



Administración de *Sistemas y Redes*

Sesión 9

Omar Teixeira González,
UO281847

Tabla de contenidos.

Tabla de contenidos	2
OPCIONAL	7
1. Balanceo de carga con HAProxy	
Harán falta tres máquinas con Linux que llamaremos balanceador, web1 y web2 aunque podrían ser más de dos los servidores web y no necesariamente Linux. Inicialmente estarán conectadas a Internet vía NAT con el adaptador por defecto. Se pueden hacer tres instalaciones limpias o partir de una y clonarla dos veces más. Si se hace una clonación, en la política de dirección MAC debe estar activa la opción "Incluir solo dirección MAC de adaptador de red NAT" o bien "Generar nuevas direcciones MAC para todos los adaptadores de red" antes de empezar a clonar. Como es lógico no se puede tener tres máquinas en una misma red con una misma MAC. Instalar el servidor web en los nodos web1 y web2 y haproxy en el nodo balanceador. Por comodidad se puede tener todo en las tres máquinas y luego se clonan. También se instalará el php. 7	
2. Apagar ahora la máquina virtual y cambiar su adaptador de NAT a red sólo anfitrión. Si nuestro anfitrión anda escaso de memoria podemos rebajar la RAM a 1,5 GB en las máquinas virtuales. Hacer dos clones más, serán necesarios tres equipos. En las preferencias globales de red VirtualBox deshabilitar el servidor DHCP para la red de solo anfitrión. Iniciar las tres máquinas. Con la orden ip addr hay que mirar qué adaptador de red está activo. Si las máquinas proceden de instalaciones limpias probablemente será enp0s3.	9
3. En el balanceador modificar la configuración de enp0s3 para que tenga una dirección IP 192.168.56.20 estática. Reiniciar el equipo (o la red y comprobar con la orden ip addr que el adaptador tiene la dirección IP correcta.	12
Repetir los pasos anteriores con los equipos web1 y web2 pero poniendo las direcciones IP respectivas 192.168.56.21 y 192.168.56.22. Con las tres máquinas iniciadas se puede comprobar que hay conectividad entre ellas con la orden ping, bien desde una de ellas o bien desde el anfitrión:	12
4. El siguiente paso es activar los servidores web. En web1 y web2 crear el archivo. Hay que acordarse de poner "Servidor web 2" en web2.	15
5. Abrir el cortafuegos para tráfico web en las tres máquinas:	17
6. En web1 y web2 iniciar el servicio httpd:	18
7. Desde el anfitrión con Windows comprobar con cualquier navegador que se puede acceder a ambos servidores web: http://192.168.56.21/ y http://192.168.56.22	19
8. En este punto ya tenemos dos servidores web activos y corriendo, se pueden minimizar ambas máquinas virtuales. El siguiente paso es configurar el balanceador de carga. En el equipo balanceador hay un archivo llamado /etc/haproxy/haproxy.cfg, hay que cambiar las siguientes líneas para que escuche en el puerto 80 y balancee entre los dos servidores web recién instalados:	20
9. Hay que iniciar ahora servicio de balanceo de carga	21
10. También se puede minimizar ahora esta máquina virtual. En el navegador del anfitrión ir a http://192.168.56.20/ ¿qué aparece? Tras refrescar la página varias veces ¿qué aparece? Si se detiene ahora uno de los servidores web (web1 o web2) con systemctl stop httpd.service (o bien se apaga la máquina) y se refresca de nuevo la página ¿qué aparece? Al detener el servicio httpd o apagar también el otro servidor web y refrescar de nuevo la página ¿qué aparece? Elimine los ficheros index.html y en su lugar ponga estos ficheros index.php en ambos servidores web.	21
11. ¿Cambia la cookie de sesión? Experimente modificando haproxy.cfg con este contenido que permite hacer sesiones "pegajosas". Borre de vez en cuando las cookies del navegador en la última hora para hacer pruebas y añada capturas de pantalla. ¿Cuál sería la utilidad de estas sesiones pegajosas frente a las de servidor alternante?	
23	
<i>No, no cambia.</i>	23

<i>Las sesiones pegajosas son capaces de mantener el estado de la sesión del usuario, así como evitar el problema de la sesión interrumpida.....</i>	24
SAN (Storage Area Network)	25
1. Los servidores NAS ya conocidos permiten proporcionar y compartir carpetas y ficheros ya sea vía protocolo SAMBA/CIFS o vía NFS sobre sistemas de ficheros muy habituales como son NTFS, ext4 o xfs. Los servidores SAN en cambio proporcionan bloques a otros equipos desde los cuales estos bloques se ven como discos externos. Para estos servidores SAN se emplean conexiones basadas en canal de fibra (FC) con el protocolo FCP que permite velocidades de hasta 16Gb/s aunque también se pueden emplear protocolos sobre Ethernet siendo el iSCSI (Internet Small Computer System Interface) el más frecuente. A diferencia de los NAS no es posible compartir un disco SAN excepto si se emplea algún tipo de sistema de ficheros de cluster diseñado específicamente para esto como puedan ser GFS2 (RedHat), CSV (Microsoft), GPFS (IBM) o Xsan (Apple). Para esta práctica se van a emplear dos equipos, uno que hará de servidor (llamado "objetivo/target" de ahora en adelante) y proporcionará los bloques de un disco completo y los de una imagen de disco. El otro hará de cliente (llamado "iniciador/initiator" de ahora en adelante) que montará los dos discos de red proporcionados por el servidor/objetivo. Este iniciador o cliente verá tales recursos como discos internos. Ambas máquinas virtuales tendrán un adaptador de red conectado a NAT para descargar el software necesario y otro conectado a una red interna que se empleará exclusivamente para el tráfico iSCSI. Las operaciones a realizar son a partir de dos Linux mínimos o con GUI: primero añadir un segundo adaptador de red interna a ambas máquinas virtuales y además al equipo que actuará como servidor añadirle un segundo disco. Puestos en marcha ambos sistemas, la configuración de los adaptadores de red interna pueden hacerse con las órdenes nmcli ya conocidas aplicándolas al adaptador enp0s8 de manera que el servidor (objetivo/target) tenga la dirección IP 192.168.222.1 y el cliente (iniciador) la 192.168.222.2 quedando este adaptador en la zona "internal" del cortafuegos. Reiniciar la red y comprobar con la orden ping que ambos equipos se ven entre sí. Verificar también que cada adaptador está en la zona correspondiente:.....	25
2. En el objetivo comprobar que aparece el disco nuevo y crear un fichero de 1 GB que se exportará como otro disco.....	29
3. A continuación instalar el software, poner en marcha el servicio y abrir el puerto TCP 3260.....	30
4. Antes de configurar el objetivo y el iniciador debemos definir dos IQN. IQN son las iniciales de iSCSI Qualified Name y deben ser únicos. El formato que se emplea (RFC 3720) es iqn.aaaa-mm.mi.dominio:algo, por ejemplo iqn.2023-02.mi.dominio:c3po. Usaremos para el objetivo iqn.2023-02.as.servidor:1111 y para el iniciador iqn.2023-02.as.cliente:2222, nótese que no es necesario que existan los dominios de Internet que se indican, es solo un convenio. A continuación de los ":" puede ponerse cualquier cosa, un número de serie, un nombre de equipo o incluso nada eliminando los dos puntos. En el servidor hay que crear al menos un IQN objetivo, dos objetos para los almacenes de bloques y dos LUN (logical unit number). Opcionalmente pueden definirse más cosas.....	31
5. Suponemos que el disco nuevo es /dev/sdb y el fichero imagen de disco es fichero.dsk, se crea cada elemento y se verifica que se ha creado satisfactoriamente.....	32
6. Si el servidor tiene varios interfaces, debería especificarse ahora la dirección IP del adaptador por donde se desea escuchar, de lo contrario el servidor escuchará por todos los adaptadores. Vamos a saltar este paso pero en la vida real habría que borrar antes el acceso por defecto y añadir un acceso exclusivo para la dirección IP del adaptador de red a emplear. En este caso el servidor debería escuchar solo por el adaptador de red interna que tiene de dirección IP 192.168.222.1.	33
7. Creación de las dos LUNs y de un ACL sin restricciones para el iniciador.	34
8. Si todo ha ido correctamente se habrá guardado la configuración en /etc/target/saveconfig.json.	34
9. En el iniciador, instalar el software.....	35
10. Editar el nombre del iniciador.....	35
11. Verificar si ve al servidor.....	36

12. Si todo es correcto se verá como respuesta la dirección IP del servidor y su IQN. Se puede hacer ahora un login interactivo (--logout para salir)	36
13. A partir de este momento con # lsblk deben aparecer en el iniciador dos nuevos discos sdb y sdc si no había previamente otros. También pueden verse con # cat /proc/scsi/scsi.	37
14. Estos dos discos ya se pueden particionar, formatear y montar. Como no se sabe si van a ser sdb1 o sdd1 o cualquier otra cosa, es conveniente en el /etc/fstab montarlos por UUID en vez de por nombre. Obtener el UUID con blkid /dev/sdb1 y poner en fstab UUID="0fc99ba2-912f-4519-ab6d-04c76608c303" /mnt/disco ext4 _netdev 0 0 De esta forma siempre se montará en /mnt/disco con independencia de que sea vea con cualquier nombre. La opción _netdev garantiza que se espera a que se inicie primero la red. En vez de ext4 puede emplearse ext2, ext3, xfs o cualquier otro sistema de ficheros que se desee. Hágalo así con ambas particiones y reinicie el sistema. Compruebe que se realiza todo de forma automática en el iniciador y que ha arrancado correctamente el demonio iscsi. 38	
15. Añada una captura de pantalla de la orden df y de la cat /proc/scsi/scsi Consideraciones de seguridad: aunque no entra en el ámbito de esta asignatura debería permitirse el acceso con targetcli solo a la dirección IP del servidor deseada y se debería poner una ACL con las especificaciones necesarias. También debería abrirse el cortafuegos solo para el iniciador y debería añadirse un nombre de usuario CHAP y contraseña, tanto en el servidor como en el iniciador. A título informativo, las acciones a realizar para dotar de usuario y contraseña a la conexión serían las que siguen.	40
16. En el cliente, lo primero cerrar la conexión actual desmontando antes las unidades si fuera necesario..	41
17. En el servidor, indicar que se necesita autenticación (en el tpg) e indicar el usuario y clave en la acl del iniciador.	42
18. De nuevo en el cliente editar el fichero donde se especifican los parámetros de conexión cambiando lo siguiente.....	42
19. Borrar los datos de contacto anteriores, muy importante.	43
20. Verificar de nuevo al servidor.	44

```

[uo281847@localhost uxxxxxx]#vi iscsid.conf
[uo281847@localhost uxxxxxx]# iscsiadm --mode node --targetname iqn.2023-02.as.servidor:1111 --portal 192.168.222.1 --op delete
[uo281847@localhost uxxxxxx]# iscsiadm --mode=discovery --type=sendtargets --portal=192.168.222.1
192.168.222.1:3260,1 iqn.2023-02.as.servidor:1111
[uo281847@localhost uxxxxxx]# 

A título informativo, las acciones a realizar para dotar de usuario y contraseña a la conexión serían las que siguen.
En el cliente, lo primero cerrar la conexión actual desmontando antes las unidades si fuera necesario.
# iscsiadm --mode node --targetname iqn.2023-02.as.servidor:1111 --portal 192.168.222.1 --logout
En el servidor, indicar que se necesita autenticación (en el tpg) e indicar el usuario y clave en la aci del iniciador.
# targetcli
/> cd /iscsi/iqn.2023-02.as.servidor:1111/tpg1> set attribute authentication=1
/iscsi/inq.20...:1111/tpg1> cd /iscsi/inq.2023-02.as.servidor:1111/tpg1/acls/inq.2023-02.as.servidor:1111> set auth userid=mi_usuario
/iscsi/inq.20...:1111/tpg1/acls/inq.2023-02.as.servidor:1111> set auth password=mi_clave
De nuevo en el cliente editar el fichero donde se especifican los parámetros de conexión cambiando lo siguiente.
# vi iscsid.conf
node.session.auth.authmethod = CHAP
node.session.auth.username = mi_usuario
node.session.auth.password = mi_clave
Borrar los datos de contacto anteriores, muy importante.
# iscsiadm --mode node --targetname iqn.2023-02.as.servidor:1111 --portal 192.168.222.1 --op delete
Verificar de nuevo al servidor.
# iscsiadm --mode=discovery --type=sendtargets --portal=192.168.222.1
E iniciar sesión.
# iscsiadm --mode=node --targetname=iqn.2023-02.as.servidor:1111 --portal=192.168.222.1 --login

```

44

21. E iniciar sesión..... 44

```

[uo281847@localhost uxxxxxx]#iscsiadm --mode=node --targetname=inq.2023-02.as.servidor:1111 --portal=192.168.222.1 --login
Logging in to [iface: default, target: iqn.2023-02.as.servidor:1111, portal: 192.168.222.1,3260]
Login to [iface: default, target: iqn.2023-02.as.servidor:1111, portal: 192.168.222.1,3260] successful.
[uo281847@localhost uxxxxxx]# 

A título informativo, las acciones a realizar para dotar de usuario y contraseña a la conexión serían las que siguen.
En el cliente, lo primero cerrar la conexión actual desmontando antes las unidades si fuera necesario.
# iscsiadm --mode node --targetname iqn.2023-02.as.servidor:1111 --portal 192.168.222.1 --logout
En el servidor, indicar que se necesita autenticación (en el tpg) e indicar el usuario y clave en la aci del iniciador.
# targetcli
/> cd /iscsi/inq.2023-02.as.servidor:1111/tpg1> set attribute authentication=1
/iscsi/inq.20...:1111/tpg1> cd /iscsi/inq.2023-02.as.servidor:1111/tpg1/acls/inq.2023-02.as.servidor:1111> set auth userid=mi_usuario
/iscsi/inq.20...:1111/tpg1/acls/inq.2023-02.as.servidor:1111> set auth password=mi_clave
De nuevo en el cliente editar el fichero donde se especifican los parámetros de conexión cambiando lo siguiente.
# vi iscsid.conf
node.session.auth.authmethod = CHAP
node.session.auth.username = mi_usuario
node.session.auth.password = mi_clave
Borrar los datos de contacto anteriores, muy importante.
# iscsiadm --mode node --targetname iqn.2023-02.as.servidor:1111 --portal 192.168.222.1 --op delete
Verificar de nuevo al servidor.
# iscsiadm --mode=discovery --type=sendtargets --portal=192.168.222.1
E iniciar sesión.
# iscsiadm --mode=node --targetname=iqn.2023-02.as.servidor:1111 --portal=192.168.222.1 --login

```

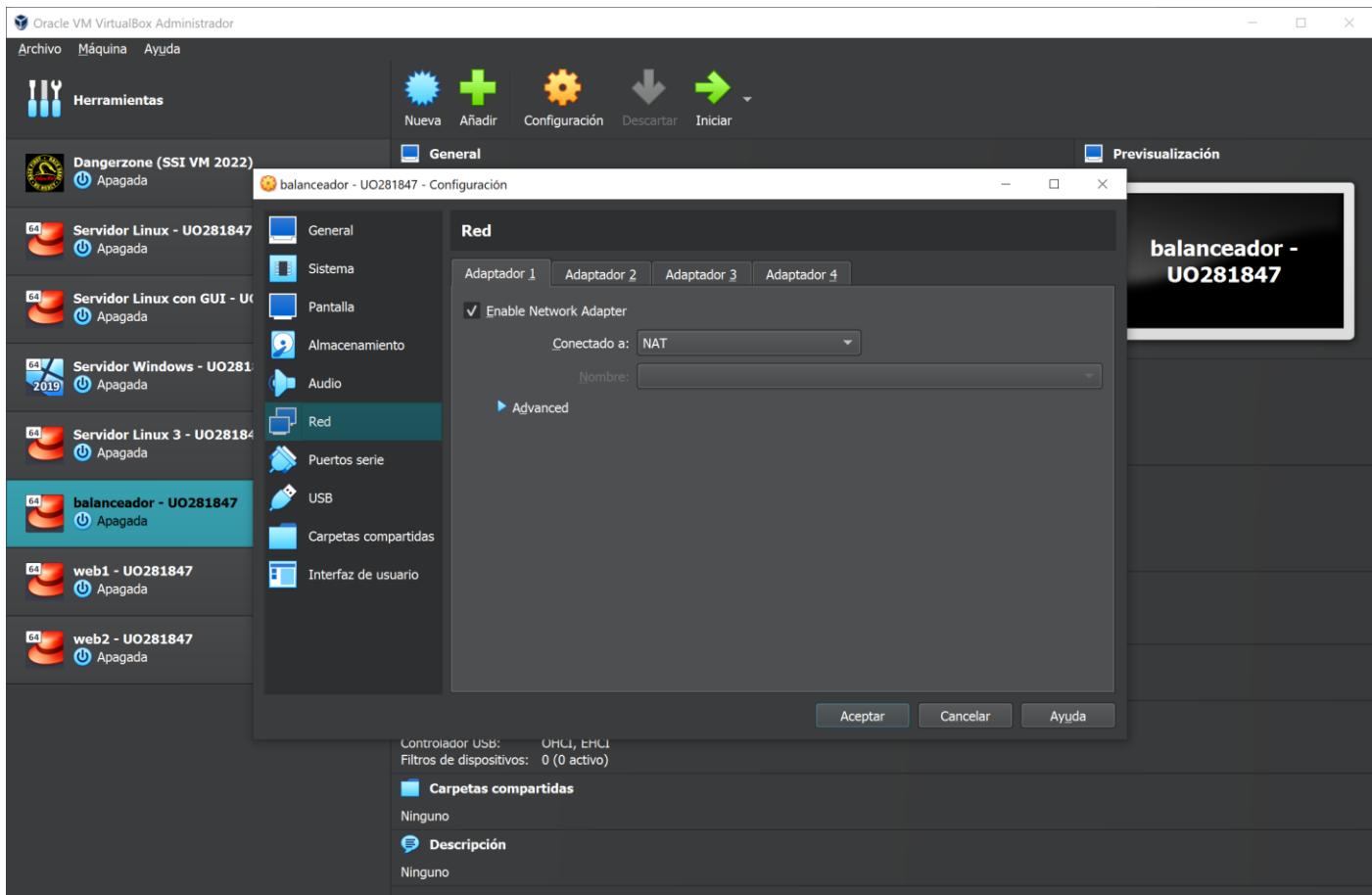
44

Balanceo de carga con HAProxy (cluster de alta disponibilidad) y SAN (Storage Area Network)

OPCIONAL

1. Balanceo de carga con HAProxy
- Harán falta tres máquinas con Linux que llamaremos balanceador, web1 y web2 aunque podrían ser más de dos los servidores web y no necesariamente Linux. Inicialmente estarán conectadas a Internet vía NAT con el adaptador por defecto. Se pueden hacer tres instalaciones limpias o partir de una y clonarla dos veces más. Si se hace una clonación, en la política de dirección MAC debe estar activa la opción "Incluir solo dirección MAC de adaptador de red NAT" o bien "Generar nuevas direcciones MAC para todos los adaptadores de red" antes de empezar a clonar. Como es lógico no se puede tener tres máquinas en una misma red con una misma MAC. Instalar el servidor web en los nodos web1 y web2 y haproxy en el nodo balanceador. Por comodidad se puede tener todo en las tres máquinas y luego se clonan. También se instalará el php.





balanceador - UO281847 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Actividades Firefox 13 de abr 09:44

Verificando : httpd-tools-2.4.53-7.el9_1.5.x86_64 10/21
 Verificando : mod_http2-1.15.19-3.el9_1.5.x86_64 11/21
 Verificando : mod_lua-2.4.53-7.el9_1.5.x86_64 12/21
 Verificando : nginx-filesystem-1:1.20.1-13.el9.alma 13/21
 Verificando : php-8.0.27-1.el9_1.x86_64 14/21
 Verificando : php-cli-8.0.27-1.el9_1.x86_64 15/21
 Verificando : php-common-8.0.27-1.el9_1.x86_64 16/21
 Verificando : php-fpm-8.0.27-1.el9_1.x86_64 17/21
 Verificando : php-mbstring-8.0.27-1.el9_1.x86_64 18/21
 Verificando : php-opcache-8.0.27-1.el9_1.x86_64 19/21
 Verificando : php-pdo-8.0.27-1.el9_1.x86_64 20/21
 Verificando : php-xml-8.0.27-1.el9_1.x86_64 21/21

Instalado:
 almalinux-logos-httdp-90.5.1-1.1.el9.noarch
 apr-1.7.0-11.el9.x86_64
 apr-util-1.6.1-20.el9.x86_64
 apr-util-bdb-1.6.1-20.el9.x86_64
 apr-util-openssl-1.6.1-20.el9.x86_64
 haproxy-2.4.17-3.el9_1.2.x86_64
 httpd-2.4.53-7.el9_1.5.x86_64
 httpd-core-2.4.53-7.el9_1.5.x86_64
 httpd-filesystem-2.4.53-7.el9_1.5.noarch
 httpd-tools-2.4.53-7.el9_1.5.x86_64
 mod_http2-1.15.19-3.el9_1.5.x86_64
 mod_lua-2.4.53-7.el9_1.5.x86_64
 nginx-filesystem-1:1.20.1-13.el9.alma.noarch
 php-8.0.27-1.el9_1.x86_64
 php-cli-8.0.27-1.el9_1.x86_64
 php-common-8.0.27-1.el9_1.x86_64
 php-fpm-8.0.27-1.el9_1.x86_64
 php-mbstring-8.0.27-1.el9_1.x86_64
 php-opcache-8.0.27-1.el9_1.x86_64
 php-pdo-8.0.27-1.el9_1.x86_64
 php-xml-8.0.27-1.el9_1.x86_64

¡Listo!
 [u0281847@localhost ~]#

Curso: Administración de Semana 5 - Práctica 9.pdf

https://www.campusvirtual.uniovi.es/pluginfile

AlmaLinux Documentation Blog Bug tracker GitHub organization

1 de 8 Tamaño automático

Curso 2022-23 - Práctica 9

Balanceo de carga con HAProxy (cluster de alta disponibilidad) y SAN (Storage Area Network)

OPCIONAL

Balanceo de carga con HAProxy

Harán falta tres máquinas con Linux que llamaremos balanceador, web1 y web2 aunque podrían ser más de dos los servidores web y no necesariamente Linux. Inicialmente estarán conectadas a Internet vía NAT con el adaptador por defecto.

Se pueden hacer tres instalaciones limpias o partir de una y clonarla dos veces más. Si se hace una clonación, en la política de dirección MAC debe estar activa la opción "Incluir solo dirección MAC de adaptador de red NAT" o bien "Generar nuevas direcciones MAC para todos los adaptadores de red" antes de empezar a clonar. Como es lógico no se puede tener tres máquinas en una misma red con una misma MAC.

Instalar el servidor web en los nodos web1 y web2 y haproxy en el nodo balanceador. Por comodidad se puede tener todo en las tres máquinas y luego se clonan. También se instalará el php.

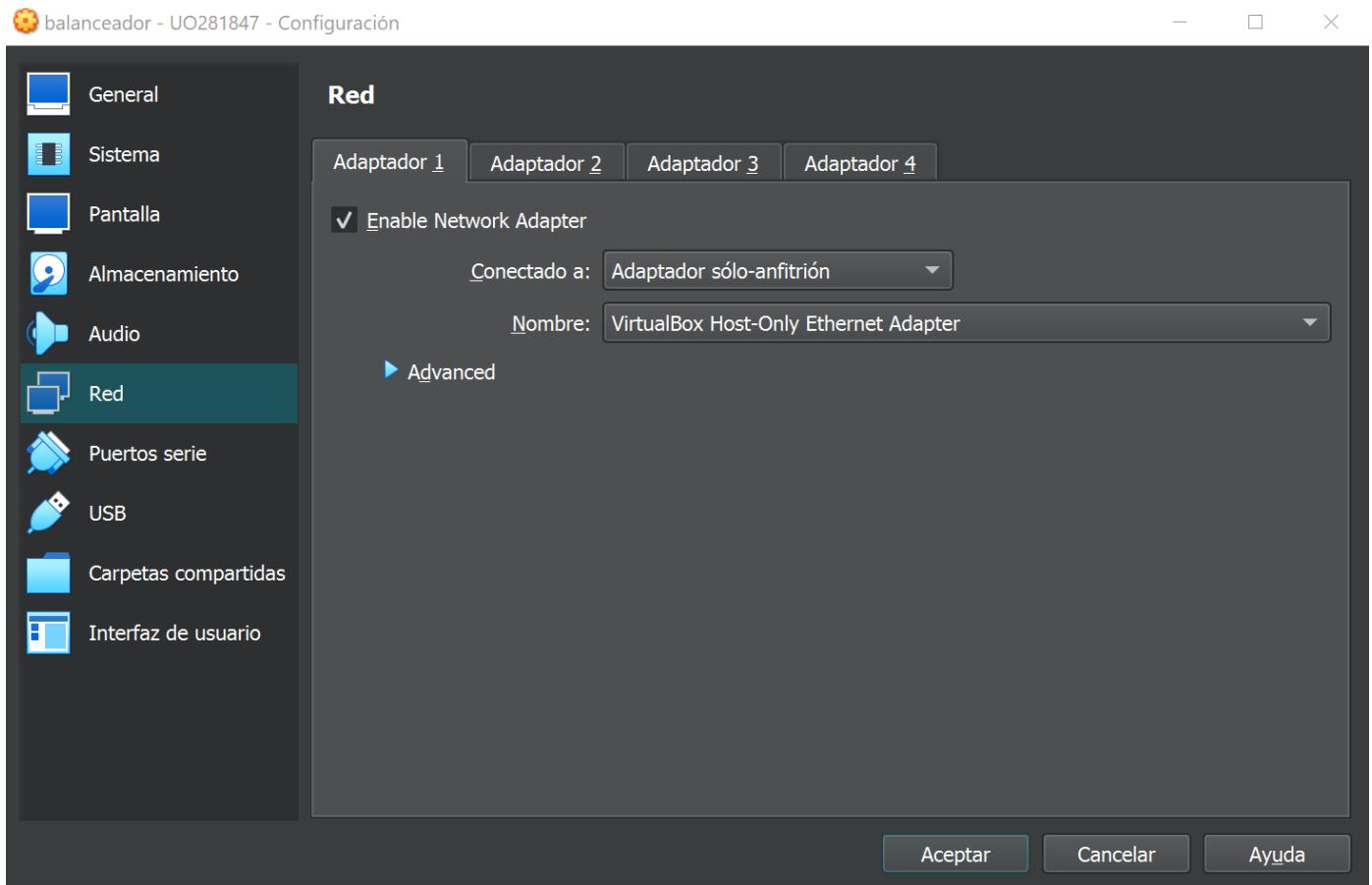
dnf install httpd haproxy php

Apagar ahora la máquina virtual y cambiar su adaptador de NAT a red sólo anfitrión. Si nuestro anfitrión anda escaso de memoria podemos rebajar la RAM a 1,5 GB en las máquinas virtuales.

Hacer dos clones más, serán necesarios tres equipos.

En las preferencias globales de red VirtualBox deshabilitar el servidor DHCP para la red

2. Apagar ahora la máquina virtual y cambiar su adaptador de NAT a red sólo anfitrión. Si nuestro anfitrión anda escaso de memoria podemos rebajar la RAM a 1,5 GB en las máquinas virtuales. Hacer dos clones más, serán necesarios tres equipos. En las preferencias globales de red VirtualBox deshabilitar el servidor DHCP para la red de solo anfitrión. Iniciar las tres máquinas. Con la orden ip addr hay que mirar qué adaptador de red está activo. Si las máquinas proceden de instalaciones limpias probablemente será enp0s3.



balanceador - UO281847 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Actividades Terminal 13 de abr 10:14

uoxxxxxx@localhost:home/uoxxxxxx

```
[uoxxxxxx@localhost uoxxxxxx]# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:4c:00:ab brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.101/24 brd 192.168.56.255 scope global dynamic noprefixroute enp0s3
        valid_lft 313sec preferred_lft 313sec
    inet6 fe80::a00:27ff:fe4c:ab/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
[uoxxxxxx@localhost uoxxxxxx]#
```

1 de 8

1 Semana 5 Practica 9...

46,1% 100% 100%

Balanza de carga con HAProxy

Hay falta tres máquinas con Linux que llamaremos balanceador, web1 y web2 aunque podrían ser más de dos los servidores web y no necesariamente Linux. Inicialmente estarán conectadas a Internet vía NAT con el adaptador por defecto.

Se pueden hacer tres instalaciones limpias a partir de una y clonarlas dos veces más. Si se hace una clonación, en la política de dirección MAC data estar activa la opción "Incluir solo dirección MAC de adaptador de red NAT" e bien "Generar nuevas direcciones MAC para todos los adaptadores de red" antes de empezar a clonar. Como es lógico no se puede tener tres máquinas en una misma red con una misma MAC.

Instalar el servidor web en los nodos web1 y web2 y haproxy en el nodo balanceador. Para comodidad se puede tener todo en las tres máquinas y luego se clonen. También se instala el php.

dnf install httpd haproxy php

Apagar ahora la máquina virtual y cambiar su adaptador de NAT a red sólo anfitrión. Si nuestro anfitrión anda escasos de memoria podemos rebajar la RAM a 1,5 GB en las máquinas virtuales.

Hacer dos clones más, serán necesarios tres equipos.

En las preferencias globales de red VirtualBox deshabilitar el servidor DHCP para la red de sólo anfitrión.

Irizar las tres máquinas. Con la orden # ip addr hay que mirar qué adaptador de red está activo. Si las máquinas proceden de instalaciones limpias probablemente será enp0s3.

En el balanceador modificar la configuración de enp0s3 para que tenga una dirección IP 192.168.56.20 estática.

