en la línea de comandos	227
2.5.5	Uso de variables en las plantillas Jinja2.	227
2.6	Facts.	227
2.6.1	Ejemplo de uso de facts en un playbook.	228
2.6.2	Ejemplos de facts comúnmente utilizados	228
2.7	Roles	229
2.7.1	Estructura del archivo defaults/main.yml	229
2.7.2	Estructura del archivo handlers/main.yml	230
2.7.3	Estructura del archivo meta/main.yml	231
2.7.4	Estructura del archivo tasks/main.yml.	232
2.7.5	Estructura del archivo templates/nginx.conf.j2	234
2.7.6	Estructura del archivo vars/main.yml.	235
2.8	Funcionamiento global.	237
2.9	Instalación y configuración de Ansible	237
2.10	Añada la clave pública SSH en otra máquina.	238
2.11	Configuración básica de Ansible para utilizar la máquina.	239

- 3. Ejemplos prácticos de uso de Puppet y Ansible 242
 - 3.1 Escenario A: configuración de un servidor web NGINX con SSL y redirección 243
 - 3.2 Escenario B: configuración de un servidor de base de datos PostgreSQL con replicación 245
 - 3.3 Escenario C: configuración de un servidor web NGINX 249
 - 3.4 Escenario D: configuración de reglas de cortafuegos con UFW 252
 - 3.5 Escenario E: Replicación de bases de datos PostgreSQL. 254
 - 3.6 Escenario F: copias de seguridad automatizadas 259

Capítulo 10

Gestión de los permisos y seguridad en Linux

- 1. Riesgos comunes de seguridad y escalada de permisos 261
 - 1.1 Enumeración en la máquina 266
 - 1.2 Mecanismos internos 276
 - 1.2.1 Interfaces de red 276
 - 1.2.2 Último inicio de sesión de usuario. 277
 - 1.2.3 Historial de comandos 277
 - 1.2.4 Buscar archivos históricos 277
 - 1.2.5 Proc 278
 - 1.2.6 Servicios. 278
 - 1.2.7 Búsqueda de identificadores. 282
 - 1.2.8 Claves SSH 283
 - 1.3 Abuso de permisos sudo. 283
 - 1.4 Capacidades (capabilities) 285
 - 1.5 Scripts y herramientas automatizadas 291
 - 1.6 Permisos especiales 292
 - 1.7 Abuso de PATH 295
- 2. Medidas preventivas contra la escalada de permisos 297

8 --- Linux

De la línea de comandos a la administración del sistema

Capítulo 11

Conclusión

1. Perspectivas y retos para Linux	299
2. Mejores prácticas para un uso óptimo	300
Índice	303