2

3

4

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

31

32

33

34

35

36

37

38

39

40

41

42

43

44

45

46

47

48

49

50

51

52

53

54

55

56

57

58

59

60

61

62

63

64

65

66

67

68

69

70

71

72

73

74

75

76

77

78

79

80

81

82

83

84

85

86

87

88

89

90

91

92

93

94

95

96

97

98

99

100

101

102

103

104

105

106

107

108

109

110

111

112

113

114

115

116

117

118

119

120

121

122

123

124

125

126

127

128

129

130

131

132

133

134

135

136

137

138

139

140

141

142

143

144

145

146

147

148

149

150

151

152

153

154

155

156

157

158

159

160

161

162

163

164

165

166

167

168

169

170

171

172

173

174

175

176

177

178

179

180

181

182

183

184

185

186

187

188

189

190

191

192

193

194

195

196

197

198

199

200

201

202

203

204

205

206

207

208

209

210

211

212

213

214

215

216

217

218

219

220

221

222

223

224

225

226

227

228

229

230

231

232

233

234

235

236

237

238

239

240

241

242

243

244

245

246

247

248

249

250

251

252

253

254

255

256

257

258

259

260

261

262

263

264

265

266

267

268

269

270

271

272

273

274

275

276

277

278

279

280

281

282

283

284

285

286

287

288

289

290

291

292

293

294

295

296

297

298

299

300

301

302

303

304

305

306

307

308

309

310

311

312

313

314

315

316

317

318

319

320

321

322

323

324

325

326

327

328

329

330

331

332

333

334

335

336

337

338

339

340

341

342

343

344

345

346

347

348

349

350

351

352

353

354

355

356

357

358

359

360

361

362

363

364

365

366

367

368

369

370

371

372

373

374

375

376

377

378

379

380

381

382

383

384

385

386

387

388

389

390

391

392

393

394

395

396

397

398

399

400

401

402

403

404

405

406

407

408

409

410

411

412

413

414

415

416

417

418

419

420

421

422

423

424

425

426

427

428

429

430

431

432

433

434

435

436

437

438

439

440

441

442

443

444

445

446

447

448

449

450

451

452

453

454

455

456

457

458

459

460

461

462

463

464

465

466

467

468

469

470

471

472

473

474

475

476

477

478

479

480

481

482

483

484

485

486

487

488

489

490

491

492

493

494

495

496

497

498

499

500

501

502

503

504

505

506

507

508

509

510

511

512

513

514

515

516

517

518

519

520

521

522

523

524

525

526

527

528

529

530

531

532

533

534

535

536

537

538

539

540

541

542

543

544

545

546

547

548

549

550

551

552

553

554

555

556

557

558

559

560

561

562

563

564

565

566

567

568

569

570

571

572

573

574

575

576

577

578

579

580

581

582

583

584

585

586

587

588

589

590

591

592

593

594

595

596

597

598

599

600

601

602

603

604

605

606

607

608

609

610

611

612

613

614

615

616

617

618

619

620

621

622

623

624

625

626

627

628

629

630

631

632

633

634

635

636

637

638

639

640

641

642

643

644

645

646

647

648

649

650

651

652

653

654

655

656

657

658

659

660

661

662

663

664

665

666

667

668

669

660

661

662

663

664

665

666

667

668

669

670

671

672

673

674

675

676

677

678

679

680

681

682

683

684

685

686

687

688

689

690

691

692

693

694

695

696

697

698

699

700

701

702

703

704

705

706

707

708

709

710

711

712

713

714

715

716

717

718

719

720

721

722

723

724

725

726

727

728

729

730

731

732

733

734

735

736

737

738

739

730

731

732

733

734

735

736

737

738

739

740

741

742

743

744

745

746

747

748

749

740

741

742

743

744

745

746

747

748

749

750

751

752

753

754

755

756

757

758

759

750

751

752

753

754

755

756

757

758

759

760

761

762

763

764

765

766

767

768

769

760

761

762

763

764

765

766

767

768

769

770

771

772

773

774

775

776

777

778

779

770

771

772

773

774

775

776

777

778

779

780

781

782

783

784

785

786

787

788

789

780

781

782

783

784

785

786

787

788

789

790

791

792

793

794

795

796

797

798

799

790

791

792

793

794

795

796

797

798

799

800

801

802

803

804

805

806

807

808

809

800

801

802

803

804

805

806

807

808

809

810

811

812

813

814

815

816

817

818

819

810

811

812

813

814

815

816

817

818

819

820

821

822

823

824

825

826

827

828

829

820

821

822

823

824

825

826

827

828

829

830

831

832

833

834

835

836

837

838

839

830

831

832

833

834

835

836

837

838

839

840

841

842

843

844

845

846

847

848

849

840

841

842

843

844

845

846

847

848

849

850

851

852

853

854

855

856

857

858

859

850

851

852

853

854

855

856

857

858

859

860

861

862

863

864

865

866

867

868

869

860

861

862

863

864

865

866

867

868

869

870

871

872

873

874

875

876

877

878

879

870

871

872

873

874

875

876

877

878

879

880

881

882

883

884

885

886

887

888

889

880

881

882

883

884

885

886

887

888

889

890

891

892

893

894

895

896

897

898

899

890

891

892

893

894

895

896

897

898

899

900

901

902

903

904

905

906

907

908

909

900

901

902

903

904

905

906

907

908

909

910

911

912

913

914

915

916

917

918

919

910

911

912

913

914

915

916

917

918

919

920

921

922

923

924

925

926

927

928

929

920

921

922

923

924

925

926

927

928

929

930

931

932

933

934

935

936

937

938

939

930

931

932

933

934

935

936

937

938

939

940

941

942

943

944

945

946

947

948

949

940

941

942

943

944

945

946

947

948

949

950

951

952

953

954

955

956

957

958

959

950

951

952

953

954

955

956

957

958

959

960

961

962

963

964

965

966

967

968

969

960

961

962

963

964

965

966

967

968

969

970

971

972

973

974

975

976

977

978

979

970

971

972

973

974

975

976

977

978

979

980

981

982

983

984

985

986

987

988

989

980

981

982

983

984

985

986

987

988

989

990

991

992

993

994

995

996

997

998

999

990

991

992

993

994

995

996

997

998

999

1000

1001

1002

1003

1004

1005

1006

1007

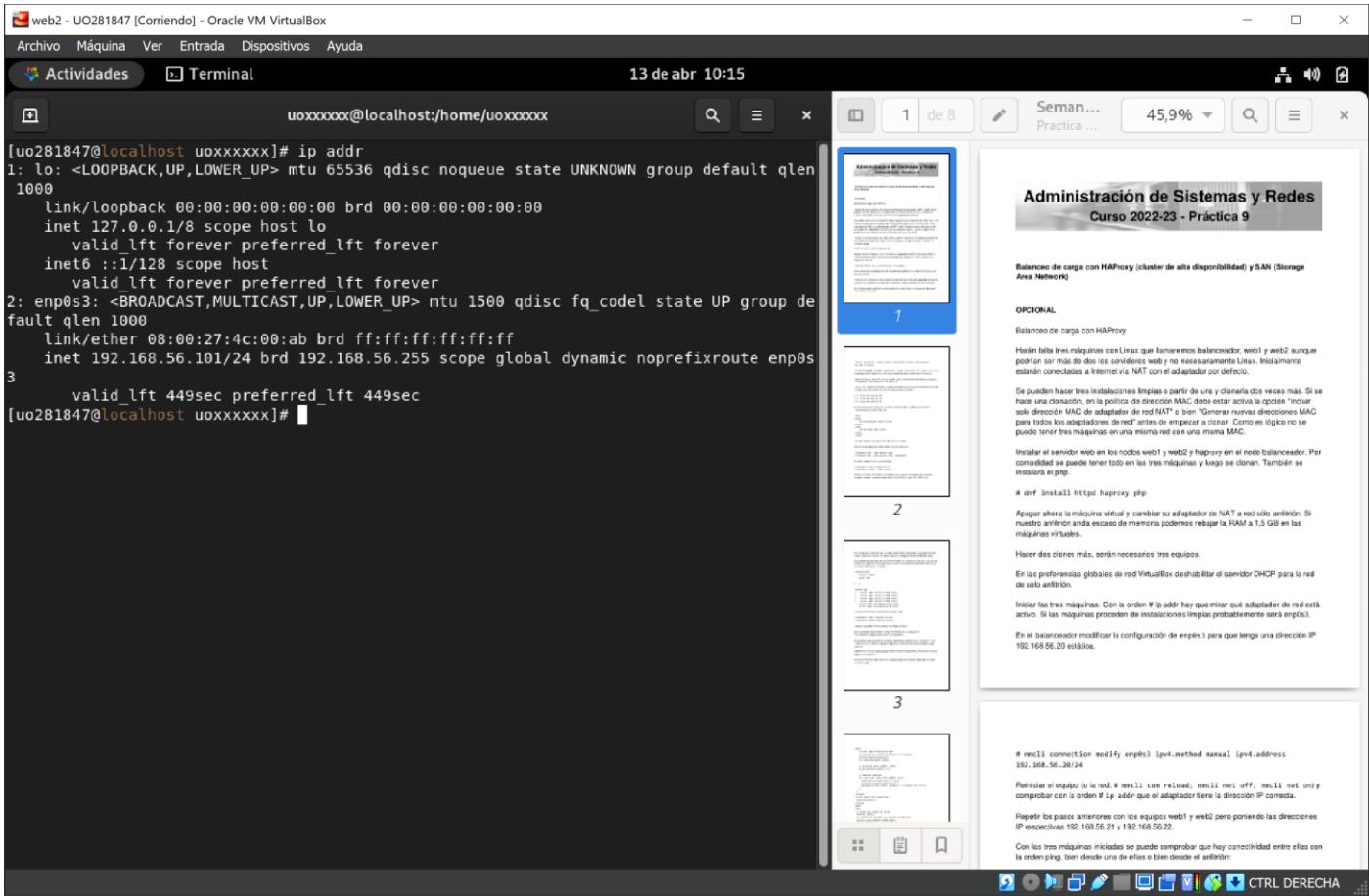
1008

1009

1000

1001

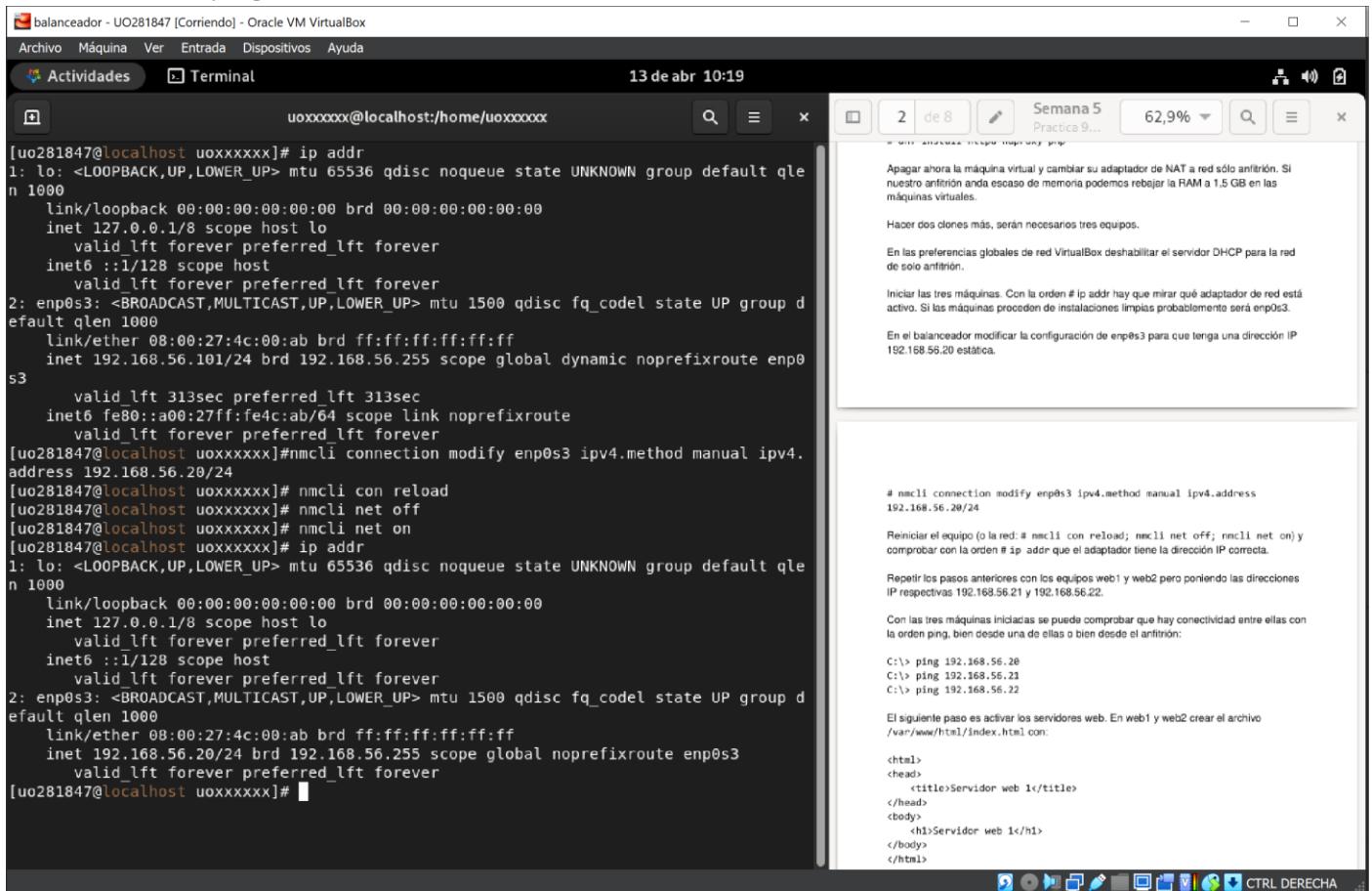
1002</p



3. En el balanceador modificar la configuración de enp0s3 para que tenga una dirección IP 192.168.56.20 estática. Reiniciar el equipo (o la red y comprobar con la orden ip addr que el adaptador tiene la dirección IP correcta).

Repetir los pasos anteriores con los equipos web1 y web2 pero poniendo las direcciones IP respectivas 192.168.56.21 y 192.168.56.22.

Con las tres máquinas iniciadas se puede comprobar que hay conectividad entre ellas con la orden ping, bien desde una de ellas o bien desde el anfitrión:



```

balanceador - UO281847 [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Actividades Terminal 13 de abr 10:19
u0xxxxxx@localhost:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:4c:00:ab brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.20/24 brd 192.168.56.255 scope global dynamic noprefixroute enp0s3
        valid_lft 313sec preferred_lft 313sec
        inet6 fe80::a00:27ff:fe4c:ab%0:4 brd fe80::ff:ff:ff:ff:ff:ff scope link noprefixroute
            valid_lft forever preferred_lft forever
u0xxxxxx@localhost:~$ nmcli connection modify enp0s3 ipv4.method manual ipv4.address 192.168.56.20/24
u0xxxxxx@localhost:~$ nmcli con reload
u0xxxxxx@localhost:~$ nmcli net off
u0xxxxxx@localhost:~$ nmcli net on
u0xxxxxx@localhost:~$ ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:4c:00:ab brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.20/24 brd 192.168.56.255 scope global dynamic noprefixroute enp0s3
        valid_lft forever preferred_lft forever
u0xxxxxx@localhost:~$ 

```

Apagar ahora la máquina virtual y cambiar su adaptador de NAT a red sólo anfitrión. Si nuestro anfitrión anda escaso de memoria podemos rebajar la RAM a 1.5 GB en las máquinas virtuales.

Hacer dos clones más, serán necesarios tres equipos.

En las preferencias globales de red VirtualBox deshabilitar el servidor DHCP para la red sólo anfitrión.

Iniciar las tres máquinas. Con la orden # ip addr hay que mirar qué adaptador de red está activo. Si las máquinas proceden de instalaciones limpias probablemente será enp0s3.

En el balanceador modificar la configuración de enp0s3 para que tenga una dirección IP 192.168.56.20 estática.

nmcli connection modify enp0s3 ipv4.method manual ipv4.address 192.168.56.20/24

Reiniciar el equipo (o la red: # nmcli con reload; nmcli net off; nmcli net on) y comprobar con la orden # ip addr que el adaptador tiene la dirección IP correcta.

Repetir los pasos anteriores con los equipos web1 y web2 pero poniendo las direcciones IP respectivas 192.168.56.21 y 192.168.56.22.

Con las tres máquinas iniciadas se puede comprobar que hay conectividad entre ellas con la orden ping, bien desde una de ellas o bien desde el anfitrión:

```

C:\> ping 192.168.56.20
C:\> ping 192.168.56.21
C:\> ping 192.168.56.22

```

El siguiente paso es activar los servidores web. En web1 y web2 crear el archivo /var/www/html/index.html con:

```

html>
<head>
<title>Servidor web 1</title>
</head>
<body>
<h1>Servidor web 1</h1>
</body>
</html>

```

web1 - UO281847 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Actividades Terminal 13 de abr 10:21

```
u0xxxxx@localhost:~
```

```
[u0281847@localhost u0xxxxx]# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inetc6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:4c:00:ab brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.101/24 brd 192.168.56.255 scope global dynamic noprefixroute enp0s3
        valid_lft 514sec preferred_lft 514sec
[uo281847@localhost u0xxxxx]# nmcli connection modify enp0s3 ipv4.method manual ipv4.address 192.168.56.20/24
[uo281847@localhost u0xxxxx]# nmcli con reload
[uo281847@localhost u0xxxxx]# nmcli net off
[uo281847@localhost u0xxxxx]# nmcli net on
[uo281847@localhost u0xxxxx]# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inetc6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:4c:00:ab brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.21/24 brd 192.168.56.255 scope global dynamic noprefixroute enp0s3
        valid_lft forever preferred_lft forever
[uo281847@localhost u0xxxxx]#
```

En las preferencias globales de red VirtualBox deshabilitar el servidor DHCP para la red de solo anfitrión.

Iniciar las tres máquinas. Con la orden # ip addr hay que mirar qué adaptador de red está activo. Si las máquinas proceden de instalaciones limpias probablemente será enp0s3.

En el balanceador modificar la configuración de enp0s3 para que tenga una dirección IP 192.168.56.20 estática.

web2 - UO281847 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Actividades Terminal 13 de abr 10:22

```
u0xxxxx@localhost:~
```

```
[u0281847@localhost u0xxxxx]# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inetc6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:4c:00:ab brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.101/24 brd 192.168.56.255 scope global dynamic noprefixroute enp0s3
        valid_lft 449sec preferred_lft 449sec
[uo281847@localhost u0xxxxx]# nmcli connection modify enp0s3 ipv4.method manual ipv4.address 192.168.56.22/24
[uo281847@localhost u0xxxxx]# nmcli con reload
[uo281847@localhost u0xxxxx]# nmcli net off
[uo281847@localhost u0xxxxx]# nmcli net on
[uo281847@localhost u0xxxxx]# ip addr
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inetc6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:4c:00:ab brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.22/24 brd 192.168.56.255 scope global dynamic noprefixroute enp0s3
        valid_lft forever preferred_lft forever
    inetc6 fe80::a00:27ff:fe4c:ab/64 scope link tentative noprefixroute
        valid_lft forever preferred_lft forever
[uo281847@localhost u0xxxxx]#
```

estarán conectadas a Internet vía NAT con el adaptador por defecto.

Se pueden hacer tres instalaciones limpias o partir de una y clonarla dos veces más. Si se hace una clonación en la política de dirección MAC debe estar activa la opción "Incluir solo dirección MAC de adaptador de red NAT" o bien "Generar nuevas direcciones MAC para todos los adaptadores de red" antes de empezar a clonar. Como es lógico no se puede tener tres máquinas en una misma red con una misma MAC.

Instalar el servidor web en los nodos web1 y web2 y haproxy en el nodo balanceador. Por comodidad se puede tener todo en las tres máquinas y luego se clonan. También se instalará el php.

dnf install httpd haproxy php

Apagar ahora la máquina virtual y cambiar su adaptador de NAT a red sólo anfitrión. Si nuestro anfitrión anda escaso de memoria podemos rebajar la RAM a 1.5 GB en las máquinas virtuales.

Crear dos clones más, serán necesarios tres equipos.

En las preferencias globales de red VirtualBox deshabilitar el servidor DHCP para la red de solo anfitrión.

Iniciar las tres máquinas. Con la orden # ip addr hay que mirar qué adaptador de red está activo. Si las máquinas proceden de instalaciones limpias probablemente será enp0s3.

En el balanceador modificar la configuración de enp0s3 para que tenga una dirección IP 192.168.56.20 estática.

balanceador - UO281847 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Actividades Terminal 13 de abr 10:25

```
uoxxxxxx@localhost:home/uoxxxxxx
```

```

64 bytes from 192.168.56.20: icmp_seq=8 ttl=64 time=0.072 ms
64 bytes from 192.168.56.20: icmp_seq=9 ttl=64 time=0.087 ms
64 bytes from 192.168.56.20: icmp_seq=10 ttl=64 time=0.067 ms
64 bytes from 192.168.56.20: icmp_seq=11 ttl=64 time=0.033 ms
64 bytes from 192.168.56.20: icmp_seq=12 ttl=64 time=0.075 ms
^C
--- 192.168.56.20 ping statistics ---
12 packets transmitted, 12 received, 0% packet loss, time 11257ms
rtt min/avg/max/mdev = 0.033/0.078/0.112/0.021 ms
[uo281847@localhost uoxxxxxx]# ping 192.168.56.21
PING 192.168.56.21 (192.168.56.21) 56(84) bytes of data.
64 bytes from 192.168.56.21: icmp_seq=1 ttl=64 time=0.827 ms
64 bytes from 192.168.56.21: icmp_seq=2 ttl=64 time=1.05 ms
64 bytes from 192.168.56.21: icmp_seq=3 ttl=64 time=0.794 ms
64 bytes from 192.168.56.21: icmp_seq=4 ttl=64 time=0.562 ms
64 bytes from 192.168.56.21: icmp_seq=5 ttl=64 time=0.942 ms
64 bytes from 192.168.56.21: icmp_seq=6 ttl=64 time=0.783 ms
64 bytes from 192.168.56.21: icmp_seq=7 ttl=64 time=1.17 ms
64 bytes from 192.168.56.21: icmp_seq=8 ttl=64 time=0.788 ms
64 bytes from 192.168.56.21: icmp_seq=9 ttl=64 time=1.17 ms
^C
--- 192.168.56.21 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8190ms
rtt min/avg/max/mdev = 0.562/0.898/1.170/0.190 ms
[uo281847@localhost uoxxxxxx]# ping 192.168.56.22
PING 192.168.56.22 (192.168.56.22) 56(84) bytes of data.
64 bytes from 192.168.56.22: icmp_seq=1 ttl=64 time=1.21 ms
64 bytes from 192.168.56.22: icmp_seq=2 ttl=64 time=1.05 ms
64 bytes from 192.168.56.22: icmp_seq=3 ttl=64 time=0.761 ms
64 bytes from 192.168.56.22: icmp_seq=4 ttl=64 time=0.722 ms
64 bytes from 192.168.56.22: icmp_seq=5 ttl=64 time=0.918 ms
64 bytes from 192.168.56.22: icmp_seq=6 ttl=64 time=0.846 ms
64 bytes from 192.168.56.22: icmp_seq=7 ttl=64 time=0.916 ms
^C
--- 192.168.56.22 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6117ms
rtt min/avg/max/mdev = 0.722/0.918/1.212/0.157 ms
[uo281847@localhost uoxxxxxx]#

```

2 de 8 Semana 5 Practica 9...

62,9% Apagar ahora la máquina virtual y cambiar su adaptador de NAT a red sólo anfitrión. Si nuestro anfitrión anda escaso de memoria podemos rebajar la RAM a 1.5 GB en las máquinas virtuales.

Hacer dos clones más, serán necesarios tres equipos.

En las preferencias globales de red VirtualBox deshabilitar el servidor DHCP para la red de solo anfitrión.

Iniciar las tres máquinas. Con la orden # ip addr hay que mirar qué adaptador de red está activo. Si las máquinas proceden de instalaciones limpias probablemente será enp0s3.

En el balanceador modificar la configuración de enp0s3 para que tenga una dirección IP 192.168.56.20 estática.

nmcli connection modify enp0s3 ipv4.method manual ipv4.address 192.168.56.20/24

Reiniciar el equipo (o la red: # nmcli con reload; nmcli net off; nmcli net on) y comprobar con la orden # ip addr que el adaptador tiene la dirección IP correcta.

Repetir los pasos anteriores con los equipos web1 y web2 pero poniendo las direcciones IP respectivas 192.168.56.21 y 192.168.56.22.

Con las tres máquinas iniciadas se puede comprobar que hay conectividad entre ellas con la orden ping, bien desde una de ellas o bien desde el anfitrión:

```
C:\> ping 192.168.56.20
C:\> ping 192.168.56.21
C:\> ping 192.168.56.22
```

El siguiente paso es activar los servidores web. En web1 y web2 crear el archivo /var/www/html/index.html con:

```
<html>
<head>
<title>Servidor web 1</title>
</head>
<body>
<h1>Servidor web 1</h1>
</body>
</html>
```

CTRL DERECHA

web1 - UO281847 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Actividades Terminal 13 de abr 10:23

```
uoxxxxxx@localhost:home/uoxxxxxx
```

```

PING 192.168.56.20 (192.168.56.20) 56(84) bytes of data.
64 bytes from 192.168.56.20: icmp_seq=1 ttl=64 time=1.44 ms
64 bytes from 192.168.56.20: icmp_seq=2 ttl=64 time=0.937 ms
64 bytes from 192.168.56.20: icmp_seq=3 ttl=64 time=1.03 ms
64 bytes from 192.168.56.20: icmp_seq=4 ttl=64 time=1.05 ms
64 bytes from 192.168.56.20: icmp_seq=5 ttl=64 time=1.09 ms
64 bytes from 192.168.56.20: icmp_seq=6 ttl=64 time=1.16 ms
64 bytes from 192.168.56.20: icmp_seq=7 ttl=64 time=1.19 ms
64 bytes from 192.168.56.20: icmp_seq=8 ttl=64 time=0.987 ms
64 bytes from 192.168.56.20: icmp_seq=9 ttl=64 time=0.464 ms
^C
--- 192.168.56.20 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8007ms
rtt min/avg/max/mdev = 0.464/1.037/1.440/0.245 ms
[uo281847@localhost uoxxxxxx]# ping 192.168.56.21
PING 192.168.56.21 (192.168.56.21) 56(84) bytes of data.
64 bytes from 192.168.56.21: icmp_seq=1 ttl=64 time=0.104 ms
64 bytes from 192.168.56.21: icmp_seq=2 ttl=64 time=0.078 ms
64 bytes from 192.168.56.21: icmp_seq=3 ttl=64 time=0.097 ms
64 bytes from 192.168.56.21: icmp_seq=4 ttl=64 time=0.088 ms
64 bytes from 192.168.56.21: icmp_seq=5 ttl=64 time=0.069 ms
64 bytes from 192.168.56.21: icmp_seq=6 ttl=64 time=0.061 ms
64 bytes from 192.168.56.21: icmp_seq=7 ttl=64 time=0.104 ms
^C
--- 192.168.56.21 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6181ms
rtt min/avg/max/mdev = 0.061/0.085/0.104/0.015 ms
[uo281847@localhost uoxxxxxx]# ping 192.168.56.22
PING 192.168.56.22 (192.168.56.22) 56(84) bytes of data.
64 bytes from 192.168.56.22: icmp_seq=1 ttl=64 time=1.34 ms
64 bytes from 192.168.56.22: icmp_seq=2 ttl=64 time=0.554 ms
64 bytes from 192.168.56.22: icmp_seq=3 ttl=64 time=0.967 ms
64 bytes from 192.168.56.22: icmp_seq=4 ttl=64 time=0.634 ms
64 bytes from 192.168.56.22: icmp_seq=5 ttl=64 time=0.943 ms
64 bytes from 192.168.56.22: icmp_seq=6 ttl=64 time=0.617 ms
^Z
[1]+  Detenido                  ping 192.168.56.22
[uo281847@localhost uoxxxxxx]#

```

2 de 8 Semana 5 Practica ...

62,7% En las preferencias globales de red VirtualBox deshabilitar el servidor DHCP para la red de solo anfitrión.

Iniciar las tres máquinas. Con la orden # ip addr hay que mirar qué adaptador de red está activo. Si las máquinas proceden de instalaciones limpias probablemente será enp0s3.

En el balanceador modificar la configuración de enp0s3 para que tenga una dirección IP 192.168.56.20 estática.

nmcli connection modify enp0s3 ipv4.method manual ipv4.address 192.168.56.20/24

Reiniciar el equipo (o la red: # nmcli con reload; nmcli net off; nmcli net on) y comprobar con la orden # ip addr que el adaptador tiene la dirección IP correcta.

Repetir los pasos anteriores con los equipos web1 y web2 pero poniendo las direcciones IP respectivas 192.168.56.21 y 192.168.56.22.

Con las tres máquinas iniciadas se puede comprobar que hay conectividad entre ellas con la orden ping, bien desde una de ellas o bien desde el anfitrión:

```
C:\> ping 192.168.56.20
C:\> ping 192.168.56.21
C:\> ping 192.168.56.22
```

El siguiente paso es activar los servidores web. En web1 y web2 crear el archivo /var/www/html/index.html con:

```
<html>
<head>
<title>Servidor web 1</title>
</head>
<body>
<h1>Servidor web 1</h1>
</body>
</html>
```

Hay que acordarse de poner "Servidor web 2" en web2.

Abrir el cortafuegos para tráfico web en las tres máquinas:

```
# Firewall-cmd --add-service http
# Firewall-cmd --add-service http --permanent
```

CTRL DERECHA

web2 - UO281847 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Actividades Terminal 13 de abr 10:26

```
u0xxxxx@localhost:home/u0xxxxx
```

```
64 bytes from 192.168.56.20: icmp_seq=3 ttl=64 time=0.906 ms
64 bytes from 192.168.56.20: icmp_seq=4 ttl=64 time=0.550 ms
64 bytes from 192.168.56.20: icmp_seq=5 ttl=64 time=1.03 ms
64 bytes from 192.168.56.20: icmp_seq=6 ttl=64 time=0.928 ms
64 bytes from 192.168.56.20: icmp_seq=7 ttl=64 time=0.440 ms
^C
--- 192.168.56.20 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6041ms
rtt min/avg/max/mdev = 0.440/0.787/1.032/0.205 ms
[uo281847@localhost u0xxxxxx]# ping 192.168.56.21
PING 192.168.56.21 (192.168.56.21) 56(84) bytes of data.
64 bytes from 192.168.56.21: icmp_seq=1 ttl=64 time=0.879 ms
64 bytes from 192.168.56.21: icmp_seq=2 ttl=64 time=0.986 ms
64 bytes from 192.168.56.21: icmp_seq=3 ttl=64 time=0.929 ms
64 bytes from 192.168.56.21: icmp_seq=4 ttl=64 time=1.03 ms
64 bytes from 192.168.56.21: icmp_seq=5 ttl=64 time=1.08 ms
64 bytes from 192.168.56.21: icmp_seq=6 ttl=64 time=0.833 ms
64 bytes from 192.168.56.21: icmp_seq=7 ttl=64 time=0.518 ms
64 bytes from 192.168.56.21: icmp_seq=8 ttl=64 time=0.863 ms
^C
--- 192.168.56.21 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7055ms
rtt min/avg/max/mdev = 0.518/0.890/1.082/0.162 ms
[uo281847@localhost u0xxxxxx]# ping 192.168.56.22
PING 192.168.56.22 (192.168.56.22) 56(84) bytes of data.
64 bytes from 192.168.56.22: icmp_seq=1 ttl=64 time=0.053 ms
64 bytes from 192.168.56.22: icmp_seq=2 ttl=64 time=0.102 ms
64 bytes from 192.168.56.22: icmp_seq=3 ttl=64 time=0.100 ms
64 bytes from 192.168.56.22: icmp_seq=4 ttl=64 time=0.099 ms
64 bytes from 192.168.56.22: icmp_seq=5 ttl=64 time=0.058 ms
64 bytes from 192.168.56.22: icmp_seq=6 ttl=64 time=0.089 ms
64 bytes from 192.168.56.22: icmp_seq=7 ttl=64 time=0.083 ms
64 bytes from 192.168.56.22: icmp_seq=8 ttl=64 time=0.086 ms
^C
--- 192.168.56.22 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7192ms
rtt min/avg/max/mdev = 0.053/0.083/0.102/0.017 ms
[uo281847@localhost u0xxxxxx]#
```

62,7% Seman... Practica ... 1 de 8

estarán conectadas a Internet vía NAT con el adaptador por defecto.

Se pueden hacer tres instalaciones limpias o partir de una y clonarla dos veces más. Si se hace una clonación, en la política de dirección MAC debe estar activa la opción "Incluir solo dirección MAC de adaptador de red NAT" o bien "Generar nuevas direcciones MAC para todos los adaptadores de red" antes de empezar a clonar. Como es lógico no se puede tener tres máquinas en una misma red con una misma MAC.

Instalar el servidor web en los nodos web1 y web2 y haproxy en el nodo balanceador. Por comodidad se puede tener todo en las tres máquinas y luego se clonen. También se instalará el php.

dnf install httpd haproxy php

Apagar ahora la máquina virtual y cambiar su adaptador de red sólo anfitrión. Si nuestro anfitrión anda escaso de memoria podemos rebajar la RAM a 1.5 GB en las máquinas virtuales.

Hacer los clones más, serán necesarios tres equipos.

En las preferencias globales de red VirtualBox deshabilitar el servidor DHCP para la red de sólo anfitrión.

Iniciar las tres máquinas. Con la orden # ip addr hay que mirar qué adaptador de red está activo. Si las máquinas proceden de instalaciones limpias probablemente será enp0s3.

En el balanceador modificar la configuración de enp0s3 para que tenga una dirección IP 192.168.56.20 estática.

nmcli connection modify enp0s3 ipv4.method manual ipv4.address 192.168.56.20/24

Reiniciar el equipo (o la red: # nmcli con reload; nmcli net off; nmcli net on) y comprobar con la orden # ip addr que el adaptador tiene la dirección IP correcta.

Repetir los pasos anteriores con los equipos web1 y web2 pero poniendo las direcciones IP respectivas 192.168.56.21 y 192.168.56.22.

Con las tres máquinas iniciadas se puede comprobar que hay conectividad entre ellas con la orden ping, bien desde una de ellas o bien desde el anfitrión:

C:\> ping 192.168.56.20
C:\> ping 192.168.56.21
C:\> ping 192.168.56.22

CTRL DERECHA

4. El siguiente paso es activar los servidores web. En web1 y web2 crear el archivo. Hay que acordarse de poner "Servidor web 2" en web2.

web1 - UO281847 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Actividades Terminal 13 de abr 10:28

```
u0xxxxx@localhost:home/u0xxxxx — nano -c /var/www/html/index.html
```

```
GNU nano 5.6.1 /var/www/html/index.html
```

```
<html>
<head>
  <title>Servidor web 1</title>
</head>
<body>
  <h1>Servidor web 1</h1>
</body>
</html>
```

8 líneas escritas

^6 Ayuda ^O Guardar ^W Buscar ^K Cortar ^T Ejecutar ^C Ubicación
^X Salir ^R Leer fich. ^\ Reemplazar ^U Pegar ^J Justificar ^I Ir a línea

62,7% Seman... Practica ... 2 de 8

En las preferencias globales de red VirtualBox deshabilitar el servidor DHCP para la red de sólo anfitrión.

Iniciar las tres máquinas. Con la orden # ip addr hay que mirar qué adaptador de red está activo. Si las máquinas proceden de instalaciones limpias probablemente será enp0s3.

En el balanceador modificar la configuración de enp0s3 para que tenga una dirección IP 192.168.56.20 estática.

nmcli connection modify enp0s3 ipv4.method manual ipv4.address 192.168.56.20/24

Reiniciar el equipo (o la red: # nmcli con reload; nmcli net off; nmcli net on) y comprobar con la orden # ip addr que el adaptador tiene la dirección IP correcta.

Repetir los pasos anteriores con los equipos web1 y web2 pero poniendo las direcciones IP respectivas 192.168.56.21 y 192.168.56.22.

Con las tres máquinas iniciadas se puede comprobar que hay conectividad entre ellas con la orden ping, bien desde una de ellas o bien desde el anfitrión:

C:\> ping 192.168.56.20
C:\> ping 192.168.56.21
C:\> ping 192.168.56.22

El siguiente paso es activar los servidores web. En web1 y web2 crear el archivo /var/www/html/index.html con:

```
<html>
<head>
  <title>Servidor web 1</title>
</head>
<body>
  <h1>Servidor web 1</h1>
</body>
</html>
```

Hay que acordarse de poner "Servidor web 2" en web2.

Abrir el cortafuegos para tráfico web en las tres máquinas:

```
# firewall-cmd --add-service http
# firewall-cmd --add-service http --permanent
```

CTRL DERECHA

web2 - UO281847 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Actividades Terminal 13 de abr 10:29

```
uoxxxxxx@localhost:/home/uoxxxxxx — nano -c /var/www/html/index.html
```

GNU nano 5.6.1 /var/www/html/index.html

```
<html>
<head>
    <title>Servidor web 1</title>
</head>
<body>
    <h1>Servidor web 1</h1>
</body>
</html>
```

Hacer dos clones más, serán necesarios tres equipos.

En las preferencias globales de red VirtualBox deshabilitar el servidor DHCP para la red de solo anfitrión.

Iniciar las tres máquinas. Con la orden # ip addr hay que mirar qué adaptador de red está activo. Si las máquinas proceden de instalaciones limpias probablemente será enp0s3.

En el balanceador modificar la configuración de enp0s3 para que tenga una dirección IP 192.168.56.20 estática.

nmcli connection modify enp0s3 ipv4.method manual ipv4.address 192.168.56.20/24

Reiniciar el equipo (o la red # nmcli con reload; nmcli net off; nmcli net on) y comprobar con la orden # ip addr que el adaptador tiene la dirección IP correcta.

Repetir los pasos anteriores con los equipos web1 y web2 pero poniendo las direcciones IP respectivas 192.168.56.21 y 192.168.56.22.

Con las tres máquinas iniciadas se puede comprobar que hay conectividad entre ellas con la orden ping, bien desde una de ellas o bien desde el anfitrión:

```
C:\> ping 192.168.56.20
C:\> ping 192.168.56.21
C:\> ping 192.168.56.22
```

El siguiente paso es activar los servidores web. En web1 y web2 crear el archivo /var/www/html/index.html con:

```
<html>
<head>
    <title>Servidor web 1</title>
</head>
<body>
    <h1>Servidor web 1</h1>
</body>
</html>
```

Hay que acordarse de poner "Servidor web 2" en web2.

Abrir el cortafuegos para tráfico web en las tres máquinas:

CTRL DERECHA

[8 líneas leidas]

^6 Ayuda ^0 Guardar ^W Buscar ^K Cortar ^T Ejecutar ^C Ubicación
 ^X Salir ^R Leer fich. ^\ Reemplazar ^U Pegar ^J Justificar ^_ Ir a línea

web2 - UO281847 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Actividades Terminal 13 de abr 10:30

```
uoxxxxxx@localhost:/home/uoxxxxxx — nano -c /var/www/html/index.html
```

GNU nano 5.6.1 /var/www/html/index.html

```
<html>
<head>
    <title>Servidor web 2</title>
</head>
<body>
    <h1>Servidor web 2</h1>
</body>
</html>
```

Hacer dos clones más, serán necesarios tres equipos.

En las preferencias globales de red VirtualBox deshabilitar el servidor DHCP para la red de solo anfitrión.

Iniciar las tres máquinas. Con la orden # ip addr hay que mirar qué adaptador de red está activo. Si las máquinas proceden de instalaciones limpias probablemente será enp0s3.

En el balanceador modificar la configuración de enp0s3 para que tenga una dirección IP 192.168.56.20 estática.

nmcli connection modify enp0s3 ipv4.method manual ipv4.address 192.168.56.20/24

Reiniciar el equipo (o la red # nmcli con reload; nmcli net off; nmcli net on) y comprobar con la orden # ip addr que el adaptador tiene la dirección IP correcta.

Repetir los pasos anteriores con los equipos web1 y web2 pero poniendo las direcciones IP respectivas 192.168.56.21 y 192.168.56.22.

Con las tres máquinas iniciadas se puede comprobar que hay conectividad entre ellas con la orden ping, bien desde una de ellas o bien desde el anfitrión:

```
C:\> ping 192.168.56.20
C:\> ping 192.168.56.21
C:\> ping 192.168.56.22
```

El siguiente paso es activar los servidores web. En web1 y web2 crear el archivo /var/www/html/index.html con:

```
<html>
<head>
    <title>Servidor web 1</title>
</head>
<body>
    <h1>Servidor web 1</h1>
</body>
</html>
```

Hay que acordarse de poner "Servidor web 2" en web2.

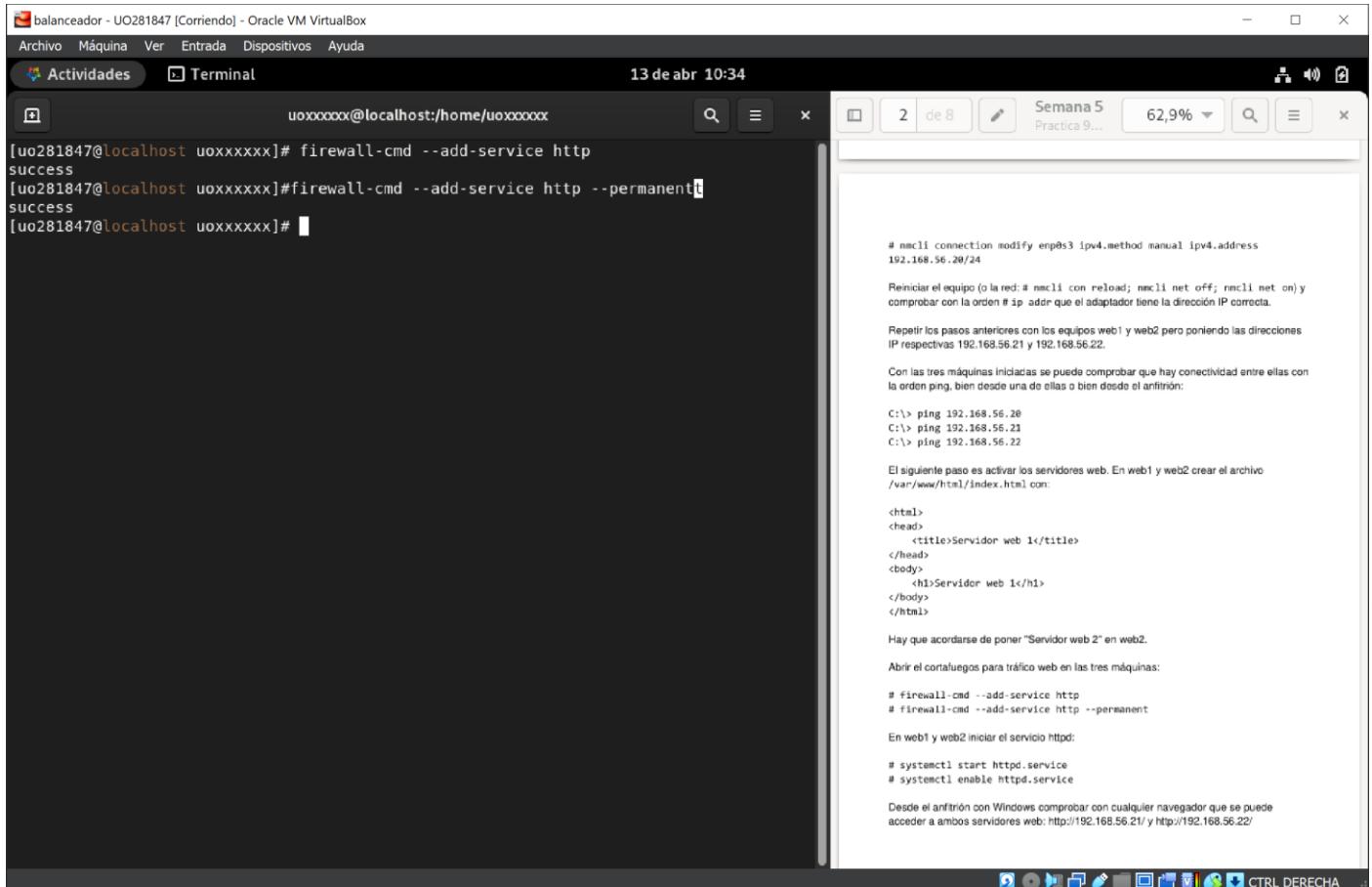
Abrir el cortafuegos para tráfico web en las tres máquinas:

CTRL DERECHA

[8 líneas escritas]

^6 Ayuda ^0 Guardar ^W Buscar ^K Cortar ^T Ejecutar ^C Ubicación
 ^X Salir ^R Leer fich. ^\ Reemplazar ^U Pegar ^J Justificar ^_ Ir a línea

5. Abrir el cortafuegos para tráfico web en las tres máquinas:



```

balanceador - UO281847 [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Actividades Terminal 13 de abr 10:34
u0xxxxxx@localhost:~$ firewall-cmd --add-service http
success
u0xxxxxx@localhost:~$ firewall-cmd --add-service http --permanent
success
u0xxxxxx@localhost:~$ 

# nmcli connection modify enp0s3 ipv4.method manual ipv4.address
192.168.56.20/24

Reiniclar el equipo (o la red: # nmcli con reload; nmcli net off; nmcli net on) y
comprobar con la orden # ip addr que el adaptador tiene la dirección IP correcta.

Repetir los pasos anteriores con los equipos web1 y web2 pero poniendo las direcciones
IP respectivas 192.168.56.21 y 192.168.56.22.

Con las tres máquinas iniciadas se puede comprobar que hay conectividad entre ellas con
la orden ping, bien desde una de ellas o bien desde el anfitrión:
C:\> ping 192.168.56.20
C:\> ping 192.168.56.21
C:\> ping 192.168.56.22

El siguiente paso es activar los servidores web. En web1 y web2 crear el archivo
/var/www/html/index.html con:
<html>
<head>
<title>Servidor web 1</title>
</head>
<body>
<h1>Servidor web 1</h1>
</body>
</html>

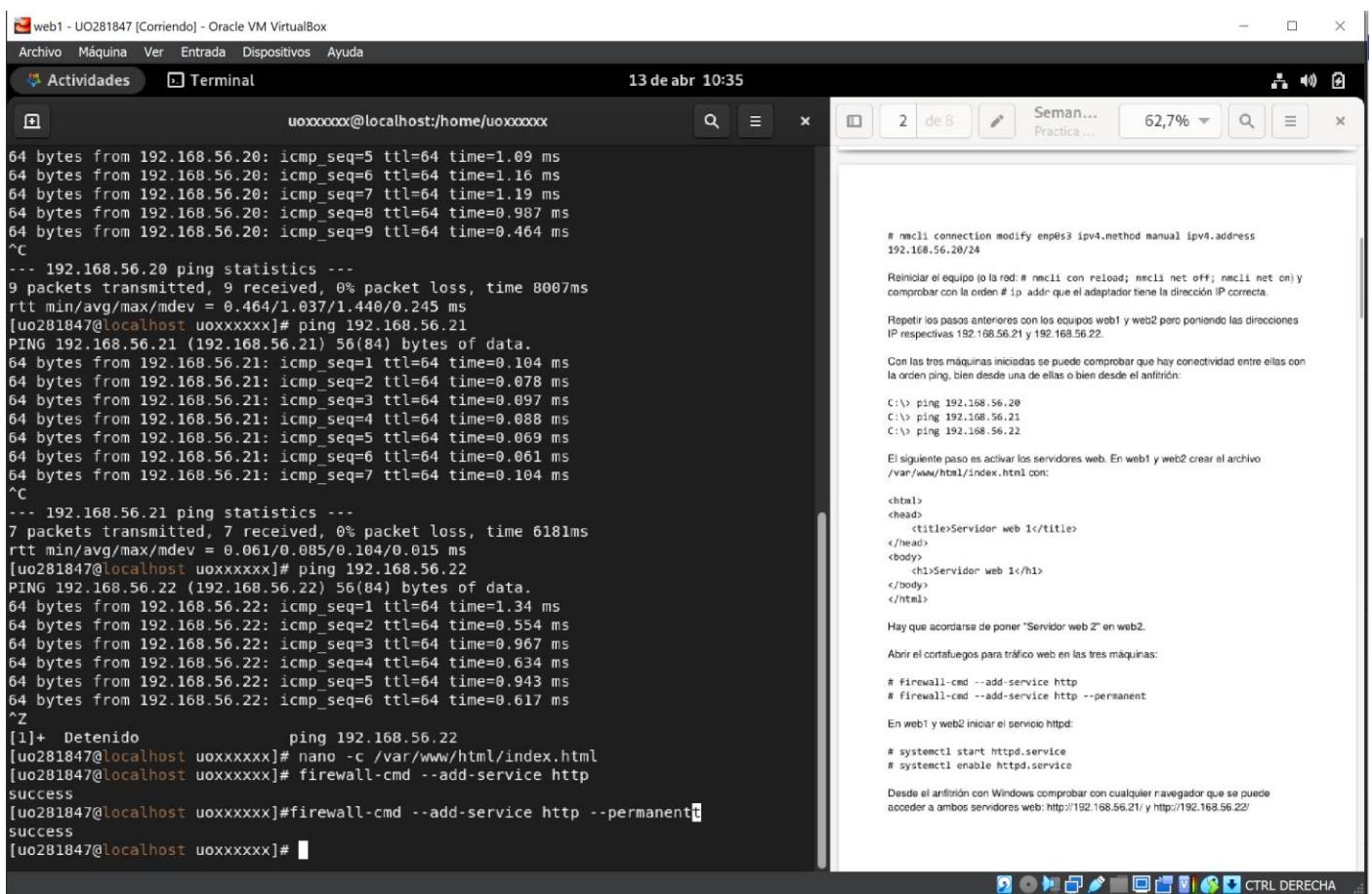
Hay que acordarse de poner "Servidor web 2" en web2.

Abrir el cortafuegos para tráfico web en las tres máquinas:
# firewall-cmd --add-service http
# firewall-cmd --add-service http --permanent

En web1 y web2 iniciar el servicio httpd:
# systemctl start httpd.service
# systemctl enable httpd.service

Desde el anfitrión con Windows comprobar con cualquier navegador que se puede
acceder a ambos servidores web: http://192.168.56.21/ y http://192.168.56.22/

```



```

web1 - UO281847 [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Actividades Terminal 13 de abr 10:35
u0xxxxxx@localhost:~$ ping 192.168.56.21
PING 192.168.56.21 (192.168.56.21) 56(84) bytes of data.
64 bytes from 192.168.56.21: icmp_seq=1 ttl=64 time=0.104 ms
64 bytes from 192.168.56.21: icmp_seq=2 ttl=64 time=0.078 ms
64 bytes from 192.168.56.21: icmp_seq=3 ttl=64 time=0.097 ms
64 bytes from 192.168.56.21: icmp_seq=4 ttl=64 time=0.088 ms
64 bytes from 192.168.56.21: icmp_seq=5 ttl=64 time=0.069 ms
64 bytes from 192.168.56.21: icmp_seq=6 ttl=64 time=0.061 ms
64 bytes from 192.168.56.21: icmp_seq=7 ttl=64 time=0.104 ms
^C
--- 192.168.56.21 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8007ms
rtt min/avg/max/mdev = 0.061/0.1037/1.440/0.245 ms
u0xxxxxx@localhost:~$ ping 192.168.56.22
PING 192.168.56.22 (192.168.56.22) 56(84) bytes of data.
64 bytes from 192.168.56.22: icmp_seq=1 ttl=64 time=1.34 ms
64 bytes from 192.168.56.22: icmp_seq=2 ttl=64 time=0.554 ms
64 bytes from 192.168.56.22: icmp_seq=3 ttl=64 time=0.967 ms
64 bytes from 192.168.56.22: icmp_seq=4 ttl=64 time=0.634 ms
64 bytes from 192.168.56.22: icmp_seq=5 ttl=64 time=0.943 ms
64 bytes from 192.168.56.22: icmp_seq=6 ttl=64 time=0.617 ms
^Z
[1]+  Detenido                  ping 192.168.56.22
u0xxxxxx@localhost:~$ nano -c /var/www/html/index.html
u0xxxxxx@localhost:~$ firewall-cmd --add-service http
success
u0xxxxxx@localhost:~$ firewall-cmd --add-service http --permanent
success
u0xxxxxx@localhost:~$ 

# nmcli connection modify enp0s3 ipv4.method manual ipv4.address
192.168.56.20/24

Reiniclar el equipo (o la red: # nmcli con reload; nmcli net off; nmcli net on) y
comprobar con la orden # ip addr que el adaptador tiene la dirección IP correcta.

Repetir los pasos anteriores con los equipos web1 y web2 pero poniendo las direcciones
IP respectivas 192.168.56.21 y 192.168.56.22.

Con las tres máquinas iniciadas se puede comprobar que hay conectividad entre ellas con
la orden ping, bien desde una de ellas o bien desde el anfitrión:
C:\> ping 192.168.56.20
C:\> ping 192.168.56.21
C:\> ping 192.168.56.22

El siguiente paso es activar los servidores web. En web1 y web2 crear el archivo
/var/www/html/index.html con:
<html>
<head>
<title>Servidor web 1</title>
</head>
<body>
<h1>Servidor web 1</h1>
</body>
</html>

Hay que acordarse de poner "Servidor web 2" en web2.

Abrir el cortafuegos para tráfico web en las tres máquinas:
# firewall-cmd --add-service http
# firewall-cmd --add-service http --permanent

En web1 y web2 iniciar el servicio httpd:
# systemctl start httpd.service
# systemctl enable httpd.service

Desde el anfitrión con Windows comprobar con cualquier navegador que se puede
acceder a ambos servidores web: http://192.168.56.21/ y http://192.168.56.22/

```

```

web2 - UO281847 [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Actividades Terminal 13 de abr 10:36
u0xxxxx@localhost:home/u0xxxxx
44 bytes from 192.168.56.21: icmp_seq=2 ttl=64 time=0.986 ms
44 bytes from 192.168.56.21: icmp_seq=3 ttl=64 time=0.929 ms
44 bytes from 192.168.56.21: icmp_seq=4 ttl=64 time=1.03 ms
44 bytes from 192.168.56.21: icmp_seq=5 ttl=64 time=1.08 ms
44 bytes from 192.168.56.21: icmp_seq=6 ttl=64 time=0.833 ms
44 bytes from 192.168.56.21: icmp_seq=7 ttl=64 time=0.518 ms
44 bytes from 192.168.56.21: icmp_seq=8 ttl=64 time=0.863 ms
^C
--- 192.168.56.21 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7055ms
rtt min/avg/max/mdev = 0.518/0.890/1.082/0.162 ms
[uo281847@localhost u0xxxxxx]# ping 192.168.56.22
PING 192.168.56.22 (192.168.56.22) 56(84) bytes of data.
44 bytes from 192.168.56.22: icmp_seq=1 ttl=64 time=0.053 ms
44 bytes from 192.168.56.22: icmp_seq=2 ttl=64 time=0.102 ms
44 bytes from 192.168.56.22: icmp_seq=3 ttl=64 time=0.100 ms
44 bytes from 192.168.56.22: icmp_seq=4 ttl=64 time=0.099 ms
44 bytes from 192.168.56.22: icmp_seq=5 ttl=64 time=0.058 ms
44 bytes from 192.168.56.22: icmp_seq=6 ttl=64 time=0.089 ms
44 bytes from 192.168.56.22: icmp_seq=7 ttl=64 time=0.083 ms
44 bytes from 192.168.56.22: icmp_seq=8 ttl=64 time=0.086 ms
^C
--- 192.168.56.22 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7192ms
rtt min/avg/max/mdev = 0.053/0.083/0.102/0.017 ms
[uo281847@localhost u0xxxxxx]# nano -c /var/www/html/index.html
[uo281847@localhost u0xxxxxx]# nano -c /var/www/html/index.html
[uo281847@localhost u0xxxxxx]# firewall-cmd --add-service http
success
[uo281847@localhost u0xxxxxx]# firewall-cmd --add-service http
Warning: ALREADY_ENABLED: 'http' already in 'public'
success
[uo281847@localhost u0xxxxxx]# firewall-cmd --add-service http
Warning: ALREADY_ENABLED: 'http' already in 'public'
success
[uo281847@localhost u0xxxxxx]# firewall-cmd --add-service http --permanent
success
[uo281847@localhost u0xxxxxx]# 

```

nmcli connection modify enp0s3 ipv4.method manual ipv4.address 192.168.56.24

Reiniclar el equipo (o la red: # nmcli con reload; nmcli net off; nmcli net on) y comprobar con la orden # ip addr que el adaptador tiene la dirección IP correcta.

Repetir los pasos anteriores con los equipos web1 y web2 pero poniendo las direcciones IP respectivas 192.168.56.21 y 192.168.56.22.

Con las tres máquinas iniciadas se puede comprobar que hay conectividad entre ellas con la orden ping, bien desde una de ellas o bien desde el anfitrión:

```

C:\> ping 192.168.56.20
C:\> ping 192.168.56.21
C:\> ping 192.168.56.22

```

El siguiente paso es activar los servidores web. En web1 y web2 crear el archivo /var/www/html/index.html:

```

<html>
<head>
<title>Servidor web 1</title>
</head>
<body>
<h1>Servidor web 1</h1>
</body>
</html>

```

Hay que acordarse de poner "Servidor web 2" en web2.

Abrir el cortafuegos para tráfico web en las tres máquinas:

```

# firewall-cmd --add-service http
# firewall-cmd --add-service http --permanent

```

En web1 y web2 iniciar el servicio httpd:

```

# systemctl start httpd.service
# systemctl enable httpd.service

```

Desde el anfitrión con Windows comprobar con cualquier navegador que se puede acceder a ambos servidores web: http://192.168.56.21/ y http://192.168.56.22/

6. En web1 y web2 iniciar el servicio httpd:

```

web1 - UO281847 [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Actividades Visor de documentos 13 de abr 10:36
u0xxxxx@localhost:home/u0xxxxx
44 bytes from 192.168.56.20: icmp_seq=9 ttl=64 time=0.464 ms
^C
--- 192.168.56.20 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8007ms
rtt min/avg/max/mdev = 0.464/1.037/1.440/0.245 ms
[uo281847@localhost u0xxxxxx]# ping 192.168.56.21
PING 192.168.56.21 (192.168.56.21) 56(84) bytes of data.
64 bytes from 192.168.56.21: icmp_seq=1 ttl=64 time=0.104 ms
64 bytes from 192.168.56.21: icmp_seq=2 ttl=64 time=0.078 ms
64 bytes from 192.168.56.21: icmp_seq=3 ttl=64 time=0.097 ms
64 bytes from 192.168.56.21: icmp_seq=4 ttl=64 time=0.088 ms
64 bytes from 192.168.56.21: icmp_seq=5 ttl=64 time=0.069 ms
64 bytes from 192.168.56.21: icmp_seq=6 ttl=64 time=0.061 ms
64 bytes from 192.168.56.21: icmp_seq=7 ttl=64 time=0.104 ms
^C
--- 192.168.56.21 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6181ms
rtt min/avg/max/mdev = 0.061/0.085/0.104/0.015 ms
[uo281847@localhost u0xxxxxx]# ping 192.168.56.22
PING 192.168.56.22 (192.168.56.22) 56(84) bytes of data.
64 bytes from 192.168.56.22: icmp_seq=1 ttl=64 time=1.34 ms
64 bytes from 192.168.56.22: icmp_seq=2 ttl=64 time=0.554 ms
64 bytes from 192.168.56.22: icmp_seq=3 ttl=64 time=0.967 ms
64 bytes from 192.168.56.22: icmp_seq=4 ttl=64 time=0.634 ms
64 bytes from 192.168.56.22: icmp_seq=5 ttl=64 time=0.943 ms
64 bytes from 192.168.56.22: icmp_seq=6 ttl=64 time=0.617 ms
^Z
[1]+  Detenido          ping 192.168.56.22
[uo281847@localhost u0xxxxxx]# nano -c /var/www/html/index.html
[uo281847@localhost u0xxxxxx]# firewall-cmd --add-service http
success
[uo281847@localhost u0xxxxxx]# firewall-cmd --add-service http --permanent
success
[uo281847@localhost u0xxxxxx]# systemctl start httpd.service
[uo281847@localhost u0xxxxxx]# systemctl enable httpd.service
Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service → /usr/lib/systemd/system/httpd.service.
[uo281847@localhost u0xxxxxx]# 

```

En este punto ya tenemos dos servidores web activos y corriendo, se pueden minimizar ambas máquinas virtuales. El siguiente paso es configurar el balanceador de carga.

En el equipo balanceador hay un archivo llamado /etc/haproxy/haproxy.cfg, hay que cambiar las siguientes líneas para que escuche en el puerto 80 y balancee entre los dos servidores web recién instalados:

```

frontend main
  bind *:5000
  bind *:80
  [...]
  backend app
    server app1 127.0.0.1:5000 check
    server app2 127.0.0.1:5002 check
    server app3 127.0.0.1:5003 check

```

```

64 bytes from 192.168.56.21: icmp_seq=6 ttl=64 time=0.833 ms
64 bytes from 192.168.56.21: icmp_seq=7 ttl=64 time=0.518 ms
64 bytes from 192.168.56.21: icmp_seq=8 ttl=64 time=0.863 ms
^C
--- 192.168.56.21 ping statistics ---
8 packets transmitted, 0% received, 0% packet loss, time 7055ms
rtt min/avg/max/mdev = 0.518/0.890/1.082/0.162 ms
[uo281847@localhost uxxxxxx]# ping 192.168.56.22
PING 192.168.56.22 (192.168.56.22) 56(84) bytes of data.
64 bytes from 192.168.56.22: icmp_seq=1 ttl=64 time=0.053 ms
64 bytes from 192.168.56.22: icmp_seq=2 ttl=64 time=0.102 ms
64 bytes from 192.168.56.22: icmp_seq=3 ttl=64 time=0.100 ms
64 bytes from 192.168.56.22: icmp_seq=4 ttl=64 time=0.099 ms
64 bytes from 192.168.56.22: icmp_seq=5 ttl=64 time=0.058 ms
64 bytes from 192.168.56.22: icmp_seq=6 ttl=64 time=0.089 ms
64 bytes from 192.168.56.22: icmp_seq=7 ttl=64 time=0.083 ms
64 bytes from 192.168.56.22: icmp_seq=8 ttl=64 time=0.086 ms
^C
--- 192.168.56.22 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 7192ms
rtt min/avg/max/mdev = 0.053/0.083/0.102/0.017 ms
[uo281847@localhost uxxxxxx]# nano -c /var/www/html/index.html
[uo281847@localhost uxxxxxx]# nano -c /var/www/html/index.html
[uo281847@localhost uxxxxxx]# firewall-cmd --add-service http
success
[uo281847@localhost uxxxxxx]# firewall-cmd --add-service http
Warning: ALREADY_ENABLED: 'http' already in 'public'
success
[uo281847@localhost uxxxxxx]# firewall-cmd --add-service http
Warning: ALREADY_ENABLED: 'http' already in 'public'
success
[uo281847@localhost uxxxxxx]# firewall-cmd --add-service http --permanent
success
[uo281847@localhost uxxxxxx]# systemctl start httpd.service
[uo281847@localhost uxxxxxx]# systemctl enable httpd.service
Created symlink /etc/systemd/system/multi-user.target.wants/httpd.service → /usr/lib/systemd/system/httpd.service.
[uo281847@localhost uxxxxxx]#

```

nmcli connection modify enp0s3 ipv4.method manual ipv4.address 192.168.56.24

Reinicar el equipo (o la red) # nmcli con reload; nmcli net off; nmcli net on) y comprobar con la orden # ip addr que el adaptador tiene la dirección IP correcta.

Repetir los pasos anteriores con los equipos web1 y web2 pero poniendo las direcciones IP respectivas 192.168.56.21 y 192.168.56.22.

Con las tres máquinas iniciadas se puede comprobar que hay conectividad entre ellas con la orden ping, bien desde una de ellas o bien desde el anfitrión:

```

C:\> ping 192.168.56.20
C:\> ping 192.168.56.21
C:\> ping 192.168.56.22

```

El siguiente paso es activar los servidores web. En web1 y web2 crear el archivo /var/www/html/index.html con:

```

<html>
<head>
<title>Servidor web 1</title>
</head>
<body>
<h1>Servidor web 1</h1>
</body>
</html>

```

Hay que acordarse de poner "Servidor web 2" en web2.

Abrir el cortafuegos para tráfico web en las tres máquinas:

```

# firewall-cmd --add-service http
# firewall-cmd --add-service http --permanent

```

En web1 y web2 iniciar el servicio httpd:

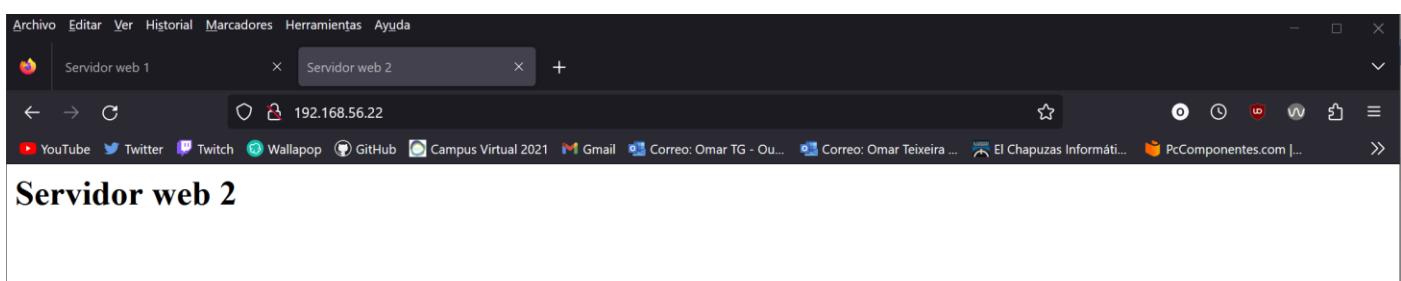
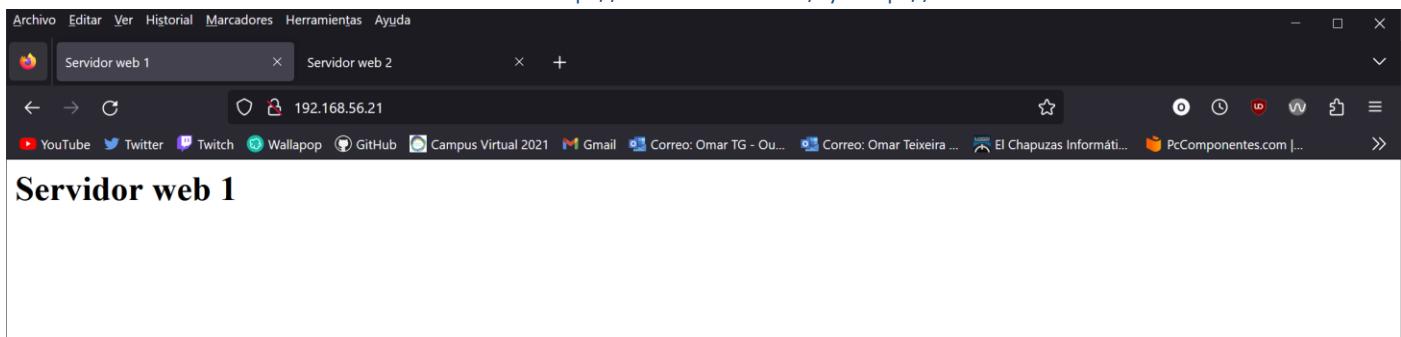
```

# systemctl start httpd.service
# systemctl enable httpd.service

```

Desde el anfitrión con Windows comprobar con cualquier navegador que se puede acceder a ambos servidores web: http://192.168.56.21/ y http://192.168.56.22

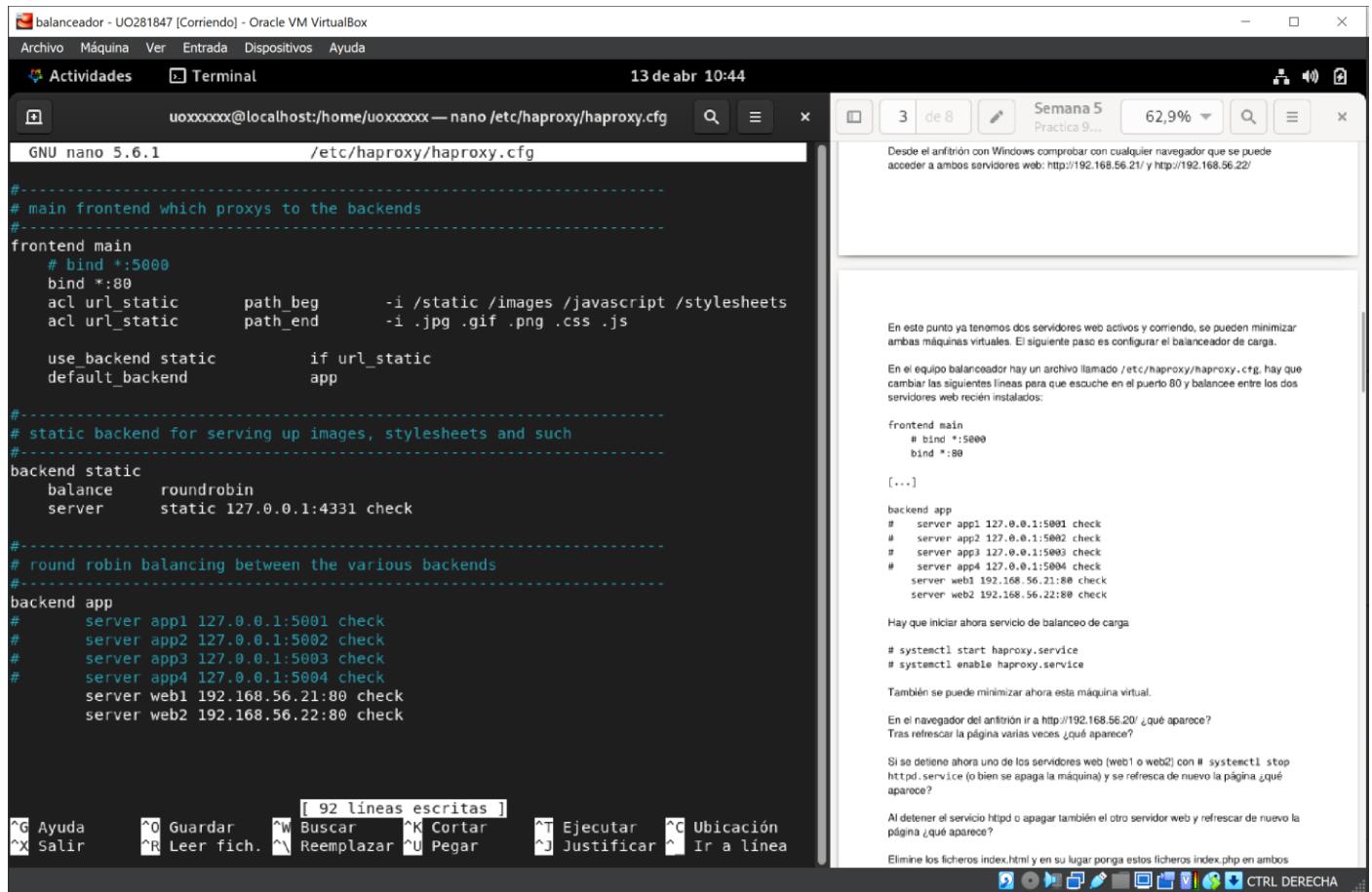
7. Desde el anfitrión con Windows comprobar con cualquier navegador que se puede acceder a ambos servidores web: <http://192.168.56.21/> y <http://192.168.56.22>



Servidor web 1

Servidor web 2

8. En este punto ya tenemos dos servidores web activos y corriendo, se pueden minimizar ambas máquinas virtuales. El siguiente paso es configurar el balanceador de carga. En el equipo balanceador hay un archivo llamado /etc/haproxy/haproxy.cfg, hay que cambiar las siguientes líneas para que escuche en el puerto 80 y balancee entre los dos servidores web recién instalados:



The screenshot shows a desktop environment with two virtual machines running in Oracle VM VirtualBox. The 'balanceador' machine is in the foreground, displaying a terminal window with the configuration file for HAProxy. The 'Practica 9...' machine is in the background, showing a slide with instructions for testing the load balancer.

```

balanceador - UO281847 [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Actividades Terminal 13 de abr 10:44
uoxxxxx@localhost:/home/uoxxxxx — nano /etc/haproxy/haproxy.cfg
GNU nano 5.6.1 /etc/haproxy/haproxy.cfg

#-----#
# main frontend which proxys to the backends
#-----#
frontend main
  # bind *:5000
  bind *:80
  acl url_static      path_beg     -i /static /images /javascript /stylesheets
  acl url_static      path_end     -i .jpg .gif .png .css .js

  use_backend static      if url_static
  default_backend      app

#-----#
# static backend for serving up images, stylesheets and such
#-----#
backend static
  balance  roundrobin
  server   static 127.0.0.1:4331 check

#-----#
# round robin balancing between the various backends
#-----#
backend app
  server app1 127.0.0.1:5001 check
  server app2 127.0.0.1:5002 check
  server app3 127.0.0.1:5003 check
  server app4 127.0.0.1:5004 check
  server web1 192.168.56.21:80 check
  server web2 192.168.56.22:80 check

[ 92 líneas escritas ]
^6 Ayuda      ^O Guardar      ^W Buscar      ^K Cortar      ^T Ejecutar      ^C Ubicación
^X Salir      ^R Leer fich.  ^Y Reemplazar  ^U Pegar       ^J Justificar  ^I Ir a línea

```

Terminal content (continued from the screenshot):

```

Desde el anfitrión con Windows comprobar con cualquier navegador que se puede acceder a ambos servidores web: http://192.168.56.21/ y http://192.168.56.22/
```

Background window (Practica 9...):

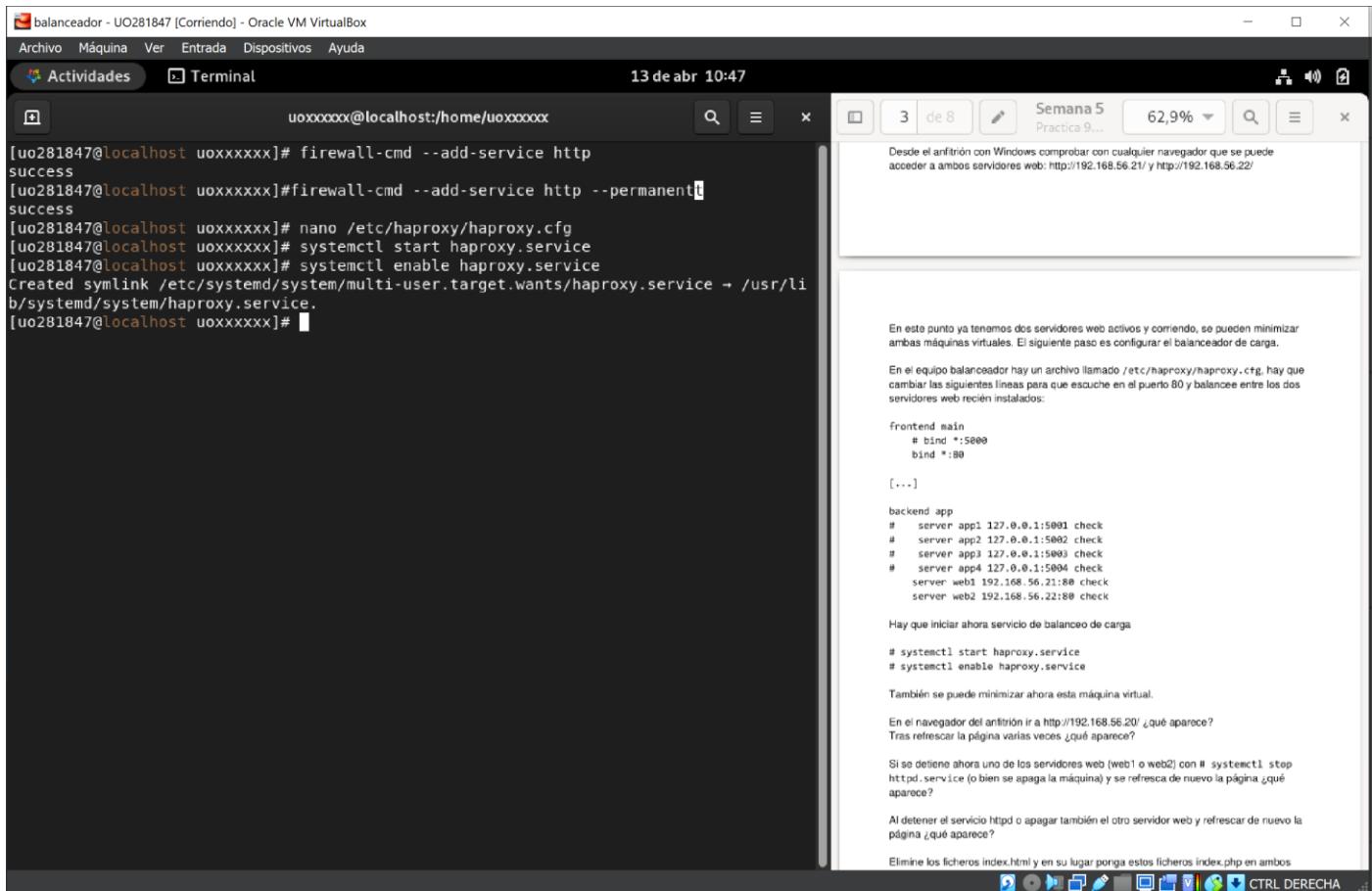
- Slide 3 of 8: Semana 5 Practica 9...
- 62,9% progress
- Text: En este punto ya tenemos dos servidores web activos y corriendo, se pueden minimizar ambas máquinas virtuales. El siguiente paso es configurar el balanceador de carga.
- Text: En el equipo balanceador hay un archivo llamado /etc/haproxy/haproxy.cfg, hay que cambiar las siguientes líneas para que escuche en el puerto 80 y balancee entre los dos servidores web recién instalados:
- Code snippet (continued from the terminal):

```

frontend main
  # bind *:5000
  bind *:80
  [...]
backend app
  # server app1 127.0.0.1:5001 check
  # server app2 127.0.0.1:5002 check
  # server app3 127.0.0.1:5003 check
  # server app4 127.0.0.1:5004 check
  server web1 192.168.56.21:80 check
  server web2 192.168.56.22:80 check

```
- Text: Hay que iniciar ahora servicio de balanceo de carga
- Text: # systemctl start haproxy.service
- Text: # systemctl enable haproxy.service
- Text: También se puede minimizar ahora esta máquina virtual.
- Text: En el navegador del anfitrión ir a http://192.168.56.20/ ¿Qué aparece?
- Text: Tras refresh la página varias veces ¿Qué aparece?
- Text: Si se detiene ahora uno de los servidores web (web1 o web2) con # systemctl stop httpd.service (o bien se apaga la máquina) y se refresca de nuevo la página ¿Qué aparece?
- Text: Al detener el servicio httpd o apagar también el otro servidor web y refreshar de nuevo la página ¿Qué aparece?
- Text: Elimine los ficheros index.html y en su lugar ponga estos ficheros index.php en ambos

9. Hay que iniciar ahora servicio de balanceo de carga



```
[uo281847@localhost uoxxxxxx]# firewall-cmd --add-service http
success
[uo281847@localhost uoxxxxxx]# firewall-cmd --add-service http --permanent
success
[uo281847@localhost uoxxxxxx]# nano /etc/haproxy/haproxy.cfg
[uo281847@localhost uoxxxxxx]# systemctl start haproxy.service
[uo281847@localhost uoxxxxxx]# systemctl enable haproxy.service
Created symlink /etc/systemd/system/multi-user.target.wants/haproxy.service → /usr/lib/systemd/system/haproxy.service.
[uo281847@localhost uoxxxxxx]#
```

Desde el anfitrión con Windows comprobar con cualquier navegador que se puede acceder a ambos servidores web: <http://192.168.56.21> y <http://192.168.56.22>

En este punto ya tenemos dos servidores web activos y corriendo, se pueden minimizar ambas máquinas virtuales. El siguiente paso es configurar el balanceador de carga.

En el equipo balanceador hay un archivo llamado `/etc/haproxy/haproxy.cfg`, hay que cambiar las siguientes líneas para que escuche en el puerto 80 y balancee entre los dos servidores web recién instalados:

```
Frontend main
  # bind *:8000
  bind *:80

[...]

Backend app
  # server app1 127.0.0.1:5001 check
  # server app2 127.0.0.1:5002 check
  # server app3 127.0.0.1:5003 check
  # server app4 127.0.0.1:5004 check
  server web1 192.168.56.21:80 check
  server web2 192.168.56.22:80 check
```

Hay que iniciar ahora servicio de balanceo de carga

```
# systemctl start haproxy.service
# systemctl enable haproxy.service
```

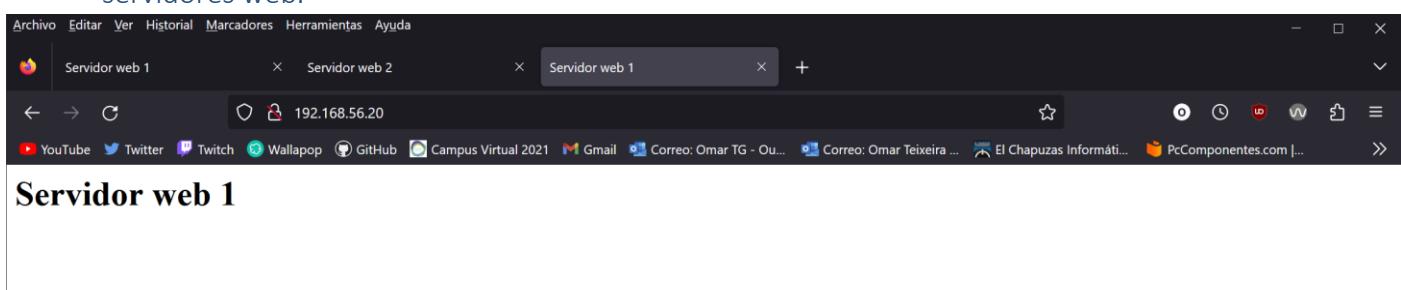
También se puede minimizar ahora esta máquina virtual.

En el navegador del anfitrión ir a <http://192.168.56.20> ¿qué aparece? Tras refrescar la página varias veces ¿qué aparece?

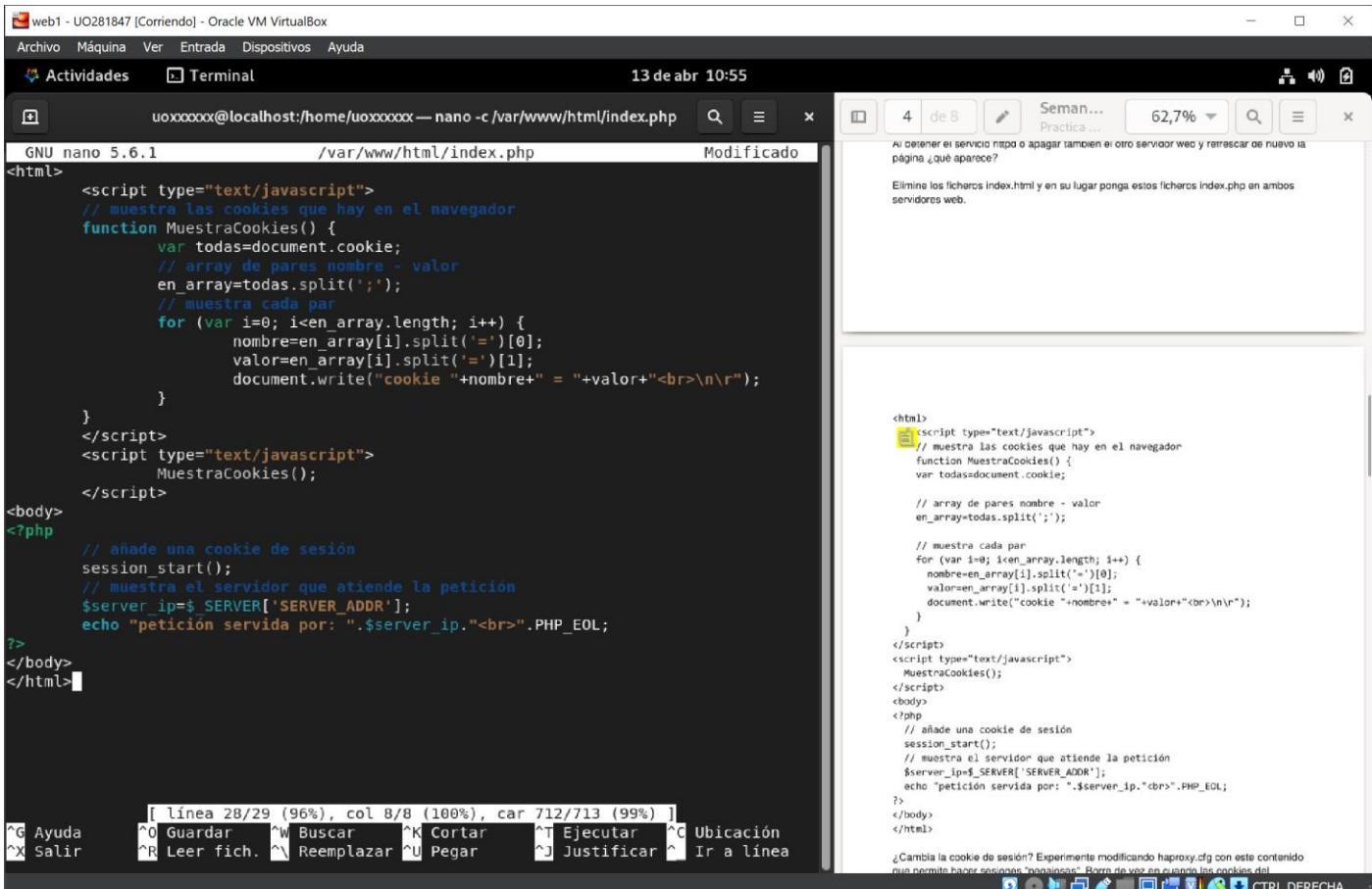
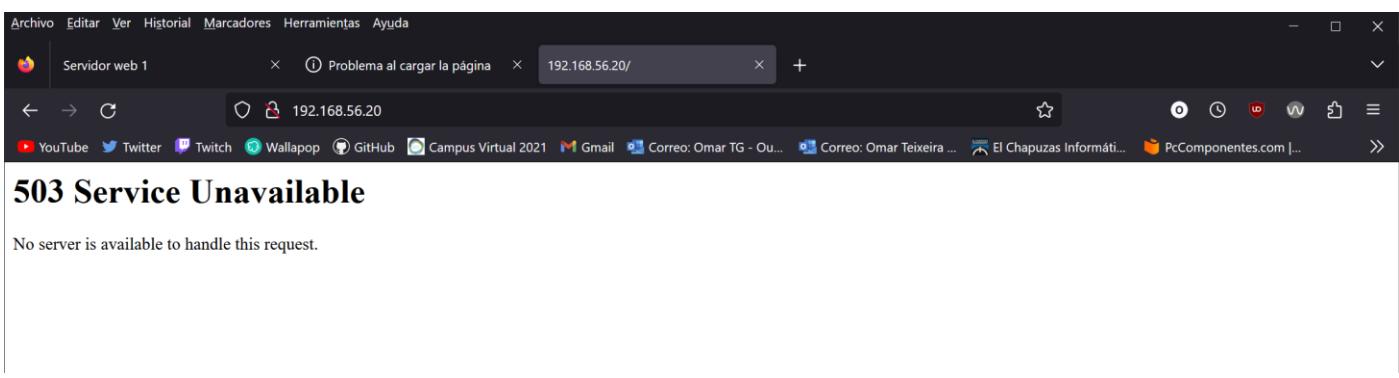
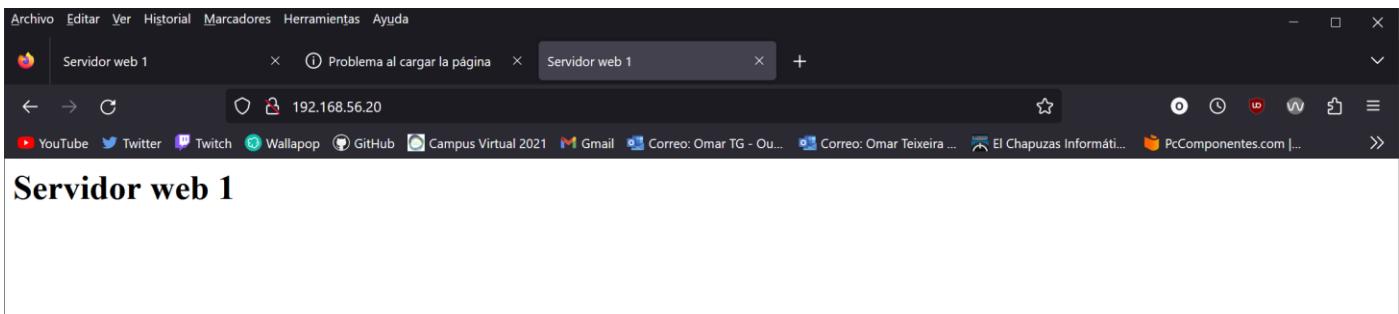
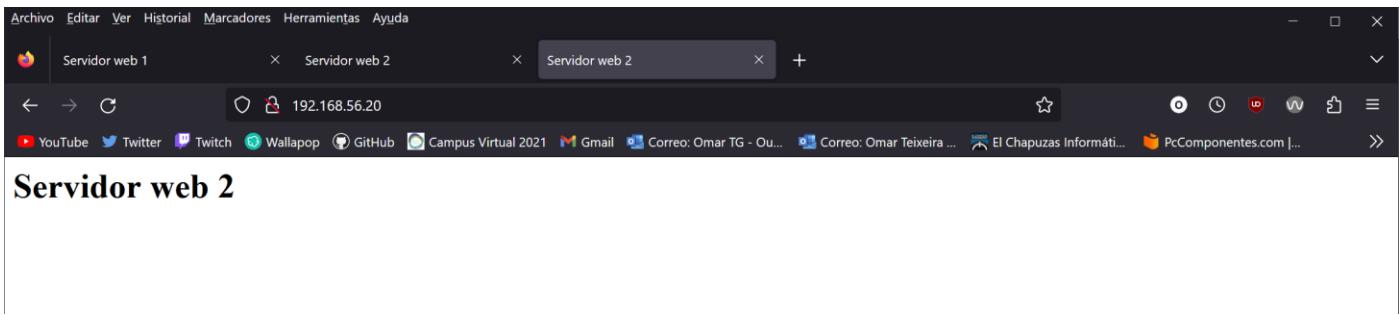
Si se detiene ahora uno de los servidores web (web1 o web2) con `systemctl stop httpd.service` (o bien se apaga la máquina) y se refresca de nuevo la página ¿qué aparece?

Al detener el servicio httpd o apagar también el otro servidor web y refrescar de nuevo la página ¿qué aparece?

Eliminar los ficheros `index.html` y en su lugar ponga estos ficheros `index.php` en ambos servidores web.



Servidor web 1



```

uoxxxxxx@localhost:/home/uoxxxxxx — nano -c /var/www/html/index.php
13 de abr 10:56
GNU nano 5.6.1          /var/www/html/index.php

<html>
<script type="text/javascript">
// muestra las cookies que hay en el navegador
function MuestraCookies() {
    var todas=document.cookie;
    // array de pares nombre - valor
    en_array=todas.split(';');
    // muestra cada par
    for (var i=0; i<en_array.length; i++) {
        nombre=en_array[i].split('=')[0];
        valor=en_array[i].split('=')[1];
        document.write("cookie "+nombre+" = "+valor+"<br>\n\r");
    }
}
</script>
<script type="text/javascript">
    MuestraCookies();
</script>
</body>
<?php
// añade una cookie de sesión
session_start();
// muestra el servidor que atiende la petición
$server_ip=$_SERVER['SERVER_ADDR'];
echo "petición servida por: ".$server_ip."<br>".PHP_EOL;
?>
</body>
</html>

```

[28 líneas escritas]

^G Ayuda ^Q Guardar ^W Buscar ^K Cortar ^T Ejecutar ^C Ubicación
^X Salir ^R Leer fich. ^L Reemplazar ^U Pegar ^J Justificar ^I Ir a línea

AI detener el servicio httpd o apagar también el otro servidor web y refrescar de nuevo la página ¿qué aparece?

Elimine los ficheros index.html y en su lugar ponga estos ficheros index.php en ambos servidores web.

```

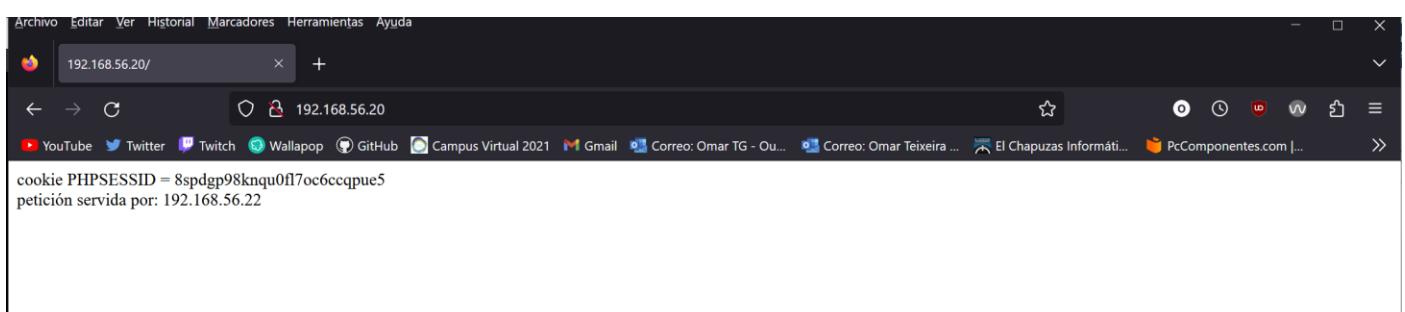
<html>
<script type="text/javascript">
// muestra las cookies que hay en el navegador
function MuestraCookies() {
    var todas=document.cookie;
    // array de pares nombre - valor
    en_array=todas.split(';');
    // muestra cada par
    for (var i=0; i<en_array.length; i++) {
        nombre=en_array[i].split('=')[0];
        valor=en_array[i].split('=')[1];
        document.write("cookie "+nombre+" = "+valor+"<br>\n\r");
    }
}
</script>
<script type="text/javascript">
    MuestraCookies();
</script>
</body>
<?php
// añade una cookie de sesión
session_start();
// muestra el servidor que atiende la petición
$server_ip=$_SERVER['SERVER_ADDR'];
echo "petición servida por: ".$server_ip."<br>".PHP_EOL;
?>
</body>
</html>

```

CTRL DERECHA

11. ¿Cambia la cookie de sesión? Experimente modificando haproxy.cfg con este contenido que permite hacer sesiones "pegajosas". Borre de vez en cuando las cookies del navegador en la última hora para hacer pruebas y añada capturas de pantalla. ¿Cuál sería la utilidad de estas sesiones pegajosas frente a las de servidor alternante?

No, no cambia.



balanceador - UO281847 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Actividades Visor de documentos 13 de abr 16:59

uoxxxxxx@localhost:/home/uoxxxxxx — nano /etc/haproxy/haproxy.cfg

```

GNU nano 5.6.1 /etc/haproxy/haproxy.cfg
timeout http-keep-alive 10s
timeout check 10s
maxconn 3000

#
# main frontend which proxys to the backends
#
frontend main
  # bind *:5000
  bind *:80
  acl url_static path_beg -i /static /images /javascript /stylesheets
  acl url_static path_end -i .jpg .gif .png .css .js

  use_backend static if url_static
  default_backend app

#
# static backend for serving up images, stylesheets and such
#
backend static
  balance roundrobin
  cookie mi_cookie insert indirect nocache
  server web1 192.168.56.21:80 check cookie valor1
  server web2 192.168.56.22:80 check cookie valor2

#
# round robin balancing between the various backends
#
backend app
  server app1 127.0.0.1:5001 check
  server app2 127.0.0.1:5002 check
  server app3 127.0.0.1:5003 check
  server app4 127.0.0.1:5004 check
  server web1 192.168.56.21:80 check

```

[94 líneas escritas]

6 Ayuda 0 Guardar ^W Buscar ^K Cortar ^T Ejecutar ^C Ubicación
 X Salir ^R Leer fich. ^L Reemplazar ^U Pegar ^J Justificar ^I Ir a línea

4 de 8 Seman... Practica ... 62,9% 4 62,9% 4

// array de pares nombre - valor
 en_array=todas.split(';');

// muestra cada par
 for (var i=0; i<en_array.length; i++) {
 nombre=en_array[i].split('=')[0];
 valor=en_array[i].split('=')[1];
 document.write("cookie "+nombre+" = "+valor+"\r\n");
 }

</script>

<script type="text/javascript">
 MuestraCookies();
</script>

</body>

<?php
// añade una cookie de sesión
session_start();
// muestra el servidor que atiende la petición
\$server_ip=\$_SERVER['SERVER_ADDR'];
echo "petición servida por: ".\$server_ip."
".PHP_EOL;
>

</body>
</html>

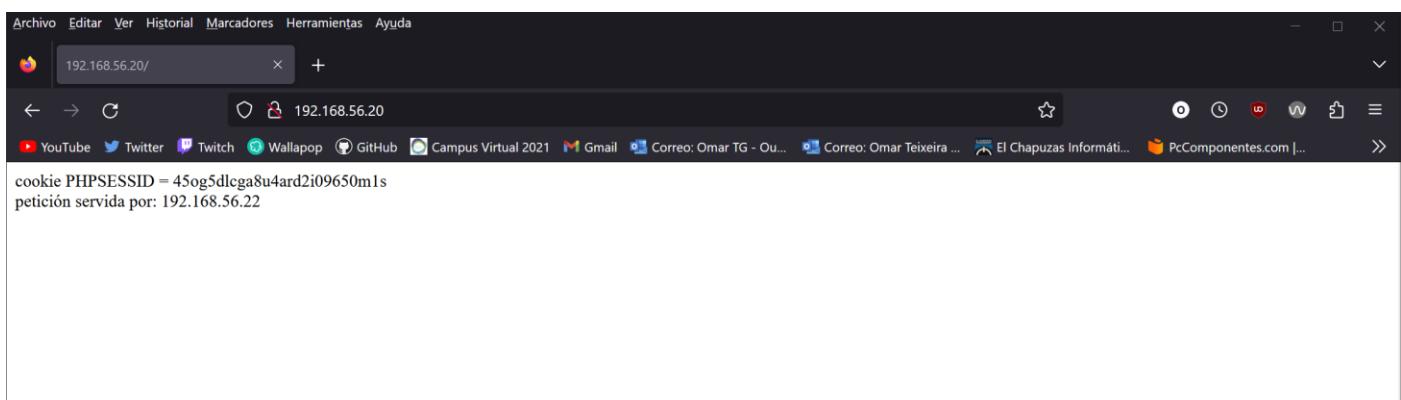
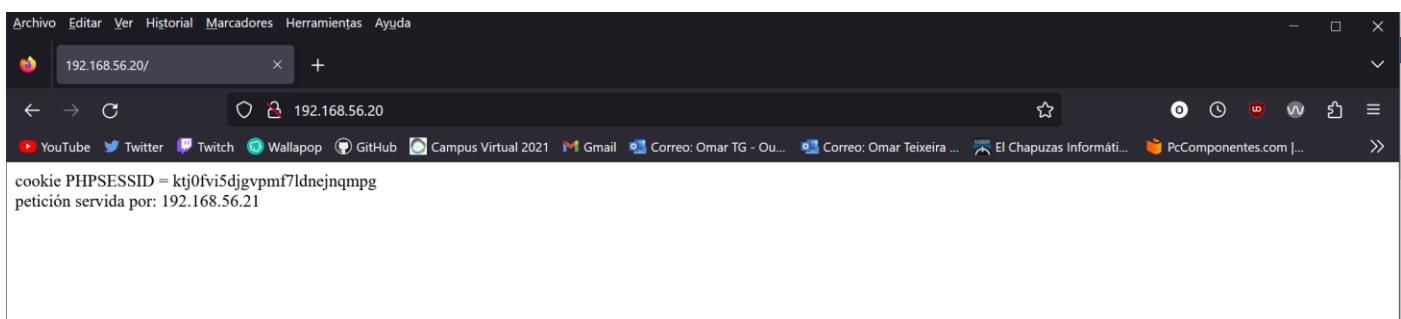
¿Cambia la cookie de sesión? Experimente modificando haproxy.cfg con este contenido que permite hacer sesiones "pegajosas". Borre de vez en cuando las cookies del navegador en la última hora para hacer pruebas y añada capturas de pantalla.

balance roundrobin
cookie mi_cookie insert indirect nocache
server web1 192.168.56.21:80 check cookie valor1
server web2 192.168.56.22:80 check cookie valor2

¿Cuál sería la utilidad de estas sesiones pegajosas frente a las de servidor alternante?

SAN (Storage Area Network)

Los servidores NAS ya conocidos permiten proporcionar y compartir carpetas y archivos ya sea vía protocolo SAMBA/CIFS o vía NFS sobre sistemas de ficheros muy habituales como los NTFS, ext4 o xfs



Las sesiones pegajosas son capaces de mantener el estado de la sesión del usuario, así como evitar el problema de la sesión interrumpida.

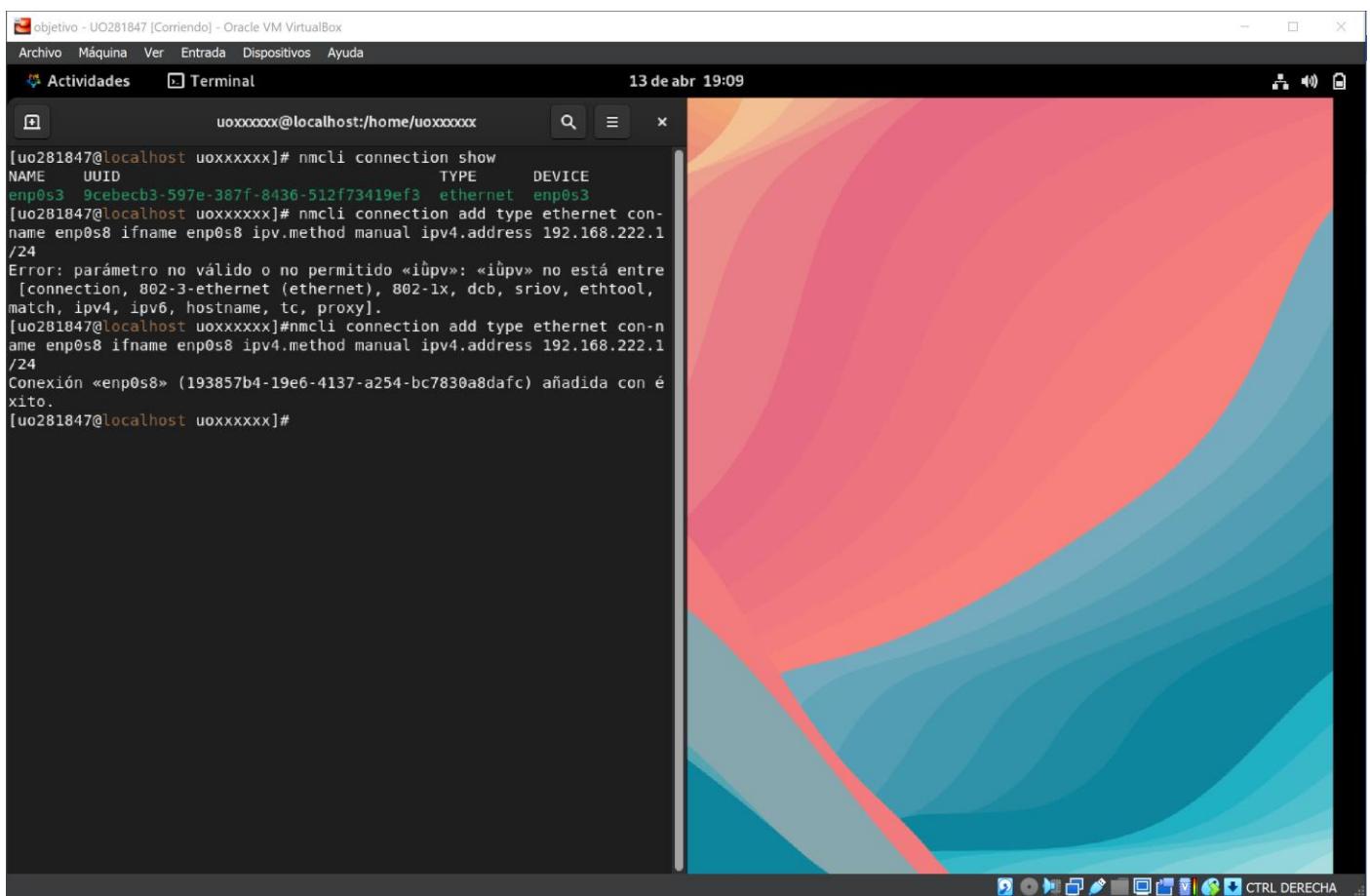
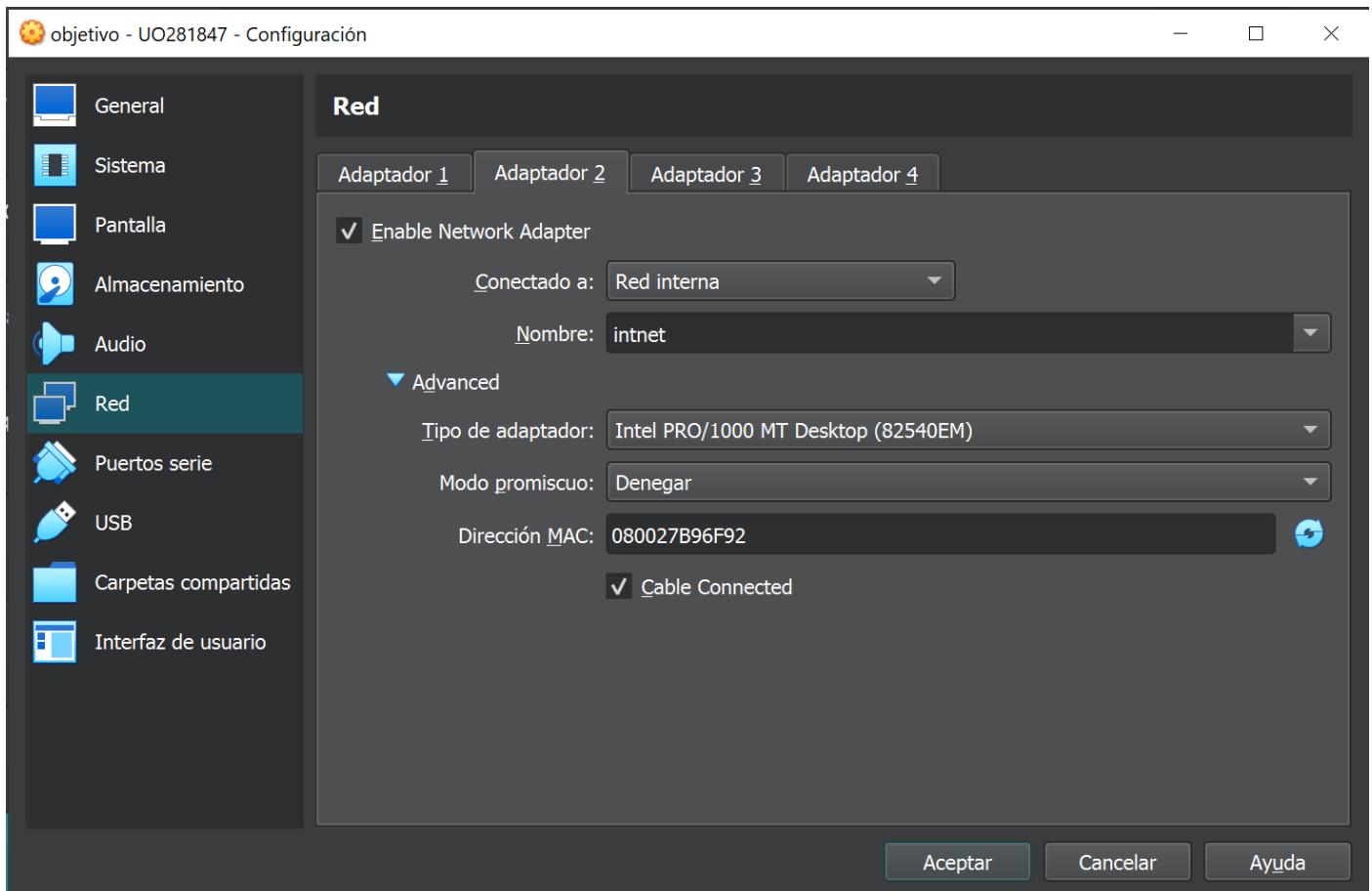
SAN (Storage Area Network).

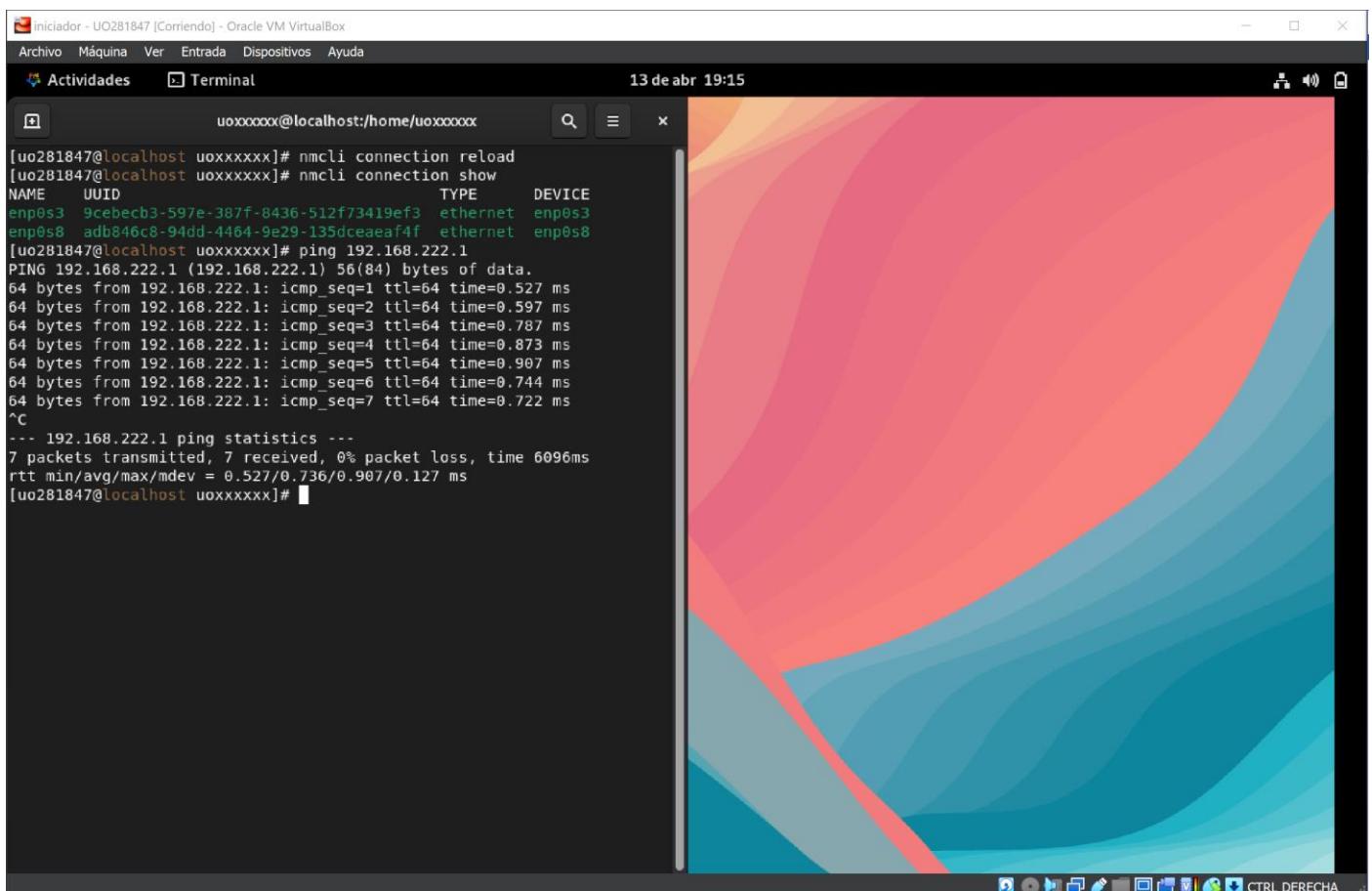
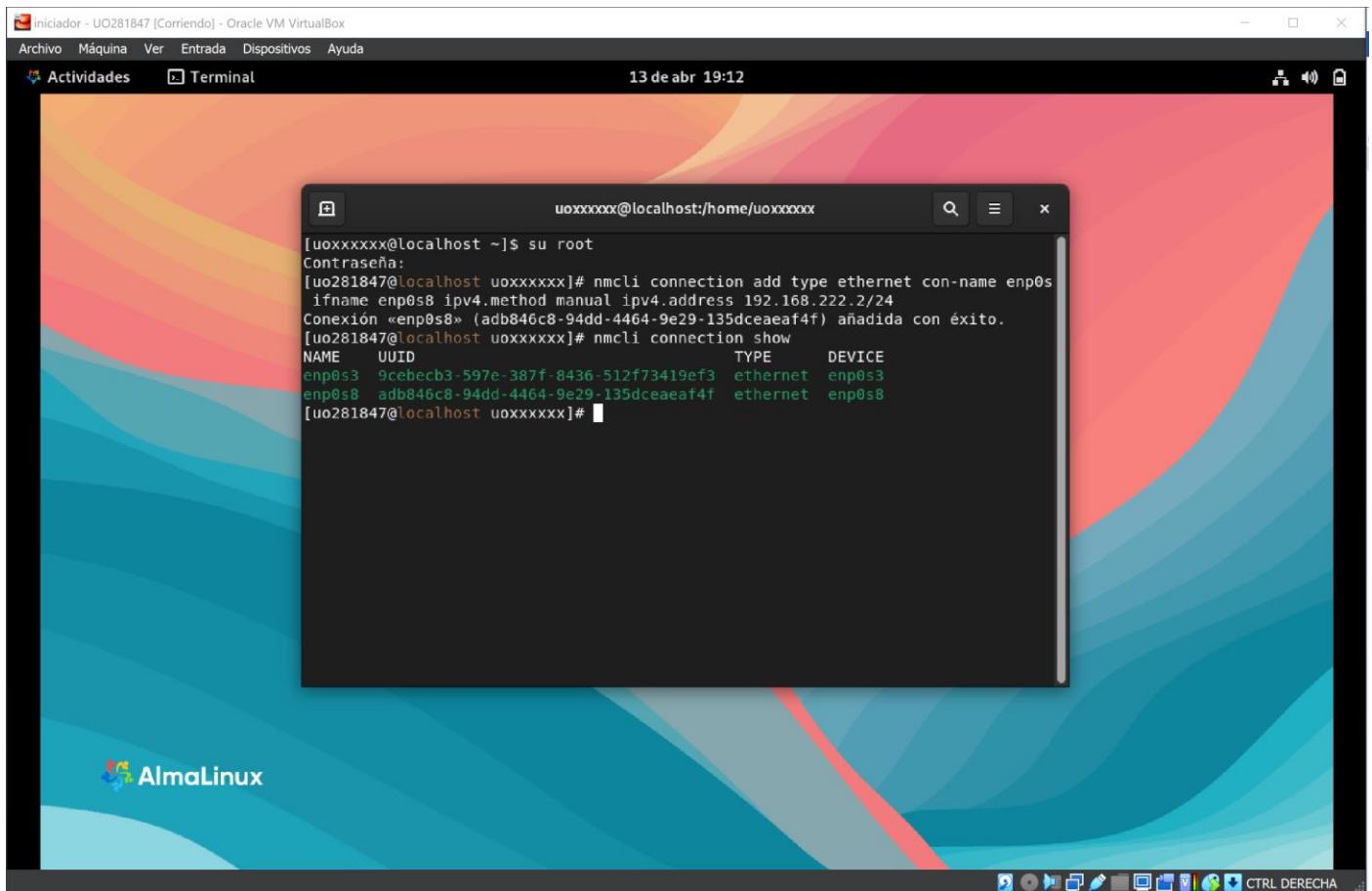
1. Los servidores NAS ya conocidos permiten proporcionar y compartir carpetas y ficheros ya sea vía protocolo SAMBA/CIFS o vía NFS sobre sistemas de ficheros muy habituales como son NTFS, ext4 o xfs.

Los servidores SAN en cambio proporcionan bloques a otros equipos desde los cuales estos bloques se ven como discos externos. Para estos servidores SAN se emplean conexiones basadas en canal de fibra (FC) con el protocolo FCP que permite velocidades de hasta 16Gb/s aunque también se pueden emplear protocolos sobre Ethernet siendo el iSCSI (Internet Small Computer System Interface) el más frecuente. A diferencia de los NAS no es posible compartir un disco SAN excepto si se emplea algún tipo de sistema de ficheros de cluster diseñado específicamente para esto como puedan ser GFS2 (RedHat), CSV (Microsoft), GPFS (IBM) o Xsan (Apple). Para esta práctica se van a emplear dos equipos, uno que hará de servidor (llamado "objetivo/target" de ahora en adelante) y proporcionará los bloques de un disco completo y los de una imagen de disco. El otro hará de cliente (llamado "iniciador/initiator" de ahora en adelante) que montará los dos discos de red proporcionados por el servidor/objetivo. Este iniciador o cliente verá tales recursos como discos internos. Ambas máquinas virtuales tendrán un adaptador de red conectado a NAT para descargar el software necesario y otro conectado a una red interna que se empleará exclusivamente para el tráfico iSCSI.

Las operaciones a realizar son a partir de dos Linux mínimos o con GUI: primero añadir un segundo adaptador de red interna a ambas máquinas virtuales y además al equipo que actuará como servidor añadirle un segundo disco. Puestos en marcha ambos sistemas, la configuración de los adaptadores de red interna pueden hacerse con las órdenes nmcli ya conocidas aplicándolas al adaptador enp0s8 de manera que el servidor (objetivo/target) tenga la dirección IP 192.168.222.1 y el cliente (iniciador) la 192.168.222.2 quedando este adaptador en la zona "internal" del cortafuegos. Reiniciar la red y comprobar con la orden ping que ambos equipos se ven entre sí. Verificar también que cada adaptador está en la zona correspondiente:







```

[uo281847@localhost uoxxxxxx]# nmcli connection reload
[uo281847@localhost uoxxxxxx]# nmcli connection show
NAME      UUID                                  TYPE      DEVICE
enp0s3    9cebecb3-597e-387f-8436-512f73419ef3  ethernet  enp0s3
enp0s8    193857b4-19e6-4137-a254-bc7830a8dafc  ethernet  enp0s8
[uo281847@localhost uoxxxxxx]# ping 192.168.222.2
PING 192.168.222.2 (192.168.222.2) 56(84) bytes of data.
64 bytes from 192.168.222.2: icmp_seq=1 ttl=64 time=0.999 ms
64 bytes from 192.168.222.2: icmp_seq=2 ttl=64 time=0.890 ms
64 bytes from 192.168.222.2: icmp_seq=3 ttl=64 time=0.681 ms
64 bytes from 192.168.222.2: icmp_seq=4 ttl=64 time=1.26 ms
64 bytes from 192.168.222.2: icmp_seq=5 ttl=64 time=0.936 ms
64 bytes from 192.168.222.2: icmp_seq=6 ttl=64 time=0.737 ms
64 bytes from 192.168.222.2: icmp_seq=7 ttl=64 time=0.731 ms
^C
--- 192.168.222.2 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6013ms
rtt min/avg/max/mdev = 0.681/0.890/1.257/0.185 ms
[uo281847@localhost uoxxxxxx]#

```

Semana 5
Práctica 9.pdf

70%

CTRL DERECHA

```

[uo281847@localhost uoxxxxxx]# nmcli connection reload
[uo281847@localhost uoxxxxxx]# nmcli connection show
NAME      UUID                                  TYPE      DEVICE
enp0s3    9cebecb3-597e-387f-8436-512f73419ef3  ethernet  enp0s3
enp0s8    193857b4-19e6-4137-a254-bc7830a8dafc  ethernet  enp0s8
[uo281847@localhost uoxxxxxx]# ping 192.168.222.2
PING 192.168.222.2 (192.168.222.2) 56(84) bytes of data.
64 bytes from 192.168.222.2: icmp_seq=1 ttl=64 time=0.999 ms
64 bytes from 192.168.222.2: icmp_seq=2 ttl=64 time=0.890 ms
64 bytes from 192.168.222.2: icmp_seq=3 ttl=64 time=0.681 ms
64 bytes from 192.168.222.2: icmp_seq=4 ttl=64 time=1.26 ms
64 bytes from 192.168.222.2: icmp_seq=5 ttl=64 time=0.936 ms
64 bytes from 192.168.222.2: icmp_seq=6 ttl=64 time=0.737 ms
64 bytes from 192.168.222.2: icmp_seq=7 ttl=64 time=0.731 ms
^C
--- 192.168.222.2 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6013ms
rtt min/avg/max/mdev = 0.681/0.890/1.257/0.185 ms
[uo281847@localhost uoxxxxxx]# firewall-cmd --get-active-zones
public
  interfaces: enp0s3 enp0s8
[uo281847@localhost uoxxxxxx]#

```

SAN (Storage Area Network)

Los servidores NAS ya conocidos permiten proporcionar y compartir carpetas y ficheros ya sea vía protocolo SMB/CIFS o vía NFS sobre sistemas de ficheros muy habituales como son NTFS, ext4 o xfs.

Los servidores SAN en cambio proporcionan bloques a otros equipos desde los cuales estos bloques se ven como discos externos. Para estos servidores SAN se emplean conexiones basadas en canal de fibra (FC) con el protocolo FCP que permite velocidades de hasta 16Gb/s aunque también se pueden emplear protocolos sobre Ethernet siendo el iSCSI (Internet Small Computer System Interface) el más frecuente.

A diferencia de los NAS no es posible compartir un disco SAN excepto si se emplea algún tipo de sistema de ficheros de cluster diseñado específicamente para esto como puedan ser QFS2 (RediHat), CSV (Microsoft), GPFS (IBM) o Xsan (Apple).

Para esta práctica se van a emplear dos equipos, uno que hará de servidor (llamado "objetivo/objetivo" de ahora en adelante) y proporcionará los bloques de un disco completo de una de las imágenes de disco. El otro hará de cliente (llamado "iniciador/iniciador" de ahora en adelante) que montará los dos discos de red proporcionados por el servidor/objetivo. Este iniciador o cliente verá tales recursos como discos internos.

Ambas máquinas virtuales tendrán un adaptador de red conectado a NAT para descargar el software necesario y otro conectado a una red interna que se empleará exclusivamente para el tráfico iSCSI.

Las operaciones a realizar son a partir de dos Linux mínimos o con GUI: primero añadir un segundo adaptador de red interna a ambas máquinas virtuales y además al equipo que actuará como servidor añadirle un segundo disco.

Puestos en marcha ambos sistemas, la configuración de los adaptadores de red interna pueden hacerse con las órdenes nmcli ya conocidas aplicándolas al adaptador enp0s8 de manera que el servidor (objetivo/objetivo) tenga la dirección IP 192.168.222.1 y el cliente (iniciador) la 192.168.222.2 quedando este adaptador en la zona "internal" del cortafuegos. Reiniciar la red y comprobar con la orden ping que ambos equipos se ven entre sí. Verificar también que cada adaptador está en la zona correspondiente:

```

# firewall-cmd --get-active-zones
En el objetivo comprobar que aparece el disco nuevo y crear un fichero de 1 GB que se exportará como otro disco.
# fallocate --length 1G fichero.dsk
A continuación instalar el software, poner en marcha el servicio y abrir el puerto TCP 3260.
# dnf -y install targetcli
# systemctl enable --now target

```

```

[uo281847@localhost uxxxxxx]# nmcli connection reload
[uo281847@localhost uxxxxxx]# nmcli connection show
NAME                UUID                                  TYPE      DEVICE
enp0s3              9cebcb3-597e-8436-512f73419ef3  ethernet  enp0s3
enp0s8              adb846c8-94dd-4464-9e29-135dceaaef4f  ethernet  enp0s8
[uo281847@localhost uxxxxxx]# ping 192.168.222.1
PING 192.168.222.1 (192.168.222.1) 56(84) bytes of data.
64 bytes from 192.168.222.1: icmp_seq=1 ttl=64 time=0.527 ms
64 bytes from 192.168.222.1: icmp_seq=2 ttl=64 time=0.597 ms
64 bytes from 192.168.222.1: icmp_seq=3 ttl=64 time=0.787 ms
64 bytes from 192.168.222.1: icmp_seq=4 ttl=64 time=0.873 ms
64 bytes from 192.168.222.1: icmp_seq=5 ttl=64 time=0.907 ms
64 bytes from 192.168.222.1: icmp_seq=6 ttl=64 time=0.744 ms
64 bytes from 192.168.222.1: icmp_seq=7 ttl=64 time=0.722 ms
^C
--- 192.168.222.1 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6096ms
rtt min/avg/max/mdev = 0.527/0.736/0.907/0.127 ms
[uo281847@localhost uxxxxxx]# firewall-cmd --get-active-zones
public
  interfaces: enp0s3 enp0s8
[uo281847@localhost uxxxxxx]#

```

SAN (Storage Area Network)

Los servidores NAS ya conocidos permiten proporcionar y compartir carpetas y ficheros ya sea vía protocolo SMBA/CIFS o vía NFS sobre sistemas de ficheros muy habituales como son NTFS, ext4 o xfs.

Los servidores SAN en cambio proporcionan bloques a otros equipos desde los cuales estos bloques se ven como discos externos. Para estos servidores SAN se emplean conexiones basadas en canal de fibra (FC) con el protocolo FCP que permite velocidades de hasta 16Gbit/s aunque también se pueden emplear protocolos sobre Ethernet siendo el iSCSI (Internet Small Computer System Interface) el más frecuente.

A diferencia de los NAS no es posible compartir un disco SAN excepto si se emplea algún tipo de sistema de ficheros de cluster diseñado específicamente para esto como puedan ser GFS2 (RedHat), CSV (Microsoft), GPFS (IBM) o Xsan (Apple).

Para esta práctica se van a emplear dos equipos, uno que hará de servidor (llamado "objetivo/target" de ahora en adelante) y proporcionará los bloques de un disco completo y los de una imagen de disco. El otro hará de cliente (llamado "iniciador/initiator" de ahora en adelante) que montará los dos discos de red proporcionados por el servidor/objetivo. Este iniciador o cliente verá tales recursos como discos internos.

Ambas máquinas virtuales tendrán un adaptador de red conectado a NAT para descargar el software necesario y otro conectado a una red interna que se empleará exclusivamente para el tráfico iSCSI.

Las operaciones a realizar son a partir de dos Linux mínimos o con GUI: primero añadir un segundo adaptador de red interna a ambas máquinas virtuales y además al equipo que actuará como servidor añadirle un segundo disco.

Puestos en marcha ambos sistemas, la configuración de los adaptadores de red interna pueden hacerse con las órdenes nmcli ya conocidas aplicándolas al adaptador enp0s8 de manera que el servidor (objetivo/target) tenga la dirección IP 192.168.222.1 y el cliente (iniciador) la 192.168.222.2 quedando este adaptador en la zona "internal" del cortafuegos. Reiniciar la red y comprobar con la orden ping que ambos equipos se ven entre sí. Verificar también que cada adaptador está en la zona correspondiente:

```

# firewall-cmd --get-active-zones

```

En el objetivo comprobar que aparece el disco nuevo y crear un fichero de 1 GB que se exportará como otro disco.

```

# fallocate --length 1G fichero.dsk

```

A continuación instalar el software, poner en marcha el servicio y abrir el puerto TCP 3260.

```

# dnf -y install targetcli
# systemctl enable --now target
# firewall-cmd --add-service=target --permanent
# firewall-cmd --add-service=target --zone=internal --permanent

```

2. En el objetivo comprobar que aparece el disco nuevo y crear un fichero de 1 GB que se exportará como otro disco.

```

[uo281847@localhost uxxxxxx]# lsblk
NAME    MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
sda      8:0    0  20G  0 disk
└─sda1   8:1    0 600M  0 part /boot/efi
└─sda2   8:2    0   1G  0 part /boot
└─sda3   8:3    0 18,4G  0 part
  ├─almalinux-root 253:0  0 16,4G  0 lvm /
  └─almalinux-swap 253:1  0   2G  0 lvm [SWAP]
sdb      8:16   0  20G  0 disk
sr0     11:0   1 1024M 0 rom
[uo281847@localhost uxxxxxx]# fallocate --length 1G fichero.dsk
[uo281847@localhost uxxxxxx]# fallocate --length 1G fichero.dsk
[uo281847@localhost uxxxxxx]# lsblk
NAME    MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
sda      8:0    0  20G  0 disk
└─sda1   8:1    0 600M  0 part /boot/efi
└─sda2   8:2    0   1G  0 part /boot
└─sda3   8:3    0 18,4G  0 part
  ├─almalinux-root 253:0  0 16,4G  0 lvm /
  └─almalinux-swap 253:1  0   2G  0 lvm [SWAP]
sdb      8:16   0  20G  0 disk
sr0     11:0   1 1024M 0 rom
[uo281847@localhost uxxxxxx]#

```

SAN (Storage Area Network)

Los servidores NAS ya conocidos permiten proporcionar y compartir carpetas y ficheros ya sea vía protocolo SMBA/CIFS o vía NFS sobre sistemas de ficheros muy habituales como son NTFS, ext4 o xfs.

Los servidores SAN en cambio proporcionan bloques a otros equipos desde los cuales estos bloques se ven como discos externos. Para estos servidores SAN se emplean conexiones basadas en canal de fibra (FC) con el protocolo FCP que permite velocidades de hasta 16Gbit/s aunque también se pueden emplear protocolos sobre Ethernet siendo el iSCSI (Internet Small Computer System Interface) el más frecuente.

A diferencia de los NAS no es posible compartir un disco SAN excepto si se emplea algún tipo de sistema de ficheros de cluster diseñado específicamente para esto como puedan ser GFS2 (RedHat), CSV (Microsoft), GPFS (IBM) o Xsan (Apple).

Para esta práctica se van a emplear dos equipos, uno que hará de servidor (llamado "objetivo/target" de ahora en adelante) y proporcionará los bloques de un disco completo y los de una imagen de disco. El otro hará de cliente (llamado "iniciador/initiator" de ahora en adelante) que montará los dos discos de red proporcionados por el servidor/objetivo. Este iniciador o cliente verá tales recursos como discos internos.

Ambas máquinas virtuales tendrán un adaptador de red conectado a NAT para descargar el software necesario y otro conectado a una red interna que se empleará exclusivamente para el tráfico iSCSI.

Las operaciones a realizar son a partir de dos Linux mínimos o con GUI: primero añadir un segundo adaptador de red interna a ambas máquinas virtuales y además al equipo que actuará como servidor añadirle un segundo disco.

Puestos en marcha ambos sistemas, la configuración de los adaptadores de red interna pueden hacerse con las órdenes nmcli ya conocidas aplicándolas al adaptador enp0s8 de manera que el servidor (objetivo/target) tenga la dirección IP 192.168.222.1 y el cliente (iniciador) la 192.168.222.2 quedando este adaptador en la zona "internal" del cortafuegos. Reiniciar la red y comprobar con la orden ping que ambos equipos se ven entre sí. Verificar también que cada adaptador está en la zona correspondiente:

```

# firewall-cmd --get-active-zones

```

En el objetivo comprobar que aparece el disco nuevo y crear un fichero de 1 GB que se exportará como otro disco.

```

# fallocate --length 1G fichero.dsk

```

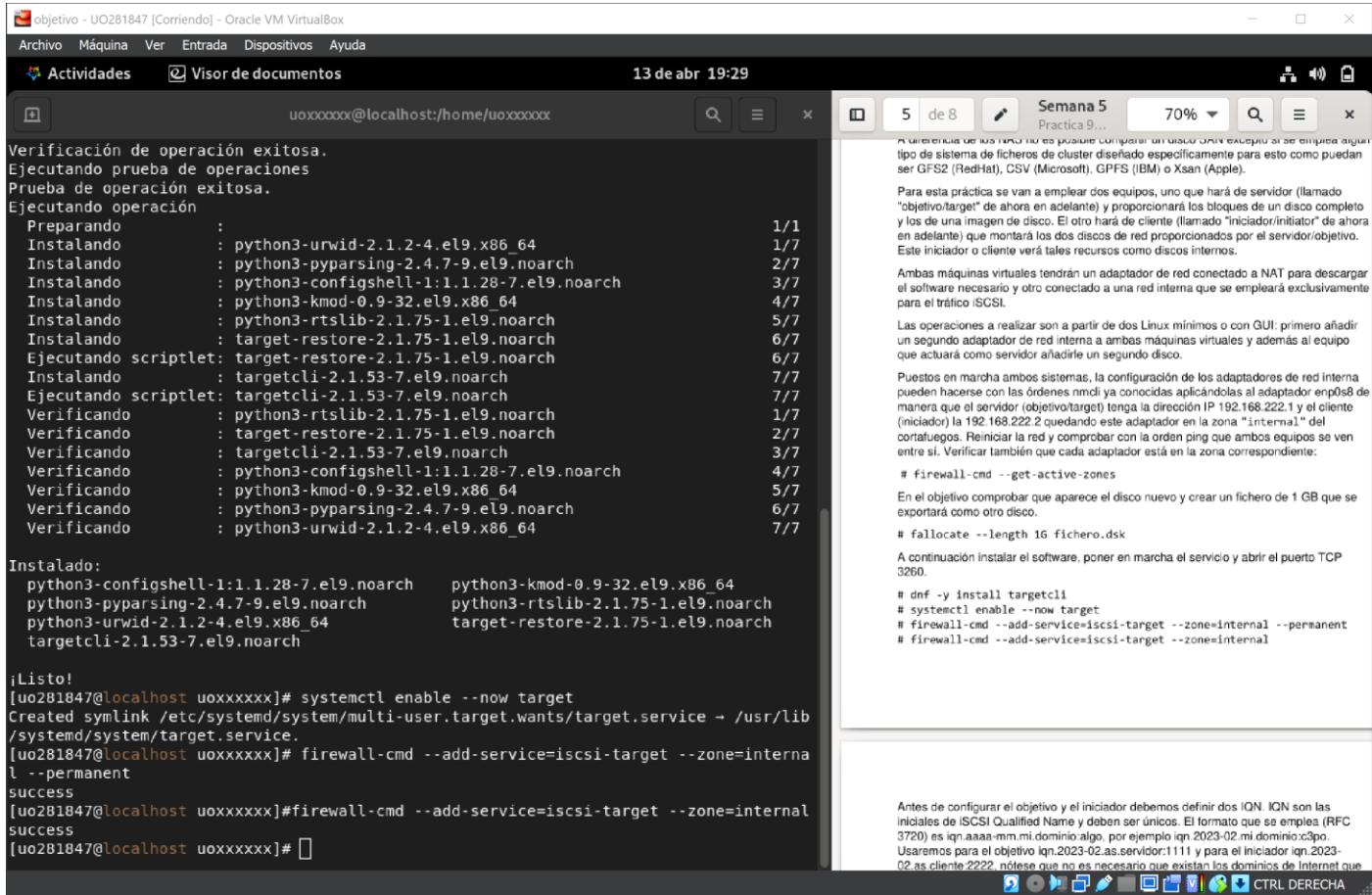
A continuación instalar el software, poner en marcha el servicio y abrir el puerto TCP 3260.

```

# dnf -y install targetcli
# systemctl enable --now target
# firewall-cmd --add-service=target --permanent
# firewall-cmd --add-service=target --zone=internal --permanent

```

3. A continuación instalar el software, poner en marcha el servicio y abrir el puerto TCP 3260.



```

objetivo - UO281847 [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Actividades Visor de documentos 13 de abr 19:29
uoxxxxxx@localhost:home/uoxxxxxx
Verificación de operación exitosa.
Ejecutando prueba de operaciones
Prueba de operación exitosa.
Ejecutando operación
Preparando : 1/1
Instalando : python3-urwid-2.1.2-4.el9.x86_64 1/7
Instalando : python3-pyparsing-2.4.7-9.el9.noarch 2/7
Instalando : python3-configshell-1:1.1.28-7.el9.noarch 3/7
Instalando : python3-kmod-0.9-32.el9.x86_64 4/7
Instalando : python3-rtslib-2.1.75-1.el9.noarch 5/7
Instalando : target-restore-2.1.75-1.el9.noarch 6/7
Ejecutando scriptlet: target-restore-2.1.75-1.el9.noarch 6/7
Instalando : targetcli-2.1.53-7.el9.noarch 7/7
Ejecutando scriptlet: targetcli-2.1.53-7.el9.noarch 7/7
Verificando : python3-rtslib-2.1.75-1.el9.noarch 1/7
Verificando : target-restore-2.1.75-1.el9.noarch 2/7
Verificando : targetcli-2.1.53-7.el9.noarch 3/7
Verificando : python3-configshell-1:1.1.28-7.el9.noarch 4/7
Verificando : python3-kmod-0.9-32.el9.x86_64 5/7
Verificando : python3-pyparsing-2.4.7-9.el9.noarch 6/7
Verificando : python3-urwid-2.1.2-4.el9.x86_64 7/7

Instalado:
python3-configshell-1:1.1.28-7.el9.noarch python3-kmod-0.9-32.el9.x86_64
python3-pyparsing-2.4.7-9.el9.noarch python3-rtslib-2.1.75-1.el9.noarch
python3-urwid-2.1.2-4.el9.x86_64 target-restore-2.1.75-1.el9.noarch
targetcli-2.1.53-7.el9.noarch

>Listo!
[uo281847@localhost uoxxxxxx]# systemctl enable --now target
Created symlink /etc/systemd/system/multi-user.target.wants/target.service → /usr/lib
/systemd/system/target.service.
[uo281847@localhost uoxxxxxx]# firewall-cmd --add-service=iscsi-target --zone=internal
--permanent
success
[uo281847@localhost uoxxxxxx]# firewall-cmd --add-service=iscsi-target --zone=internal
success
[uo281847@localhost uoxxxxxx]# 

```

Para esta práctica se van a emplear dos equipos, uno que hará de servidor (llamado "objetivo/target" de ahora en adelante) y proporcionarán los bloques de un disco completo y los de una imagen de disco. El otro hará de cliente (llamado "iniciador/initiator" de ahora en adelante) que montará los dos discos de red proporcionados por el servidor/objetivo. Este iniciador o cliente verá tales recursos como discos internos.

Ambas máquinas virtuales tendrán un adaptador de red conectado a NAT para descargar el software necesario y otro conectado a una red interna que se empleará exclusivamente para el tráfico iSCSI.

Las operaciones se realizarán a partir de dos Linux mínimos o con GUI: primero añadir un segundo adaptador de red interna a ambas máquinas virtuales y además al equipo que actuará como servidor añadirle un segundo disco.

Puestos en marcha ambos sistemas, la configuración de los adaptadores de red interna pueden hacerse con las órdenes nmcli ya conocidas aplicándolas al adaptador enp0s8 de manera que el servidor (objetivo/target) tenga la dirección IP 192.168.222.1 y el cliente (iniciador) la 192.168.222.2 quedando este adaptador en la zona "internal" del cortafuegos. Reiniciar la red y comprobar con la orden ping que ambos equipos se ven entre sí. Verificar también que cada adaptador está en la zona correspondiente:

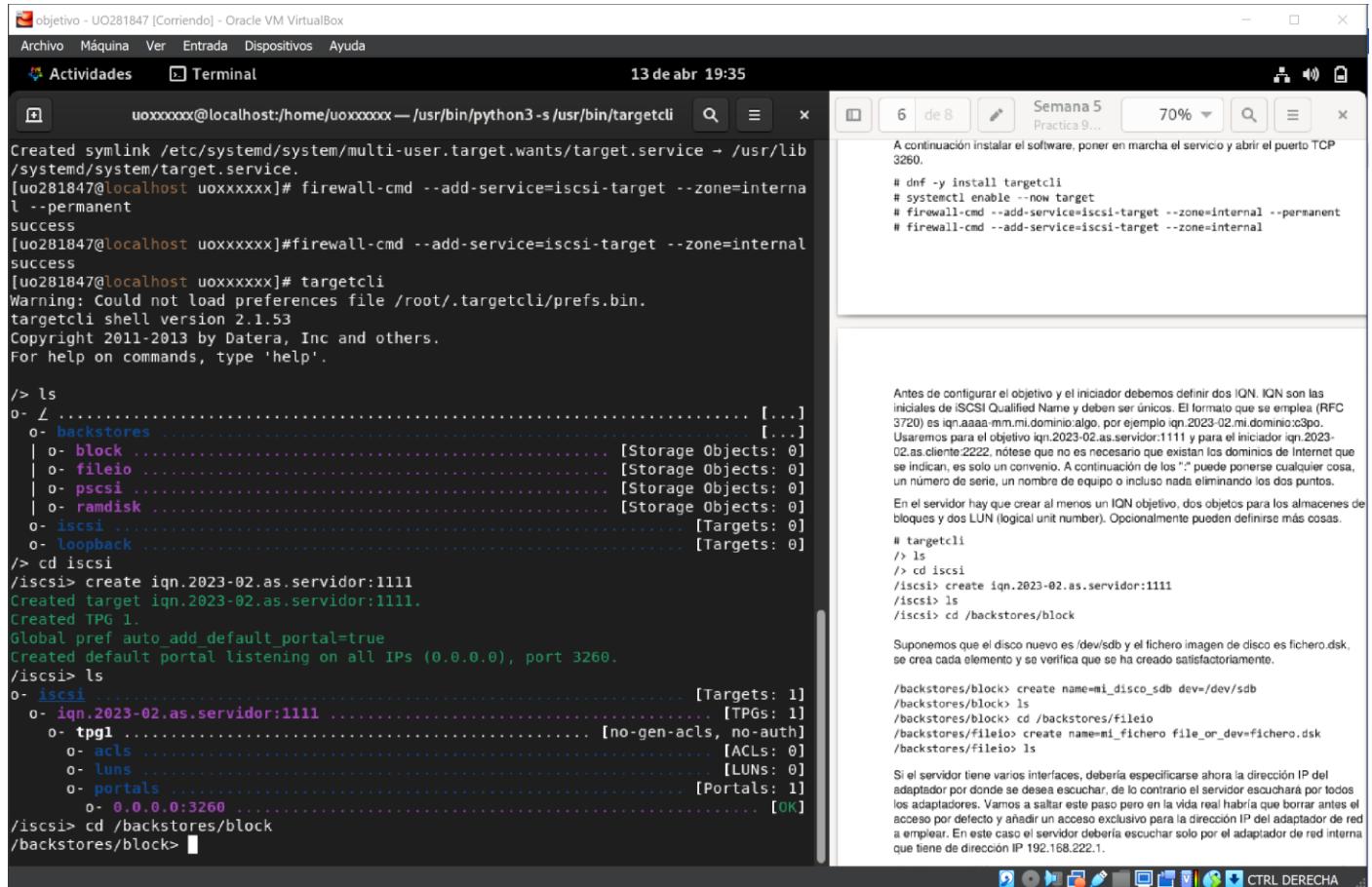
```

# firewall-cmd --get-active-zones
En el objetivo comprobar que aparece el disco nuevo y crear un fichero de 1 GB que se exportará como otro disco.
# falllocate --length 1G fichero.dsk
A continuación instalar el software, poner en marcha el servicio y abrir el puerto TCP 3260.
# dnf -y install targetcli
# systemctl enable --now target
# firewall-cmd --add-service=iscsi-target --zone=internal --permanent
# firewall-cmd --add-service=iscsi-target --zone=internal

```

Antes de configurar el objetivo y el iniciador debemos definir dos IQN. IQN son las iniciales de iSCSI Qualified Name y deben ser únicos. El formato que se emplea (RFC 3720) es iqn.aaaa-mm.mi.domínio.algo, por ejemplo iqn.2023-02.mi.domínio:c3po. Usaremos para el objetivo iqn.2023-02.as.servidor:1111 y para el iniciador iqn.2023-02.mi.cliente:2222, nótese que no es necesario que existan los dominios de Internet que

4. Antes de configurar el objetivo y el iniciador debemos definir dos IQN. IQN son las iniciales de iSCSI Qualified Name y deben ser únicos. El formato que se emplea (RFC 3720) es iqn.aaaa-mm.mi.dominio:algo, por ejemplo iqn.2023-02.mi.dominio:c3po. Usaremos para el objetivo iqn.2023-02.as.servidor:1111 y para el iniciador iqn.2023-02.as.cliente:2222, nótese que no es necesario que existan los dominios de Internet que se indican, es solo un convenio. A continuación de los ":" puede ponerse cualquier cosa, un número de serie, un nombre de equipo o incluso nada eliminando los dos puntos. En el servidor hay que crear al menos un IQN objetivo, dos objetos para los almacenes de bloques y dos LUN (logical unit number). Opcionalmente pueden definirse más cosas.



```

objetivo - UO281847 [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Actividades Terminal 13 de abr 19:35
uoxxxxxx@localhost:~/.uoxxxxxx — /usr/bin/python3 -s /usr/bin/targetcli
Created symlink /etc/systemd/system/multi-user.target.wants/target.service → /usr/lib/systemd/system/target.service.
[uo281847@localhost uoxxxxxx]# firewall-cmd --add-service=iscsi-target --zone=internal
l --permanent
success
[uo281847@localhost uoxxxxxx]# firewall-cmd --add-service=iscsi-target --zone=internal
success
[uo281847@localhost uoxxxxxx]# targetcli
Warning: Could not load preferences file /root/.targetcli/prefs.bin.
targetcli shell version 2.1.53
Copyright 2011-2013 by Datera, Inc and others.
For help on commands, type 'help'.

/> ls
o- / ..... [Targets: 0]
o- backstores ..... [Storage Objects: 0]
| o- block ..... [Storage Objects: 0]
| o- fileio ..... [Storage Objects: 0]
| o- pscsi ..... [Storage Objects: 0]
| o- ramdisk ..... [Storage Objects: 0]
o- iscsi ..... [Targets: 0]
o- loopback ..... [Targets: 0]
/> cd iscsi
/iscsi> create iqn.2023-02.as.servidor:1111
Created target iqn.2023-02.as.servidor:1111.
Created TPG 1.
Global pref auto_add_default_portal=true
Created default_portal listening on all IPs (0.0.0.0), port 3260.
/iscsi> ls
o- iscsi ..... [Targets: 1]
o- iqn.2023-02.as.servidor:1111 ..... [TPGs: 1]
| o- tpg1 ..... [no-gen-acls, no-auth]
| o- acls ..... [ACLs: 0]
| o- luns ..... [LUNs: 0]
| o- portals ..... [Portals: 1]
| o- 0.0.0.0:3260 ..... [OK]
/iscsi> cd /backstores/block
/backstores/block>

```

A continuación instalar el software, poner en marcha el servicio y abrir el puerto TCP 3260.

```

# dnf -y install targetcli
# systemctl enable --now target
# firewall-cmd --add-service=iscsi-target --zone=internal --permanent
# firewall-cmd --add-service=iscsi-target --zone=internal

```

Antes de configurar el objetivo y el iniciador debemos definir dos IQN. IQN son las iniciales de iSCSI Qualified Name y deben ser únicos. El formato que se emplea (RFC 3720) es iqn.aaaa-mm.mi.dominio:algo, por ejemplo iqn.2023-02.mi.dominio:c3po. Usaremos para el objetivo iqn.2023-02.as.servidor:1111 y para el iniciador iqn.2023-02.as.cliente:2222, nótese que no es necesario que existan los dominios de Internet que se indican, es solo un convenio. A continuación de los ":" puede ponerse cualquier cosa, un número de serie, un nombre de equipo o incluso nada eliminando los dos puntos. En el servidor hay que crear al menos un IQN objetivo, dos objetos para los almacenes de bloques y dos LUN (logical unit number). Opcionalmente pueden definirse más cosas.

```

# targetcli
/> ls
/> cd iscsi
/iscsi> create iqn.2023-02.as.servidor:1111
/iscsi> ls
/iscsi> cd /backstores/block

```

Suponemos que el disco nuevo es /dev/sdb y el fichero imagen de disco es fichero.dsk, se crea cada elemento y se verifica que se ha creado satisfactoriamente.

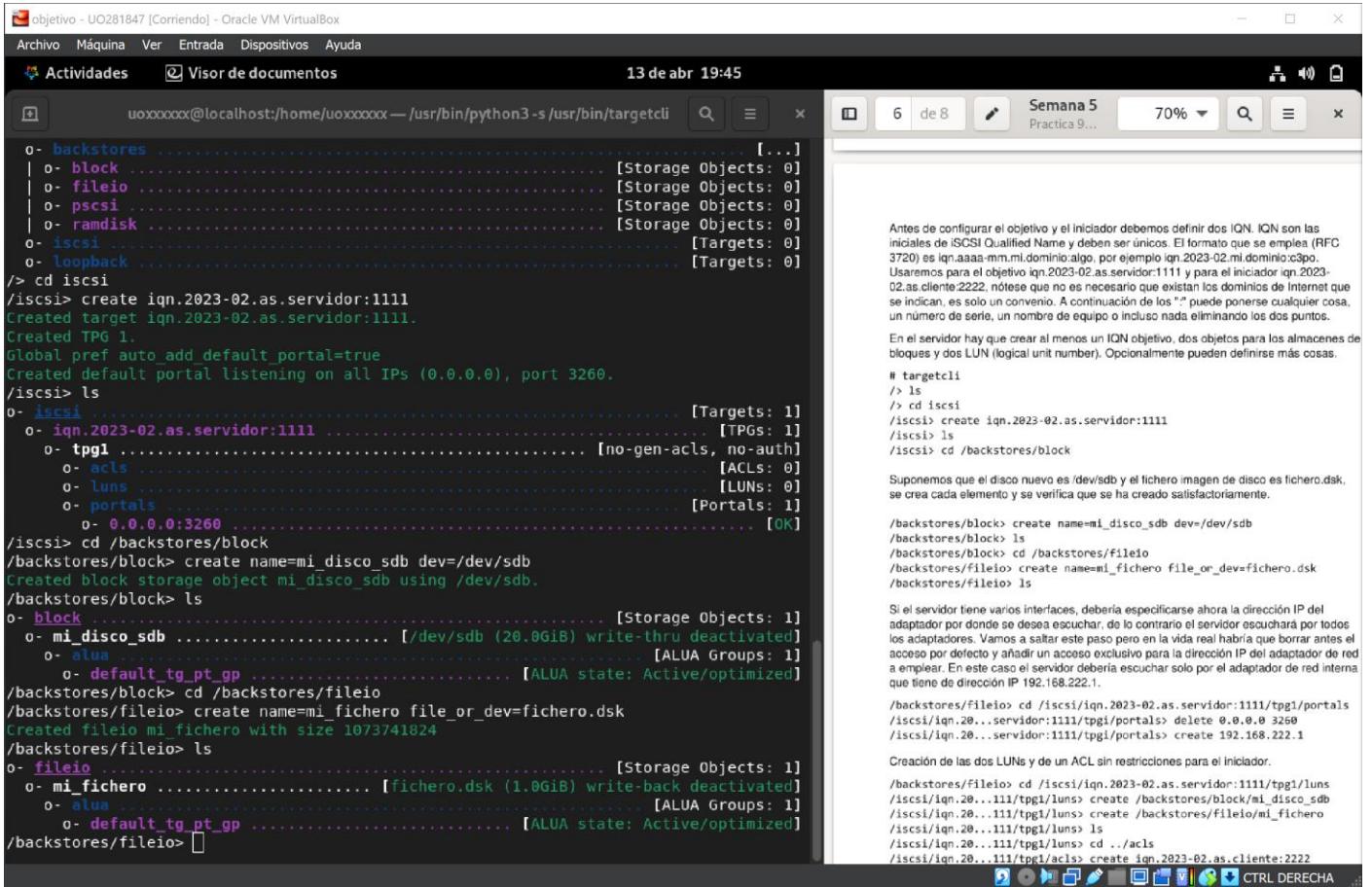
```

/backstores/block> create name=mi_disco_sdb dev=/dev/sdb
/backstores/block> ls
/backstores/block> cd /backstores/fileio
/backstores/fileio> create name=mi_fichero file_or_dev=fichero.dsk
/backstores/fileio> ls

```

Si el servidor tiene varios interfaces, debería especificarse ahora la dirección IP del adaptador por donde se desea escuchar, de lo contrario el servidor escuchará por todos los adaptadores. Vamos a saltar este paso pero en la vida real habrá que borrar antes el acceso por defecto y añadir un acceso exclusivo para la dirección IP del adaptador de red a emplear. En este caso el servidor debería escuchar solo por el adaptador de red interna que tiene de dirección IP 192.168.222.1.

5. Suponemos que el disco nuevo es /dev/sdb y el fichero imagen de disco es fichero.dsk, se crea cada elemento y se verifica que se ha creado satisfactoriamente.



```

objetivo - UO281847 [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Actividades Visor de documentos 13 de abr 19:45
uoxxxxxx@localhost:/home/uoxxxxxx — /usr/bin/python3 -s /usr/bin/targetcli
[...]
o- backstores ..... [Storage Objects: 0]
| o- block ..... [Storage Objects: 0]
| o- fileio ..... [Storage Objects: 0]
| o- pscsi ..... [Storage Objects: 0]
| o- ramdisk ..... [Storage Objects: 0]
o- iscsi ..... [Targets: 0]
o- loopback ..... [Targets: 0]
/> cd iscsi
/iscsi> create iqn.2023-02.as.servidor:1111
Created target iqn.2023-02.as.servidor:1111.
Created TPG 1.
Global pref auto_add_default_portal=true
Created default portal listening on all IPs (0.0.0.0), port 3260.
/iscsi> ls
o- iscsi ..... [Targets: 1]
o- iqn.2023-02.as.servidor:1111 ..... [TPGs: 1]
o- tpg1 ..... [no-gen-acls, no-auth] [ACLs: 0]
o- acls ..... [LUNs: 0] [LUNs: 0]
o- luns ..... [Portals: 1]
o- portals ..... [OK]
o- 0.0.0.0:3260.
/iscsi> cd /backstores/block
/backstores/block> create name=mi_disco_sdb dev=/dev/sdb
Created block storage object mi_disco_sdb using /dev/sdb.
/backstores/block> ls
o- block ..... [Storage Objects: 1]
o- mi_disco_sdb ..... [/dev/sdb (20.0GiB) write-thru deactivated] [ALUA Groups: 1]
o- alua ..... [ALUA state: Active/optimized]
o- default_tg_pt_gp ..... [ALUA state: Active/optimized]
/backstores/block> cd /backstores/fileio
/backstores/fileio> create name=mi_fichero file_or_dev=fichero.dsk
Created fileio mi_fichero with size 1073741824
/backstores/fileio> ls
o- fileio ..... [Storage Objects: 1]
o- mi_fichero ..... [fichero.dsk (1.0GiB) write-back deactivated] [ALUA Groups: 1]
o- alua ..... [ALUA state: Active/optimized]
o- default_tg_pt_gp ..... [ALUA state: Active/optimized]
/backstores/fileio> []

```

Antes de configurar el objetivo y el iniciador debemos definir dos IQN. IQN son las iniciales de iSCSI Qualified Name y deben ser únicos. El formato que se emplea (RFC 3720) es iqn.aaaa-mm.mi.dominio.algo, por ejemplo iqn.2023-02.mi.dominio:c3po. Usaremos para el objetivo iqn.2023-02.as.servidor:1111 y para el iniciador iqn.2023-02.as.cliente:2222, nótense que no es necesario que existan los dominios de Internet que se indican, es solo un convenio. A continuación de los ":" puede ponerse cualquier cosa, un número de serie, un nombre de equipo o incluso nada eliminando los dos puntos. En el servidor hay que crear al menos un IQN objetivo, dos objetos para los almacenes de bloques y dos LUN (logical unit number). Opcionalmente pueden definirse más cosas.

```

# targetcli
> ls
> cd iscsi
/iscsi> create iqn.2023-02.as.servidor:1111
/iscsi> ls
/iscsi> cd /backstores/block

Suponemos que el disco nuevo es /dev/sdb y el fichero imagen de disco es fichero.dsk, se crea cada elemento y se verifica que se ha creado satisfactoriamente.

/backstores/block> create name=mi_disco_sdb dev=/dev/sdb
/backstores/block> ls
/backstores/block> cd /backstores/fileio
/backstores/fileio> create name=mi_fichero file_or_dev=fichero.dsk
/backstores/fileio> ls

Si el servidor tiene varios interfaces, debería especificarse ahora la dirección IP del adaptador por donde se desea escuchar, de lo contrario el servidor escuchará por todos los adaptadores. Vamos a saltar este paso pero en la vida real habría que borrar antes el acceso por defecto y añadir un acceso exclusivo para la dirección IP del adaptador de red a emplear. En este caso el servidor debería escuchar solo por el adaptador de red interna que tiene de dirección IP 192.168.222.1.

/backstores/fileio> cd /iscsi/inq.2023-02.as.servidor:1111/tpg1/portals
/iscsi/inq.2023-02.as.servidor:1111/tpg1/portals> delete 0.0.0.0 3260
/iscsi/inq.2023-02.as.servidor:1111/tpg1/portals> create 192.168.222.1

Creación de las dos LUNs y de un ACL sin restricciones para el iniciador.

/backstores/fileio> cd /iscsi/inq.2023-02.as.servidor:1111/tpg1/luns
/iscsi/inq.2023-02.as.servidor:1111/tpg1/luns> create /backstores/block/mi_disco_sdb
/iscsi/inq.2023-02.as.servidor:1111/tpg1/luns> create /backstores/fileio/mi_fichero
/iscsi/inq.2023-02.as.servidor:1111/tpg1/luns> ls
/iscsi/inq.2023-02.as.servidor:1111/tpg1/luns> cd ..../acls
/iscsi/inq.2023-02.as.servidor:1111/tpg1/acls> create iqn.2023-02.as.cliente:2222

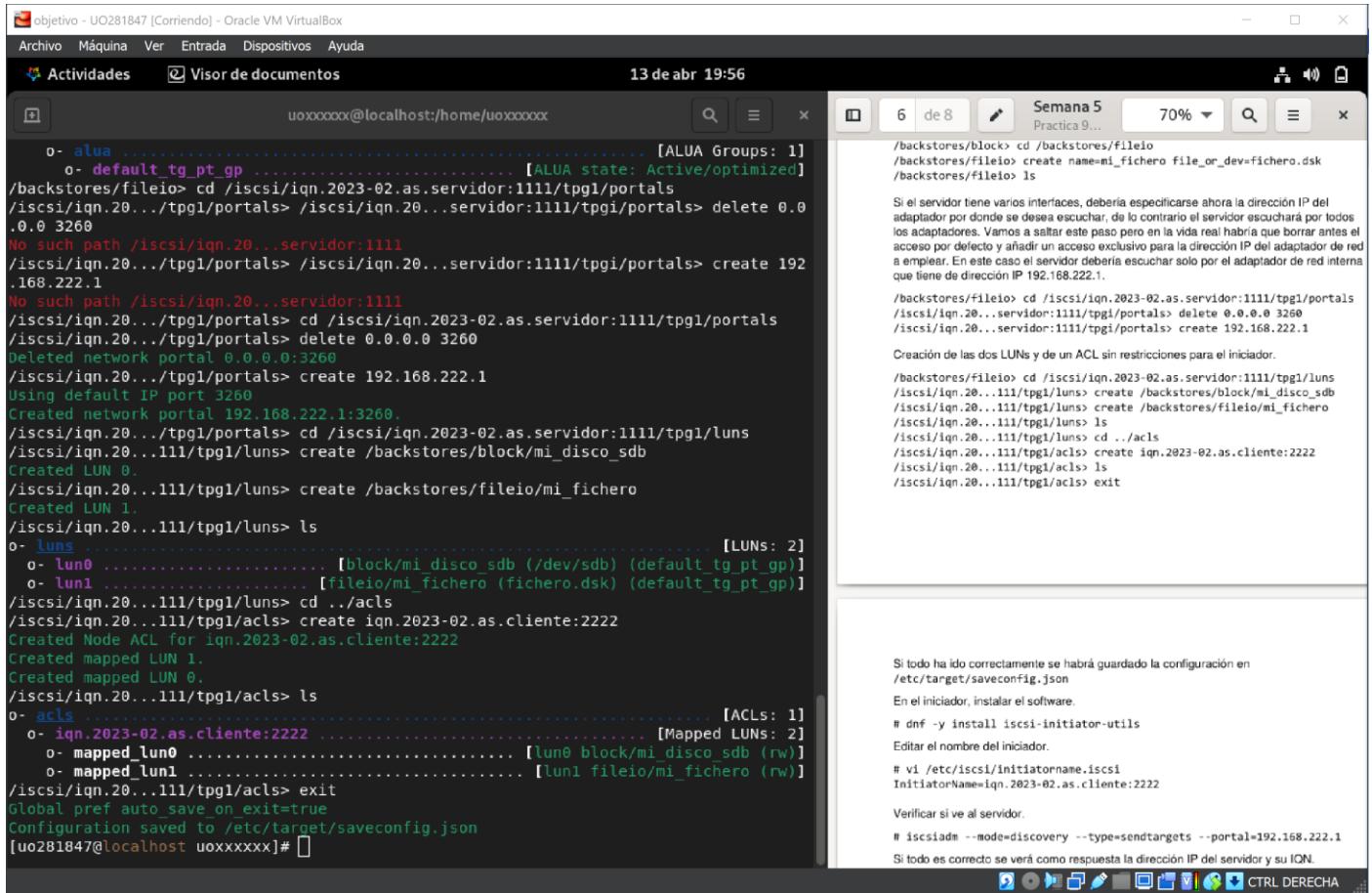
```

6. Si el servidor tiene varios interfaces, debería especificarse ahora la dirección IP del adaptador por donde se desea escuchar, de lo contrario el servidor escuchará por todos los adaptadores. Vamos a saltar este paso pero en la vida real habría que borrar antes el acceso por defecto y añadir un acceso exclusivo para la dirección IP del adaptador de red a emplear. En este caso el servidor debería escuchar solo por el adaptador de red interna que tiene de dirección IP 192.168.222.1.

```

objetivo - UO281847 [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Actividades Visor de documentos 13 de abr 19:46
6 de 8 Semana 5 70% Práctica 9...
iscsi> ls
o- iscsi ...
  o- iqn.2023-02.as.servidor:1111 ...
    o- tpg1 ...
      o- acls ...
      o- luns ...
      o- portals ...
        o- 0.0.0.0:3260 ...
/iscsi> cd /backstores/block
/backstores/block> create name=mi_disco_sdb dev=/dev/sdb
Created block storage object mi_disco_sdb using /dev/sdb.
/backstores/block> ls
o- block ...
  o- mi_disco_sdb ...
    o- alua ...
      o- default_tg_pt_gp ...
/backstores/block> cd /backstores/fileio
/backstores/fileio> create name=mi_fichero file_or_dev=fichero.dsk
Created fileio mi_fichero with size 1073741824
/backstores/fileio> ls
o- fileio ...
  o- mi_fichero ...
    o- alua ...
      o- default_tg_pt_gp ...
/backstores/fileio> cd /iscsi/1qn.2023-02.as.servidor:1111/tpg1/portals
/iscsi/1qn.20.../tpg1/portals> /iscsi/1qn.20...servidor:1111/tpg1/portals> delete 0.0.0.0 3260
No such path /iscsi/1qn.20...servidor:1111
/iscsi/1qn.20.../tpg1/portals> /iscsi/1qn.20...servidor:1111/tpg1/portals> create 192.168.222.1
No such path /iscsi/1qn.20...servidor:1111
/iscsi/1qn.20.../tpg1/portals> cd /iscsi/1qn.2023-02.as.servidor:1111/tpg1/portals
/iscsi/1qn.20.../tpg1/portals> delete 0.0.0.0 3260
Deleted network portal 0.0.0.0:3260
/iscsi/1qn.20.../tpg1/portals> create 192.168.222.1
Using default IP port 3260
Created network portal 192.168.222.1:3260.
/iscsi/1qn.20.../tpg1/portals>
```

7. Creación de las dos LUNs y de un ACL sin restricciones para el iniciador.

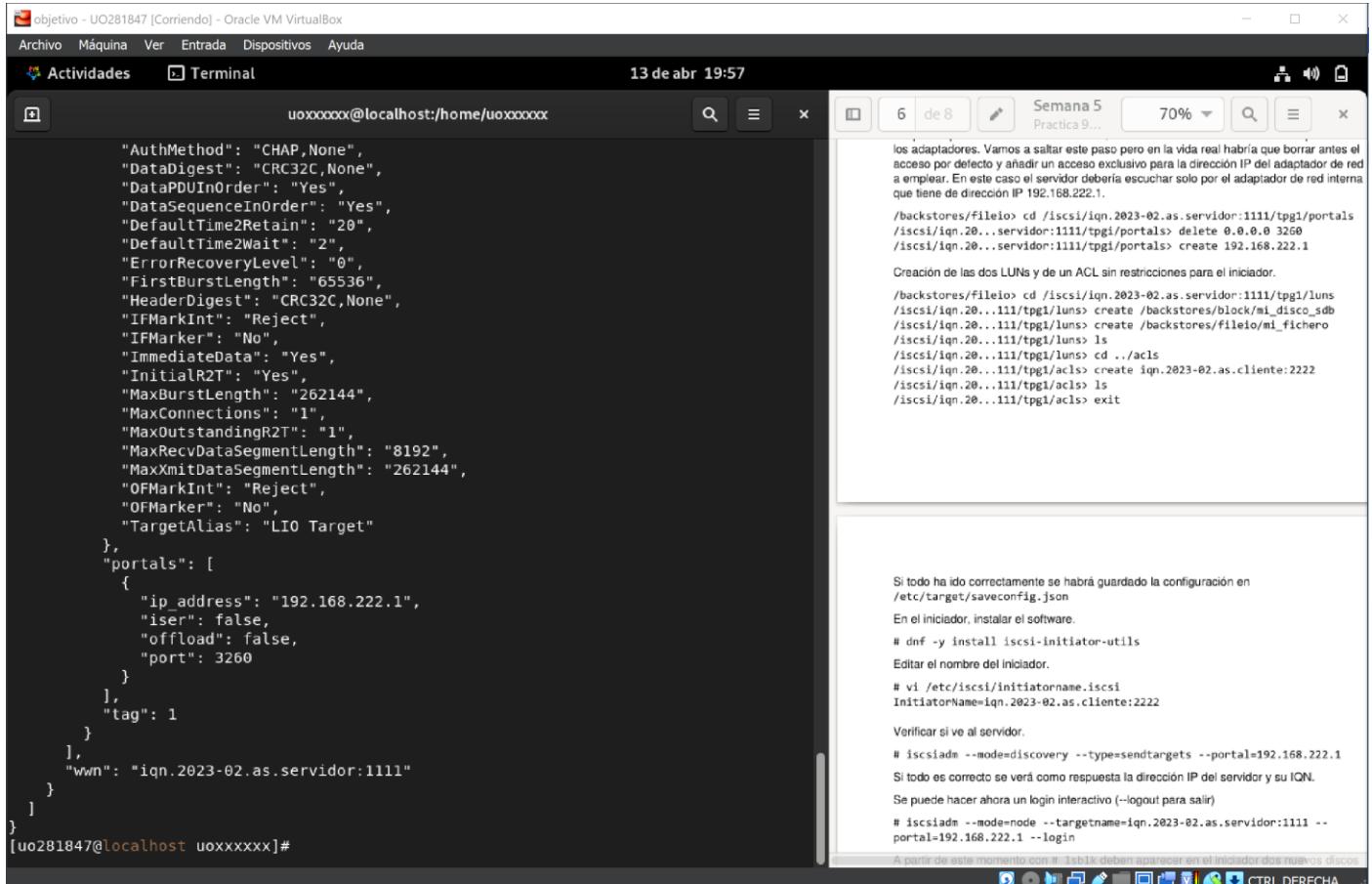


```

objetivo - UO281847 [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Actividades Visor de documentos 13 de abr 19:56
uoxxxxxx@localhost:~# iscsiadm -m node -T iqn.2023-02.as.servidor:1111/tpg1/portals -p 3260 -o alua
o- alua ..... [ALUA Groups: 1]
o- default_tg_pt_gp ..... [ALUA state: Active/optimized]
/backstores/fileio> cd /iscsi/iqn.2023-02.as.servidor:1111/tpg1/portals
/iscsi/iqn.20.../tpg1/portals> /iscsi/iqn.20...servidor:1111/tpg1/portals> delete 0.0.0.0 3260
No such path /iscsi/iqn.20...servidor:1111
/iscsi/iqn.20.../tpg1/portals> /iscsi/iqn.20...servidor:1111/tpg1/portals> create 192.168.222.1
No such path /iscsi/iqn.20...servidor:1111
/iscsi/iqn.20.../tpg1/portals> cd /iscsi/iqn.2023-02.as.servidor:1111/tpg1/portals
/iscsi/iqn.20.../tpg1/portals> delete 0.0.0.0 3260
Deleted network portal 0.0.0.0:3260
/iscsi/iqn.20.../tpg1/portals> create 192.168.222.1
Using default IP port 3260
Created network portal 192.168.222.1:3260.
/iscsi/iqn.20.../tpg1/portals> cd /iscsi/iqn.2023-02.as.servidor:1111/tpg1/luns
/iscsi/iqn.20...111/tpg1/luns> create /backstores/block/mi_disco_sdb
Created LUN 0.
/iscsi/iqn.20...111/tpg1/luns> create /backstores/fileio/mi_fichero
Created LUN 1.
/iscsi/iqn.20...111/tpg1/luns> ls
o- luns ..... [LUNs: 2]
o- lun0 ..... [block/mi_disco_sdb (/dev/sdb) (default_tg_pt_gp)]
o- lun1 ..... [fileio/mi_fichero (fichero.dsk) (default_tg_pt_gp)]
/iscsi/iqn.20...111/tpg1/luns> cd .. /acls
/iscsi/iqn.20...111/tpg1/acls> create iqn.2023-02.as.cliente:2222
Created Node ACL for iqn.2023-02.as.cliente:2222
Created mapped LUN 1.
Created mapped LUN 0.
/iscsi/iqn.20...111/tpg1/acls> ls
o- acls ..... [ACLs: 1]
o- iqn.2023-02.as.cliente:2222 ..... [Mapped LUNs: 2]
o- mapped_lun0 ..... [lun0 block/mi_disco_sdb (rw)]
o- mapped_lun1 ..... [lun1 fileio/mi_fichero (rw)]
/iscsi/iqn.20...111/tpg1/acls> exit
Global pref auto_save_on_exit=true
Configuration saved to /etc/target/saveconfig.json
[uo281847@localhost uoxxxxxx]#

```

8. Si todo ha ido correctamente se habrá guardado la configuración en /etc/target/saveconfig.json.

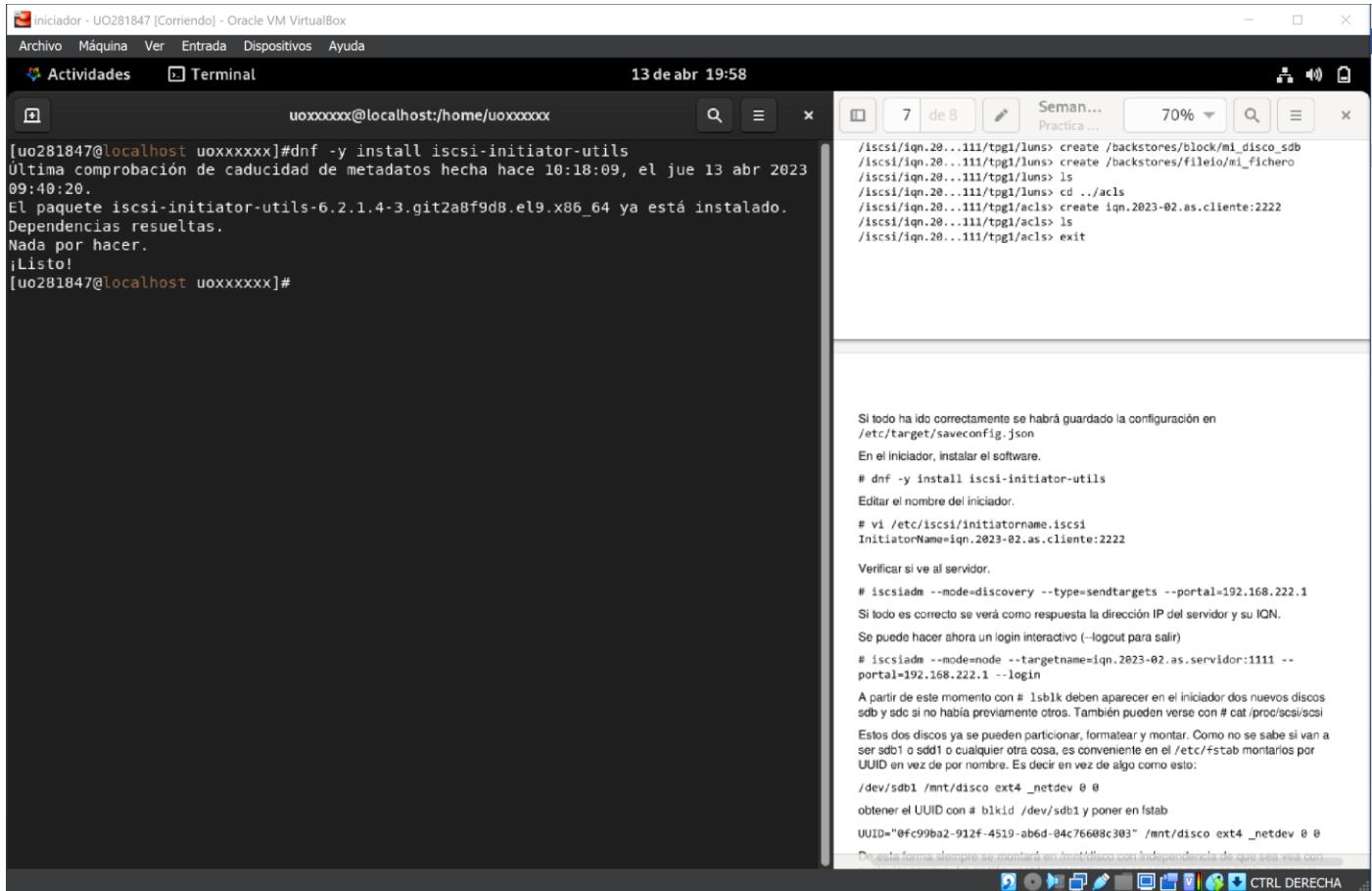


```

objetivo - UO281847 [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Actividades Terminal 13 de abr 19:57
uoxxxxxx@localhost:~# cat /etc/target/saveconfig.json
{
  "AuthMethod": "CHAP,None",
  "DataDigest": "CRC32C,None",
  "DataPDUInOrder": "Yes",
  "DataSequenceInOrder": "Yes",
  "DefaultTime2Retain": "20",
  "DefaultTime2Wait": "2",
  "ErrorRecoveryLevel": "0",
  "FirstBurstLength": "65536",
  "HeaderDigest": "CRC32C,None",
  "IFMarkInt": "Reject",
  "IFMarker": "No",
  "ImmediateData": "Yes",
  "InitialR2T": "Yes",
  "MaxBurstLength": "262144",
  "MaxConnections": "1",
  "MaxOutstandingR2T": "1",
  "MaxRecvDataSegmentLength": "8192",
  "MaxXmitDataSegmentLength": "262144",
  "OFMarkInt": "Reject",
  "OFMarker": "No",
  "TargetAlias": "LIO Target"
},
"portals": [
  {
    "ip_address": "192.168.222.1",
    "iser": false,
    "offload": false,
    "port": 3260
  }
],
"tag": 1
},
"wwn": "iqn.2023-02.as.servidor:1111"
}
[uo281847@localhost uoxxxxxx]#

```

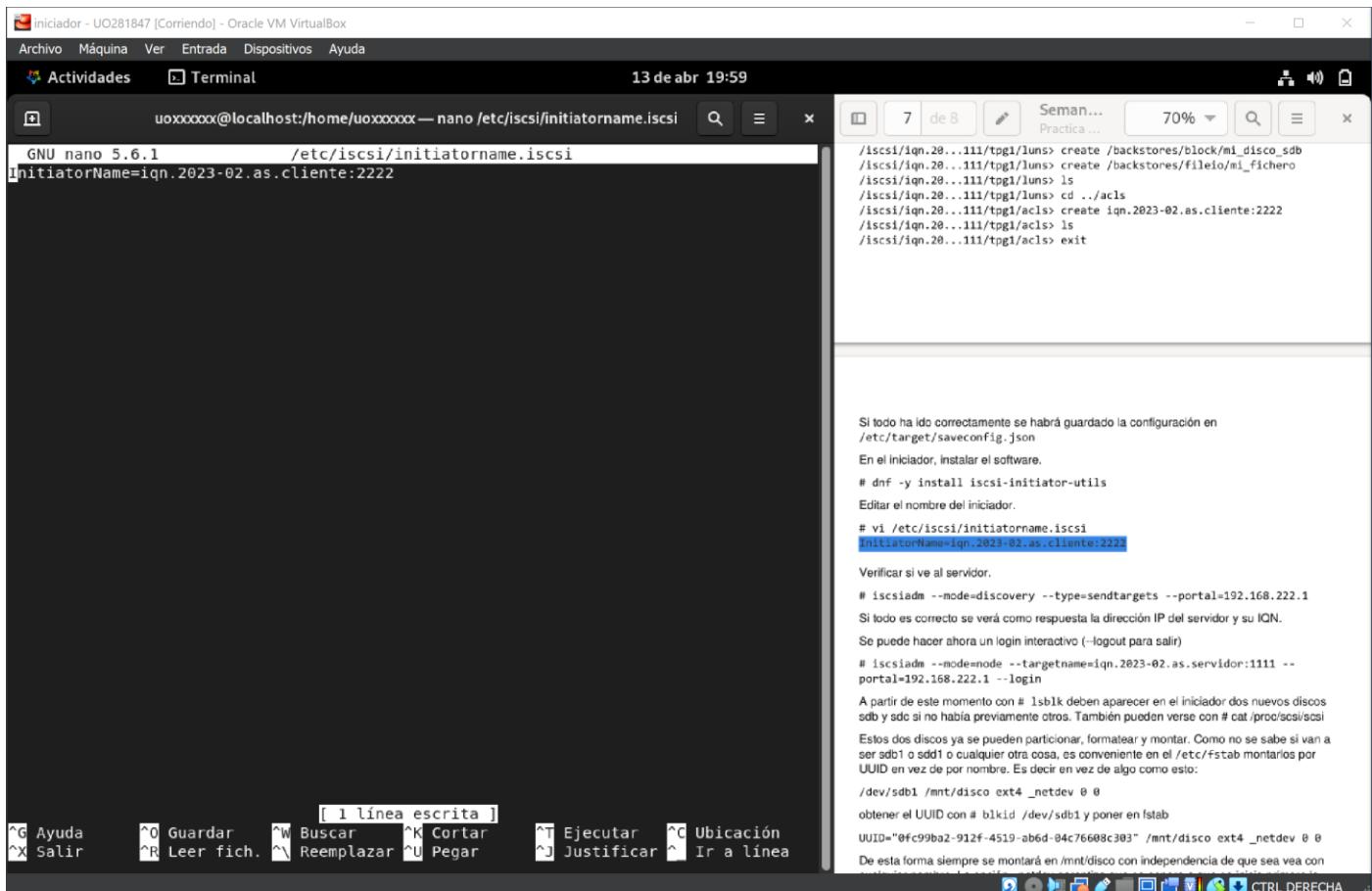
9. En el iniciador, instalar el software.



```
[uoxxxxxx@localhost uoxxxxxx]# dnf -y install iscsi-initiator-utils
Última comprobación de caducidad de metadatos hecha hace 10:18:09, el jue 13 abr 2023
09:40:20.
El paquete iscsi-initiator-utils-6.2.1.4-3.git2a8f9d8.el9.x86_64 ya está instalado.
Dependencias resueltas.
Nada por hacer.
¡Listo!
[uoxxxxxx@localhost uoxxxxxx]#
```

Si todo ha ido correctamente se habrá guardado la configuración en /etc/target/saveconfig.json
En el iniciador, instalar el software.
dnf -y install iscsi-initiator-utils
Editar el nombre del iniciador.
vi /etc/iscsi/initiatorname.iscsi
InitiatorName=iqn.2023-02.as.cliente:2222
Verificar si ve al servidor.
iscsiadm --mode=discovery --type=sendtargets --portal=192.168.222.1
Si todo es correcto se verá como respuesta la dirección IP del servidor y su IQN.
Se puede hacer ahora un login interactivo (-logout para salir)
iscsiadm --mode=node --targetname=iqn.2023-02.as.servidor:1111 --
portal=192.168.222.1 --login
A partir de este momento con # lsblk deben aparecer en el iniciador dos nuevos discos sdb y sdc si no había previamente otros. También pueden verse con # cat /proc/scsi/scsi
Estos dos discos ya se pueden particionar, formatear y montar. Como no se sabe si van a ser sdb1 o sdd1 o cualquier otra cosa, es conveniente en el /etc/fstab montarlos por UUID en vez de por nombre. Es decir en vez de algo como esto:
/dev/sdb1 /mnt/disco ext4 _netdev 0 0
obtener el UUID con # blkid /dev/sdb1 y poner en fstab
UUID="0fc99ba2-912f-4519-ab6d-04c76608c303" /mnt/disco ext4 _netdev 0 0
De esta forma siempre se montará en /mnt/disco con independencia de que sea vía con

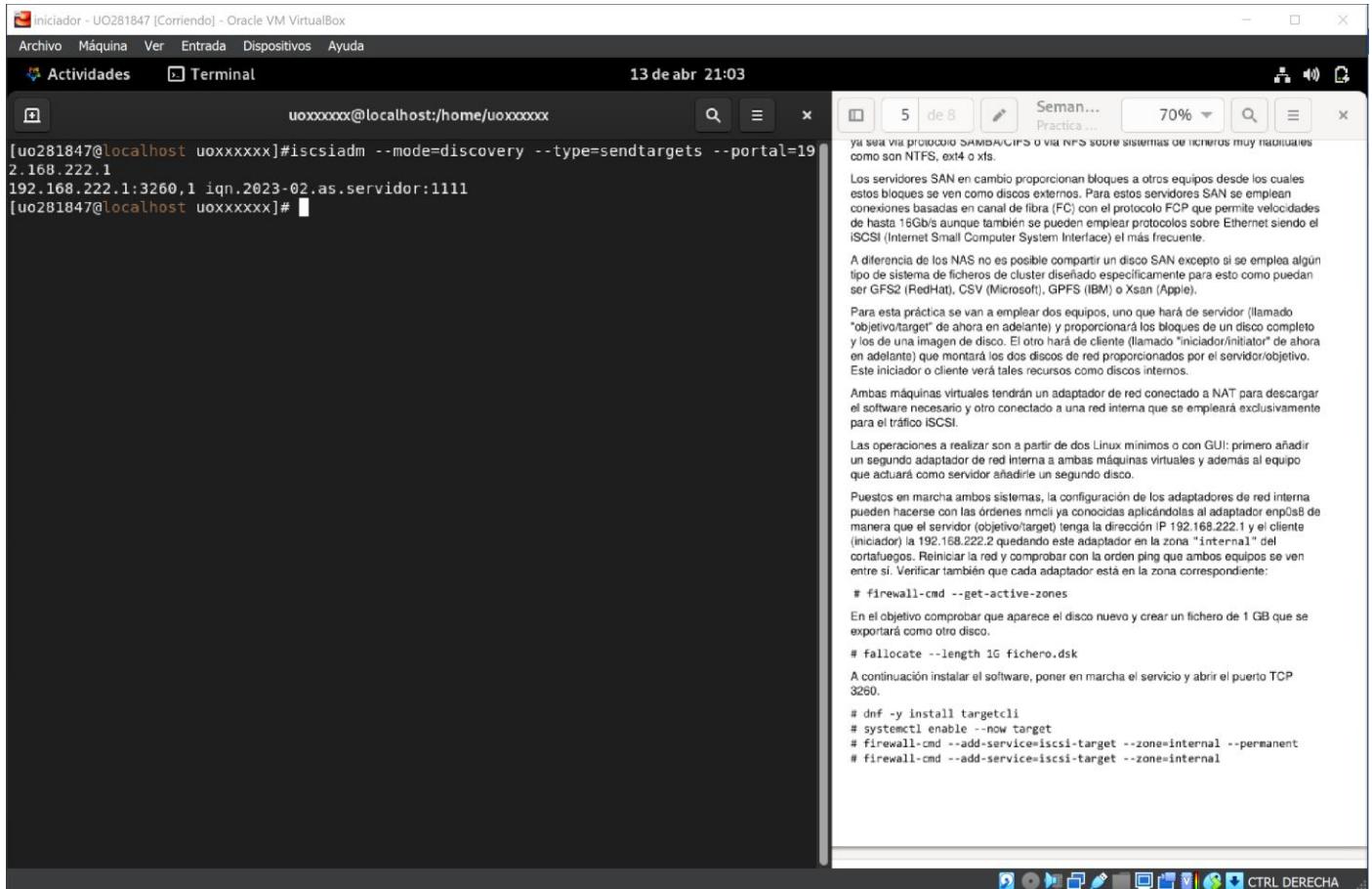
10. Editar el nombre del iniciador.



```
GNU nano 5.6.1          /etc/iscsi/initiatorname.iscsi
InitiatorName=iqn.2023-02.as.cliente:2222
```

Si todo ha ido correctamente se habrá guardado la configuración en /etc/target/saveconfig.json
En el iniciador, instalar el software.
dnf -y install iscsi-initiator-utils
Editar el nombre del iniciador.
vi /etc/iscsi/initiatorname.iscsi
InitiatorName=iqn.2023-02.as.cliente:2222
Verificar si ve al servidor.
iscsiadm --mode=discovery --type=sendtargets --portal=192.168.222.1
Si todo es correcto se verá como respuesta la dirección IP del servidor y su IQN.
Se puede hacer ahora un login interactivo (-logout para salir)
iscsiadm --mode=node --targetname=iqn.2023-02.as.servidor:1111 --
portal=192.168.222.1 --login
A partir de este momento con # lsblk deben aparecer en el iniciador dos nuevos discos sdb y sdc si no había previamente otros. También pueden verse con # cat /proc/scsi/scsi
Estos dos discos ya se pueden particionar, formatear y montar. Como no se sabe si van a ser sdb1 o sdd1 o cualquier otra cosa, es conveniente en el /etc/fstab montarlos por UUID en vez de por nombre. Es decir en vez de algo como esto:
/dev/sdb1 /mnt/disco ext4 _netdev 0 0
obtener el UUID con # blkid /dev/sdb1 y poner en fstab
UUID="0fc99ba2-912f-4519-ab6d-04c76608c303" /mnt/disco ext4 _netdev 0 0
De esta forma siempre se montará en /mnt/disco con independencia de que sea vía con

11. Verificar si ve al servidor.



```
u0xxxxx@localhost:~$ iscsiadm --mode=discovery --type=senttargets --portal=192.168.222.1:3260,1 iqn.2023-02.as.servidor:1111
[ u0xxxxx@localhost:~$ ] #
```

Los servidores SAN en cambio proporcionan bloques a otros equipos desde los cuales estos bloques se ven como discos internos. Para estos servidores SAN se emplean conexiones basadas en canal de fibra (FC) con el protocolo FCP que permite velocidades de hasta 15Gb/s aunque también se pueden emplear protocolos sobre Ethernet siendo el iSCSI (Internet Small Computer System Interface) el más frecuente.

A diferencia de los NAS no es posible compartir un disco SAN excepto si se emplea algún tipo de sistema de ficheros de cluster diseñado específicamente para esto como puedan ser GFS2 (RedHat), CSV (Microsoft), GPFS (IBM) o Xsan (Apple).

Para esta práctica se van a emplear dos equipos, uno que hará de servidor (llamado "objetivo/target" de ahora en adelante) y proporcionará los bloques de un disco completo y los de una imagen de disco. El otro hará de cliente (llamado "iniciador/initiator" de ahora en adelante) que montará los dos discos de red proporcionados por el servidor/objetivo. Este iniciador o cliente verá tales recursos como discos internos.

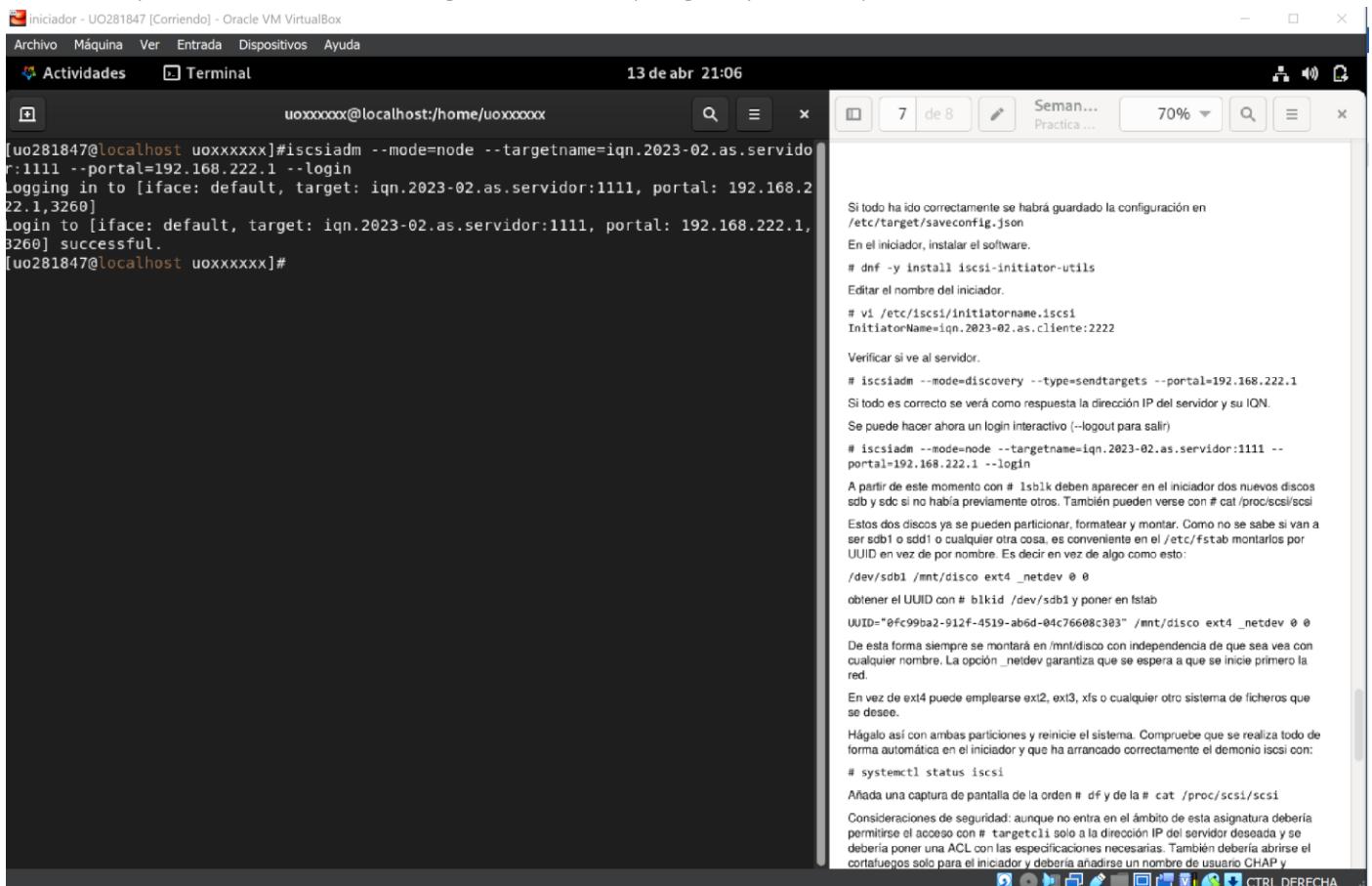
Ambas máquinas virtuales tendrán un adaptador de red conectado a NAT para descargar el software necesario y otro conectado a una red interna a ambas máquinas virtuales y además al equipo que actuará como servidor añadirá un segundo disco.

Las operaciones a realizar son a partir de dos Linux mínimos o con GUI: primero añadir un segundo adaptador de red interna a ambas máquinas virtuales y además al equipo que actuará como servidor añadirá un segundo disco.

Puestos en marcha ambos sistemas, la configuración de los adaptadores de red interna pueden hacerse con las órdenes nmcli ya conocidas aplicándolas al adaptador empújalo de manera que el servidor (objetivo/target) tenga la dirección IP 192.168.222.1 y el cliente (iniciador) la 192.168.222.2 quedando este adaptador en la zona "internal" del cortafuegos. Reiniciar la red y comprobar con la orden ping que ambos equipos se ven entre sí. Verificar también que cada adaptador está en la zona correspondiente:

```
# firewall-cmd --get-active-zones
En el objetivo comprobar que aparece el disco nuevo y crear un fichero de 1 GB que se exportará como otro disco.
# fallocate --length 1G fichero.dsk
A continuación instalar el software, poner en marcha el servicio y abrir el puerto TCP 3260.
# dnf -y install targetcli
# systemctl enable --now target
# firewall-cmd --add-service=iscsi-target --zone=internal --permanent
# firewall-cmd --add-service=iscsi-target --zone=internal
```

12. Si todo es correcto se verá como respuesta la dirección IP del servidor y su IQN. Se puede hacer ahora un login interactivo (--logout para salir)



```
u0xxxxx@localhost:~$ iscsiadm --mode=node --targetname=iqn.2023-02.as.servidor:1111 --portal=192.168.222.1 --login
Logging in to [iface: default, target: iqn.2023-02.as.servidor:1111, portal: 192.168.222.1,3260]
Login to [iface: default, target: iqn.2023-02.as.servidor:1111, portal: 192.168.222.1,3260] successful.
[ u0xxxxx@localhost:~$ ] #
```

Si todo ha ido correctamente se habrá guardado la configuración en /etc/target/saveconfig.json

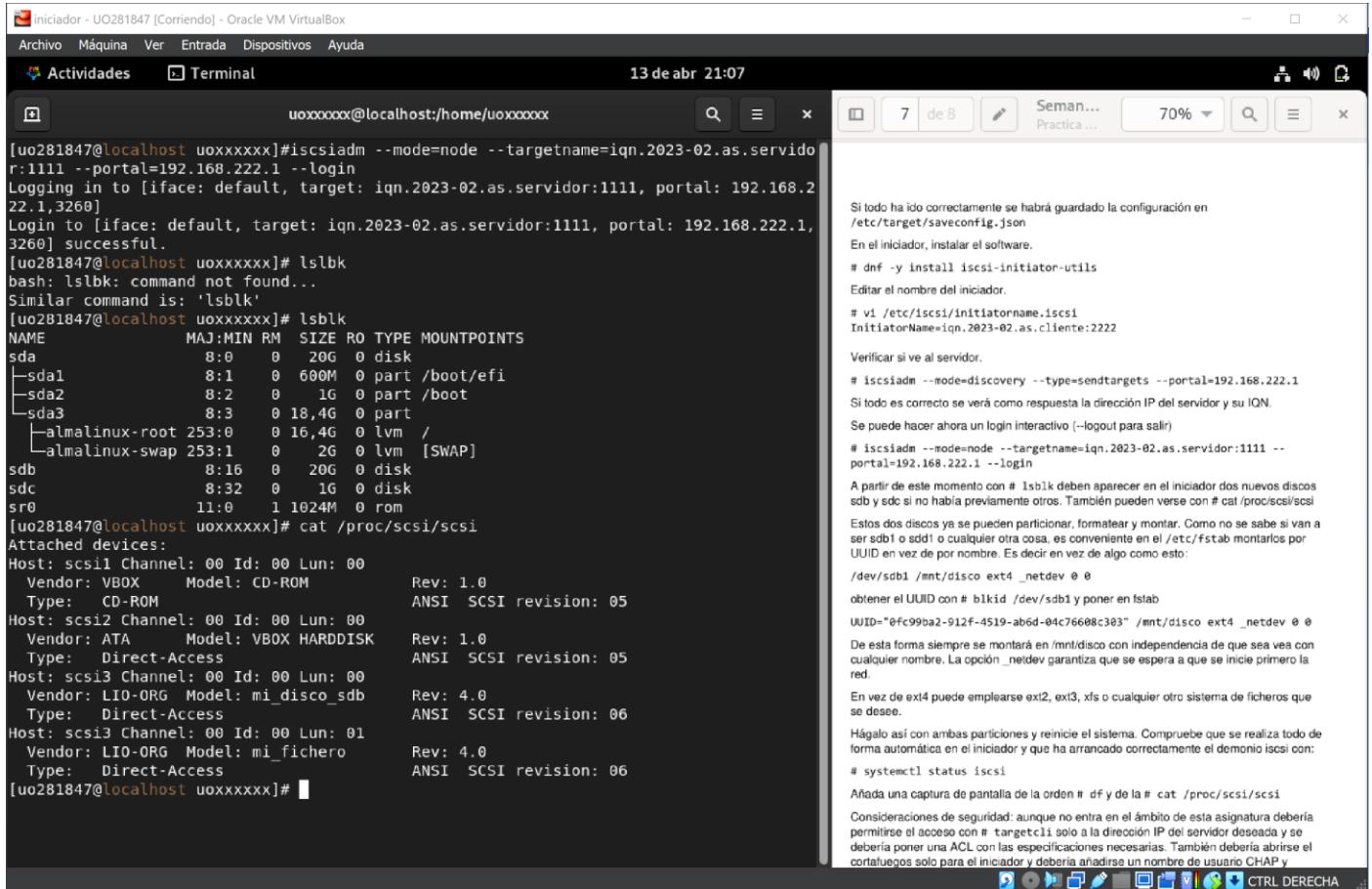
En el iniciador, instalar el software.

```
# dnf -y install iscsi-initiator-utils
Editar el nombre del iniciador.
# vi /etc/iscsi/initiatorname.iscsi
InitiatorName=iqn.2023-02.as.cliente:2222
```

Verificar si ve al servidor.

```
# iscsiadm --mode=discovery --type=senttargets --portal=192.168.222.1
Si todo es correcto se verá como respuesta la dirección IP del servidor y su IQN.
Se puede hacer ahora un login interactivo (--logout para salir)
# iscsiadm --mode=node --targetname=iqn.2023-02.as.servidor:1111 --portal=192.168.222.1 --login
A partir de este momento con # lsblk deben aparecer en el iniciador dos nuevos discos sdb y sdc si no había previamente otros. También pueden verse con # cat /proc/scsi/scsi
Estos dos discos ya se pueden particionar, formatear y montar. Como no se sabe si van a tener sdb1 o sdd1 o cualquier otra cosa es conveniente en el /etc/fstab montarlos por UUID en vez de por nombre. Es decir en vez de algo como esto:
/dev/sdb1 /mnt/disco ext4 _netdev 0 0
obtener el UUID con # blkid /dev/sdb1 y poner en fstab
UUID="0fc99ba2-912f-4519-ab6d-94c76608c303" /mnt/disco ext4 _netdev 0 0
De esta forma siempre se montará en /mnt/disco con independencia de que sea vea con cualquier nombre. La opción _netdev garantiza que se espera a que se inicie primero la red.
En vez de ext4 puede emplearse ext2, ext3, xfs o cualquier otro sistema de ficheros que se desee.
Hágalo así con ambas particiones y reinicie el sistema. Compruebe que se realiza todo de forma automática en el iniciador y que ha arrancado correctamente el demonio iscsi con:
# systemctl status iscsi
Añada una captura de pantalla de la orden # df y de la # cat /proc/scsi/scsi
Consideraciones de seguridad: aunque no entra en el ámbito de esta asignatura debería permitir el acceso con # targetcli solo a la dirección IP del servidor deseada y se debería poner una ACL con las especificaciones necesarias. También debería abrirse el cortafuegos solo para el iniciador y debería añadirse un nombre de usuario CHAP y
```

13. A partir de este momento con # lsblk deben aparecer en el iniciador dos nuevos discos sdb y sdc si no había previamente otros. También pueden verse con # cat /proc/scsi/scsi.



```
iniciador - UO281847 [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Actividades Terminal 13 de abr 21:07
u0xxxxx@localhost:~$ lsblk
[...]
[lu0281847@localhost u0xxxxx]# lsblk
bash: lsblk: command not found...
Similar command is: 'lsblk'
[lu0281847@localhost u0xxxxx]# lsblk
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINTS
sda 8:0 0 20G 0 disk
└─sda1 8:1 0 600M 0 part /boot/efi
sda2 8:2 0 16 0 part /boot
└─sda3 8:3 0 18,4G 0 part
  ├─almalinux-root 253:0 0 16,4G 0 lvm /
  └─almalinux-swap 253:1 0 2G 0 lvm [SWAP]
sdb 8:16 0 20G 0 disk
sdc 8:32 0 16 0 disk
sr0 11:0 1 1024M 0 rom
[lu0281847@localhost u0xxxxx]# cat /proc/scsi/scsi
Attached devices:
Host: scsil Channel: 00 Id: 00 Lun: 00
  Vendor: VBOX Model: CD-ROM
  Type: CD-ROM
Host: scsi2 Channel: 00 Id: 00 Lun: 00
  Vendor: ATA Model: VBOX HARDDISK
  Type: Direct-Access
Host: scsi3 Channel: 00 Id: 00 Lun: 00
  Vendor: LIO-ORG Model: mi_disco_sdb
  Type: Direct-Access
Host: scsi3 Channel: 00 Id: 00 Lun: 01
  Vendor: LIO-ORG Model: mi_fichero
  Type: Direct-Access
[lu0281847@localhost u0xxxxx]# 
```

Si todo ha ido correctamente se habrá guardado la configuración en /etc/target/saveconfig.json
En el iniciador, instalar el software.
dnf -y install iscsi-initiator-utils
Editar el nombre del iniciador.
vi /etc/iscsi/InitiatorName.iscsi
InitiatorName=iqn.2023-02.as.cliente:2222
Verificar si ve al servidor.
iscsadm --mode=discover --type=sendtargets --portal=192.168.222.1
Si todo es correcto se verá como respuesta la dirección IP del servidor y su IQN.
Se puede hacer ahora un login interactivo (-logout para salir)
iscsadm --mode=node --targetname=iqn.2023-02.as.servidor:1111 --portal=192.168.222.1 --login
A partir de este momento con # lsblk deben aparecer en el iniciador dos nuevos discos sdb y sdc si no había previamente otros. También pueden verse con # cat /proc/scsi/scsi
Estos dos discos ya se pueden particionar, formatear y montar. Como no se sabe si van a ser sdb1 o sdd1 o cualquier otra cosa, es conveniente en el /etc/fstab montarlos por UUID en vez de por nombre. Es decir en vez de algo como esto:
/dev/sdb1 /mnt/disco ext4 _netdev 0 0
obtener el UUID con # blkid /dev/sdb1 y poner en fstab
UUID="0fc99ba2-912f-4519-ab6d-04c76608c303" /mnt/disco ext4 _netdev 0 0
De esta forma siempre se montará en /mnt/disco con independencia de que sea vía con cualquier nombre. La opción _netdev garantiza que se espera a que se inicie primera la red.
En vez de ext4 puede emplearse ext2, ext3, xfs o cualquier otro sistema de ficheros que se deseé.
Hágalo así con ambas particiones y reinicie el sistema. Compruebe que se realiza todo de forma automática en el iniciador y que ha arrancado correctamente el demonio iscsi con:
systemctl status iscsi
Añada una captura de pantalla de la orden # df y de la # cat /proc/scsi/scsi
Consideraciones de seguridad: aunque no entra en el ámbito de esta asignatura debería permitirse el acceso con # targetcli solo a la dirección IP del servidor deseada y se debería poner una ACL con las especificaciones necesarias. También debería abrirse el cortafuegos solo para el iniciador y debería añadirse un nombre de usuario CHAP y

14. Estos dos discos ya se pueden particionar, formatear y montar. Como no se sabe si van a ser sdb1 o sdd1 o cualquier otra cosa, es conveniente en el /etc/fstab montarlos por UUID en vez de por nombre. Obtener el UUID con blkid /dev/sdb1 y poner en fstab
 UUID="0fc99ba2-912f-4519-ab6d-04c76608c303" /mnt/disco ext4 _netdev 0 0
 De esta forma siempre se montará en /mnt/disco con independencia de que sea vea con cualquier nombre. La opción _netdev garantiza que se espera a que se inicie primero la red. En vez de ext4 puede emplearse ext2, ext3, xfs o cualquier otro sistema de ficheros que se desee. Hágalo así con ambas particiones y reinicie el sistema. Compruebe que se realiza todo de forma automática en el iniciador y que ha arrancado correctamente el demonio iscsi.

```

iniciador - UO281847 [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Actividades Terminal 13 de abr 21:22
uoxxxxxx@localhost:~$ blkid /dev/sdb1
/dev/sdb1: UUID="77958db3-6099-48d9-91bf-201067342390" TYPE="ext4" PARTLABEL="Linux filesystem" PARTUUID="80300a4f-bb89-4f8f-bd0c-26ec8151e3cc"
[uo281847@localhost uoxxxxxx]#

```

7 de 8 Semana... Práctica ... 70% 🔍

```

/etc/iscsi/saveconfig.json
En el iniciador, instalar el software.
# dnf -y install iscsi-initiator-utils
Editar el nombre del iniciador.
# vi /etc/iscsi/initiatorname.iscsi
InitiatorName=iqn.2023-02.as.cliente:2222

Verificar si ve al servidor.
# iscsiadm --mode=discovery --type=sendtargets --portal=192.168.222.1
Si todo es correcto se verá como respuesta la dirección IP del servidor y su IQN.
Se puede hacer ahora un login interactivo (-logout para salir)
# iscsiadm --mode=node --targetname=iqn.2023-02.as.servidor:1111 --portal=192.168.222.1 --login
A partir de este momento con # lsblk deben aparecer en el iniciador los nuevos discos sdb y sdc si no había previamente otros. También pueden verse con # cat /proc/scsi/scsi
Estos dos discos ya se pueden particionar, formatear y montar. Como no se sabe si van a ser sdb1 o sdd1 o cualquier otra cosa, es conveniente en el /etc/fstab montarlos por UUID en vez de por nombre. Es decir en vez de algo como esto:
/dev/sdb1 /mnt/disco ext4 _netdev 0 0
obtener el UUID con # blkid /dev/sdb1 y poner en fstab
UUID="0fc99ba2-912f-4519-ab6d-04c76608c303" /mnt/disco ext4 _netdev 0 0
De esta forma siempre se montará en /mnt/disco con independencia de que sea vea con cualquier nombre. La opción _netdev garantiza que se espera a que se inicie primero la red.
En vez de ext4 puede emplearse ext2, ext3, xfs o cualquier otro sistema de ficheros que se desee.
Hágalo así con ambas particiones y reinicie el sistema. Compruebe que se realiza todo de forma automática en el iniciador y que ha arrancado correctamente el demonio iscsi con:
# systemctl status iscsi
Añada una captura de pantalla de la orden # df y de la # cat /proc/scsi/scsi
Consideraciones de seguridad: aunque no entra en el ámbito de esta asignatura debería permitir el acceso con # targetcli solo a la dirección IP del servidor deseada y se debería poner una ACL con las especificaciones necesarias. También debería abrirse el cortafuegos solo para el iniciador y debería añadirse un nombre de usuario CHAP y contraseña, tanto en el servidor como en el iniciador.

```

iniciador - UO281847 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Actividades Terminal 13 de abr 21:36

uoxxxxxx@localhost:/home/uoxxxxxx — nano /etc/fstab

GNU nano 5.6.1 /etc/fstab

```

#
# /etc/fstab
# Created by anaconda on Mon Mar  6 09:45:11 2023
#
# Accessible filesystems, by reference, are maintained under '/dev/disk/'.
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info.
#
# After editing this file, run 'systemctl daemon-reload' to update systemd
# units generated from this file.
#
/dev/mapper/almalinux-root / xfs defaults 0 0
UUID=078b1739-b878-45f3-97c9-c40daace99e0 /boot xfs defaults >
UUID=624D-BBA2 /boot/efi vfat umask=0077,shortname=winnt 0 2
UUID=77958db3-6099-48d9-91bf-201067342390 /mnt/disco ext4 _netdev 0 0
UUID=76ed02d2-d707-4213-9691-a8389462c143 /mnt/disco ext4 _netdev 0 0
/dev/mapper/almalinux-swap none swap defaults 0 0

```

[17 líneas escritas]

^6 Ayuda ^0 Guardar ^W Buscar ^K Cortar ^T Ejecutar ^C Ubicación
 ^X Salir ^R Leer fich. ^\ Reemplazar ^U Pegar ^J Justificar ^I Ir a línea

Si todo ha ido correctamente se habrá guardado la configuración en /etc/target/saveconfig.json
 En el iniciador, instalar el software.
 # dnf -y install iscsi-initiator-utils
 Editar el nombre del iniciador.
 # vi /etc/iscsi/initiatorname.iscsi
 InitiatorName=ign.2023-02.as.cliente:2222
 Verificar si ve al servidor.
 # iscsiadm --mode=discovery --type=senttargets --portal=192.168.222.1
 Si todo es correcto se verá como respuesta la dirección IP del servidor y su IQN.
 Se puede hacer ahora un login interactivo (-logout para salir)
 # iscsiadm - -mode=node --targetname=ign.2023-02.as.servidor:1111 --
 portal=192.168.222.1 --login
 A partir de este momento con # lsblk deben aparecer en el iniciador los nuevos discos sdb y sdc si no había previamente otros. También pueden verse con # cat /proc/scsi/scsi
 Estos dos discos ya se pueden particionar, formatear y montar. Como no se sabe si van a ser sdb1 o sdd1 o cualquier otra cosa, es conveniente en el /etc/fstab montarlos por UUID en vez de por nombre. Es decir en vez de algo como esto:
 #/dev/sdb1 /mnt/disco ext4 _netdev 0 0
 obtener el UUID con # blkid /dev/sdb1 y poner en fstab
 UUID="0fc99ba2-912f-4519-ab6d-04c7668c303" /mnt/disco ext4 _netdev 0 0
 De esta forma siempre se montará en /mnt/disco con independencia de que sea vía con cualquier nombre. La opción _netdev garantiza que se espera a que se inicie primera la red.
 En vez de ext4 puede emplearse ext2, ext3, xfs o cualquier otro sistema de ficheros que se desee.
 Hágalo así con ambas particiones y reinicie el sistema. Compruebe que se realiza todo de forma automática en el iniciador y que ha arrancado correctamente el demonio iscsi con:
 # systemctl status iscsi
 Añada una captura de pantalla de la orden # df y de la # cat /proc/scsi/scsi
 Consideraciones de seguridad: aunque no entra en el ámbito de esta asignatura debería permitirse el acceso con # targetcli solo a la dirección IP del servidor deseada y se debería poner una ACL con las especificaciones necesarias. También debería abrirse el cortafuegos solo para el iniciador y debería añadirse un nombre de usuario CHAP y contraseña, tanto en el servidor como en el iniciador.

CTRL DERECHA

iniciador - UO281847 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Actividades Visor de documentos 13 de abr 21:38

uoxxxxxx@localhost:~\$ su root
 Contraseña:

```

[uo281847@localhost uoxxxxxx]# systemctl status iscsi
● iscsi.service - Login and scanning of iSCSI devices
  Loaded: loaded (/usr/lib/systemd/system/iscsi.service; enabled; vendor preset: enabled)
  Active: active (exited) since Thu 2023-04-13 21:37:06 CEST; 1min 3s ago
    Docs: man:iscsiadm(8)
          man:iscsid(8)
  Process: 999 ExecStart=/usr/sbin/iscsiadm -m node --loginall=automatic (code=exited, status=0/SUCCESS)
  Main PID: 999 (code=exited, status=0/SUCCESS)
    CPU: 3ms

abr 13 21:37:06 localhost.localdomain systemd[1]: Starting Login and scanning of iSCSI...
abr 13 21:37:06 localhost.localdomain systemd[1]: Finished Login and scanning of iSCSI...
abr 13 21:37:06 localhost.localdomain iscsid[999]: Logging in to [iface: default, target: ign.2023-02.as.cliente:2222]
abr 13 21:37:06 localhost.localdomain iscsid[999]: Login to [iface: default, target: ign.2023-02.as.cliente:2222]
[lines 1-13/13 (END)]

```

vi /etc/iscsi/initiatorname.iscsi
 InitiatorName=ign.2023-02.as.cliente:2222
 Verificar si ve al servidor.
 # iscsiadm --mode=discovery --type=senttargets --portal=192.168.222.1
 Si todo es correcto se verá como respuesta la dirección IP del servidor y su IQN.
 Se puede hacer ahora un login interactivo (-logout para salir)
 # iscsiadm --mode=node --targetname=ign.2023-02.as.servidor:1111 --
 portal=192.168.222.1 --login
 A partir de este momento con # lsblk deben aparecer en el iniciador los nuevos discos sdb y sdc si no había previamente otros. También pueden verse con # cat /proc/scsi/scsi
 Estos dos discos ya se pueden particionar, formatear y montar. Como no se sabe si van a ser sdb1 o sdd1 o cualquier otra cosa, es conveniente en el /etc/fstab montarlos por UUID en vez de por nombre. Es decir en vez de algo como esto:
 #/dev/sdb1 /mnt/disco ext4 _netdev 0 0
 obtener el UUID con # blkid /dev/sdb1 y poner en fstab
 UUID="0fc99ba2-912f-4519-ab6d-04c7668c303" /mnt/disco ext4 _netdev 0 0
 De esta forma siempre se montará en /mnt/disco con independencia de que sea vía con cualquier nombre. La opción _netdev garantiza que se espera a que se inicie primera la red.
 En vez de ext4 puede emplearse ext2, ext3, xfs o cualquier otro sistema de ficheros que se desee.
 Hágalo así con ambas particiones y reinicie el sistema. Compruebe que se realiza todo de forma automática en el iniciador y que ha arrancado correctamente el demonio iscsi con:
 # systemctl status iscsi
 Añada una captura de pantalla de la orden # df y de la # cat /proc/scsi/scsi
 Consideraciones de seguridad: aunque no entra en el ámbito de esta asignatura debería permitirse el acceso con # targetcli solo a la dirección IP del servidor deseada y se debería poner una ACL con las especificaciones necesarias. También debería abrirse el cortafuegos solo para el iniciador y debería añadirse un nombre de usuario CHAP y contraseña, tanto en el servidor como en el iniciador.

CTRL DERECHA

15. Añada una captura de pantalla de la orden `df` y de la `cat /proc/scsi/scsi`

Consideraciones de seguridad: aunque no entra en el ámbito de esta asignatura debería permitirse el acceso con `targetcli` solo a la dirección IP del servidor deseada y se debería poner una ACL con las especificaciones necesarias. También debería abrirse el cortafuegos solo para el iniciador y debería añadirse un nombre de usuario CHAP y contraseña, tanto en el servidor como en el iniciador. A título informativo, las acciones a realizar para dotar de usuario y contraseña a la conexión serían las que siguen.

```

[initiator - UO281847 [Corriendo] - Oracle VM VirtualBox]
Archivo Máquina Ver Entrada Dispositivos Ayuda
Actividades Terminal 13 de abr 21:38

[initiator - UO281847 [Corriendo] - Oracle VM VirtualBox]
Archivo Máquina Ver Entrada Dispositivos Ayuda
Actividades Terminal 13 de abr 21:38

[uo281847@localhost uoxxxxxx]# df
S.ficheros      bloques de 1K  Usados Disponibles Uso% Montado en
devtmpfs          4096      0      4096      0% /dev
tmpfs            898632      0    898632      0% /dev/shm
tmpfs            359456    5728   353728      2% /run
/dev/mapper/almalinux-root 17197056 4892628   12304428  29% /
/dev/sda2        1038336 389400   648936  38% /boot
/dev/sda1        613160   7152   606008  2% /boot/efi
/dev/sdb1        20465212    24  19400284  1% /mnt/disco
tmpfs            179724   112   179612  1% /run/user/1000
[uo281847@localhost uoxxxxxx]# cat /proc/scsi/scsi
Attached devices:
Host: scsil Channel: 00 Id: 00 Lun: 00
  Vendor: VBOX   Model: CD-ROM
  Type:  CD-ROM
  Rev: 1.0
  ANSI  SCSI revision: 05
Host: scsi2 Channel: 00 Id: 00 Lun: 00
  Vendor: ATA    Model: VBOX HARDDISK
  Type:  Direct-Access
  Rev: 1.0
  ANSI  SCSI revision: 05
Host: scsi3 Channel: 00 Id: 00 Lun: 00
  Vendor: LIO-ORG Model: mi_disco_sdb
  Type:  Direct-Access
  Rev: 4.0
  ANSI  SCSI revision: 06
Host: scsi3 Channel: 00 Id: 00 Lun: 01
  Vendor: LIO-ORG Model: mi_fichero
  Type:  Direct-Access
  Rev: 4.0
  ANSI  SCSI revision: 06
[uo281847@localhost uoxxxxxx]# 

[initiator - UO281847 [Corriendo] - Oracle VM VirtualBox]
Archivo Máquina Ver Entrada Dispositivos Ayuda
Actividades Terminal 13 de abr 21:38

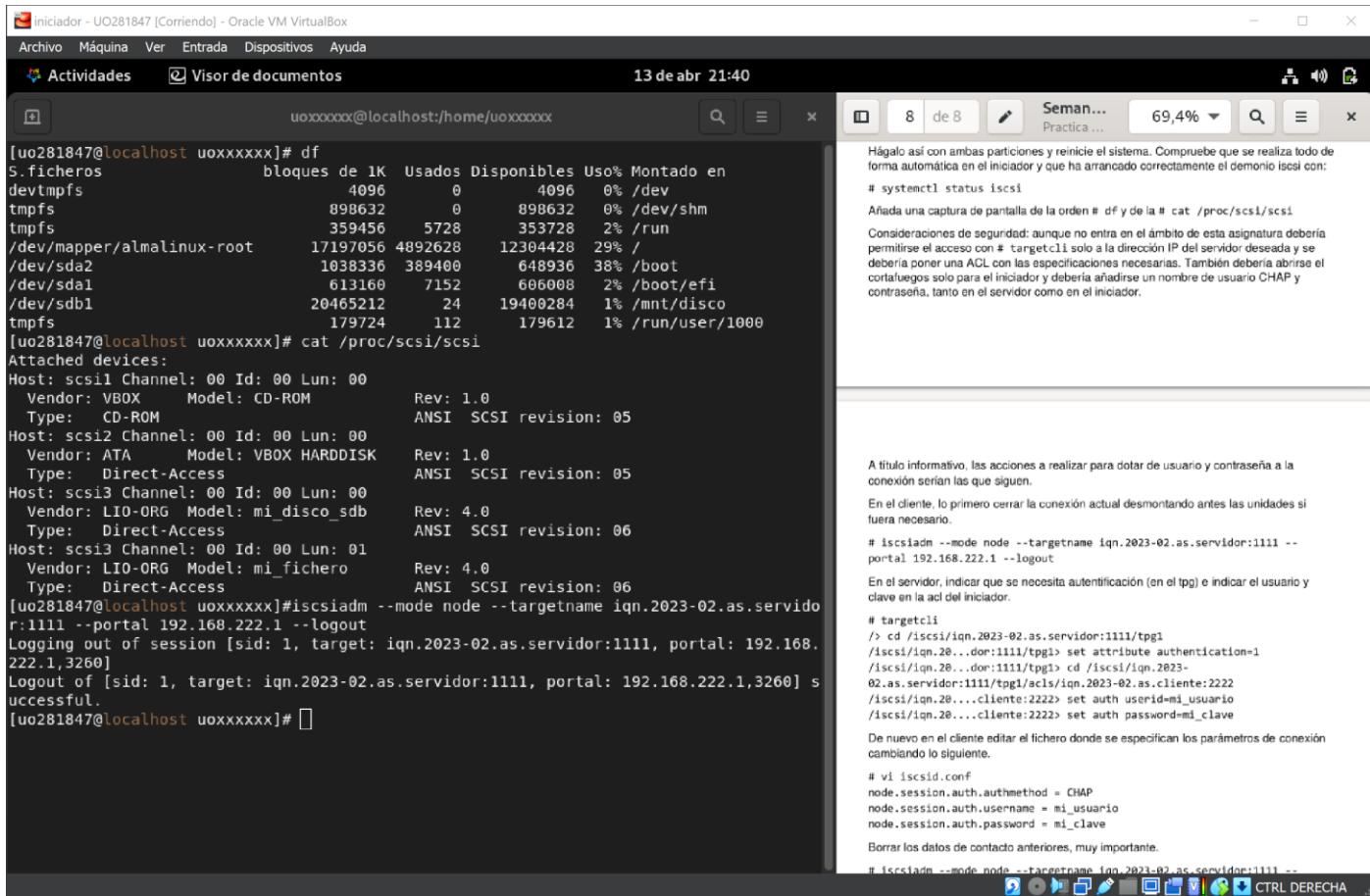
# vi /etc/iscsi/initiatorname.iscsi
InitiatorName=iqn.2023-02.as.cliente:2222

Verificar si ve al servidor.
# iscsiadm --mode=discovery --type=senttargets --portal=192.168.222.1
Si todo es correcto se verá como respuesta la dirección IP del servidor y su IQN.
Se puede hacer ahora un login interactivo (--logout para salir)
# iscsiadm --mode=node --targetname=iqn.2023-02.as.servidor:1111 --portal=192.168.222.1 --login
A partir de este momento con # lsblk deben aparecer en el iniciador los nuevos discos
sdb y sdc si no había previamente otros. También pueden verse con # cat /proc/scsi/scsi
Estos dos discos ya se pueden particionar, formatear y montar. Como no se sabe si van a
ser sdb1 o sdd1 o cualquier otra cosa, es conveniente en el /etc/fstab montarlos por
UUID en vez de por nombre. Es decir en vez de algo como esto:
/dev/sdb1 /mnt/disco ext4 _netdev 0 0
obtener el UUID con # blkid /dev/sdb1 y poner en fstab
UUID="0fc99ba2-912f-4519-ab6d-84c76668c383" /mnt/disco ext4 _netdev 0 0
De esta forma siempre se montará en /mnt/disco con independencia de que sea vía con
cualquier nombre. La opción _netdev garantiza que se espera a que se inicie primero la
red.
En vez de ext4 puede emplearse ext2, ext3, xfs o cualquier otro sistema de ficheros que
se desee.
Hágalo así con ambas particiones y reinicie el sistema. Compruebe que se realiza todo de
forma automática en el iniciador y que ha arrancado correctamente el demonio iscsi con:
# systemctl status iscsi
Añada una captura de pantalla de la orden # df y de la # cat /proc/scsi/scsi
Consideraciones de seguridad: aunque no entra en el ámbito de esta asignatura debería
permilir el acceso con # targetcli solo a la dirección IP del servidor deseada y se
debería poner una ACL con las especificaciones necesarias. También debería abrirse el
cortafuegos solo para el iniciador y debería añadirse un nombre de usuario CHAP y
contraseña, tanto en el servidor como en el iniciador.

[initiator - UO281847 [Corriendo] - Oracle VM VirtualBox]
Archivo Máquina Ver Entrada Dispositivos Ayuda
Actividades Terminal 13 de abr 21:38

```

16. En el cliente, lo primero cerrar la conexión actual desmontando antes las unidades si fuera necesario.



The screenshot shows a terminal window in Oracle VM VirtualBox. The terminal session is for user 'uoxxxxxx' on 'localhost'. The user has run several commands to disconnect an iSCSI session:

```
[uo281847@localhost uoxxxxxx]# df -h
Filesystem      Tamaño Usados  Disponibles  Uso%  Montado en
/devtmpfs        4096     0      4096   0%  /dev
tmpfs           898632     0     898632   0%  /dev/shm
tmpfs           359456   5728    353728   2%  /run
/devmapper/almalinux-root  17197056 4892628  12304428  29%  /
/dev/sda2        1038336 389400   648936  38%  /boot
/dev/sda1        613160   7152   606008  2%  /boot/efi
/dev/sdb1        20465212    24   19400284  1%  /mnt/disco
tmpfs           179724   112    179612  1%  /run/user/1000

[uo281847@localhost uoxxxxxx]# cat /proc/scsi/scsi
Attached devices:
Host: scsil Channel: 00 Id: 00 Lun: 00
  Vendor: VBOX    Model: CD-ROM
  Type:  CD-ROM
Host: scsi2 Channel: 00 Id: 00 Lun: 00
  Vendor: ATA     Model: VBOX HARDDISK
  Type:  Direct-Access
Host: scsi3 Channel: 00 Id: 00 Lun: 00
  Vendor: LIO-ORG Model: mi_disco_sdb
  Type:  Direct-Access
Host: scsi3 Channel: 00 Id: 00 Lun: 01
  Vendor: LIO-ORG Model: mi_fichero
  Type:  Direct-Access
[uo281847@localhost uoxxxxxx]#iscsiadm --mode node --targetname iqn.2023-02.as.servidor:1111 --portal 192.168.222.1 --logout
Logging out of session [sid: 1, target: iqn.2023-02.as.servidor:1111, portal: 192.168.222.1,3260]
Logout of [sid: 1, target: iqn.2023-02.as.servidor:1111, portal: 192.168.222.1,3260] successful.

[uo281847@localhost uoxxxxxx]#
```

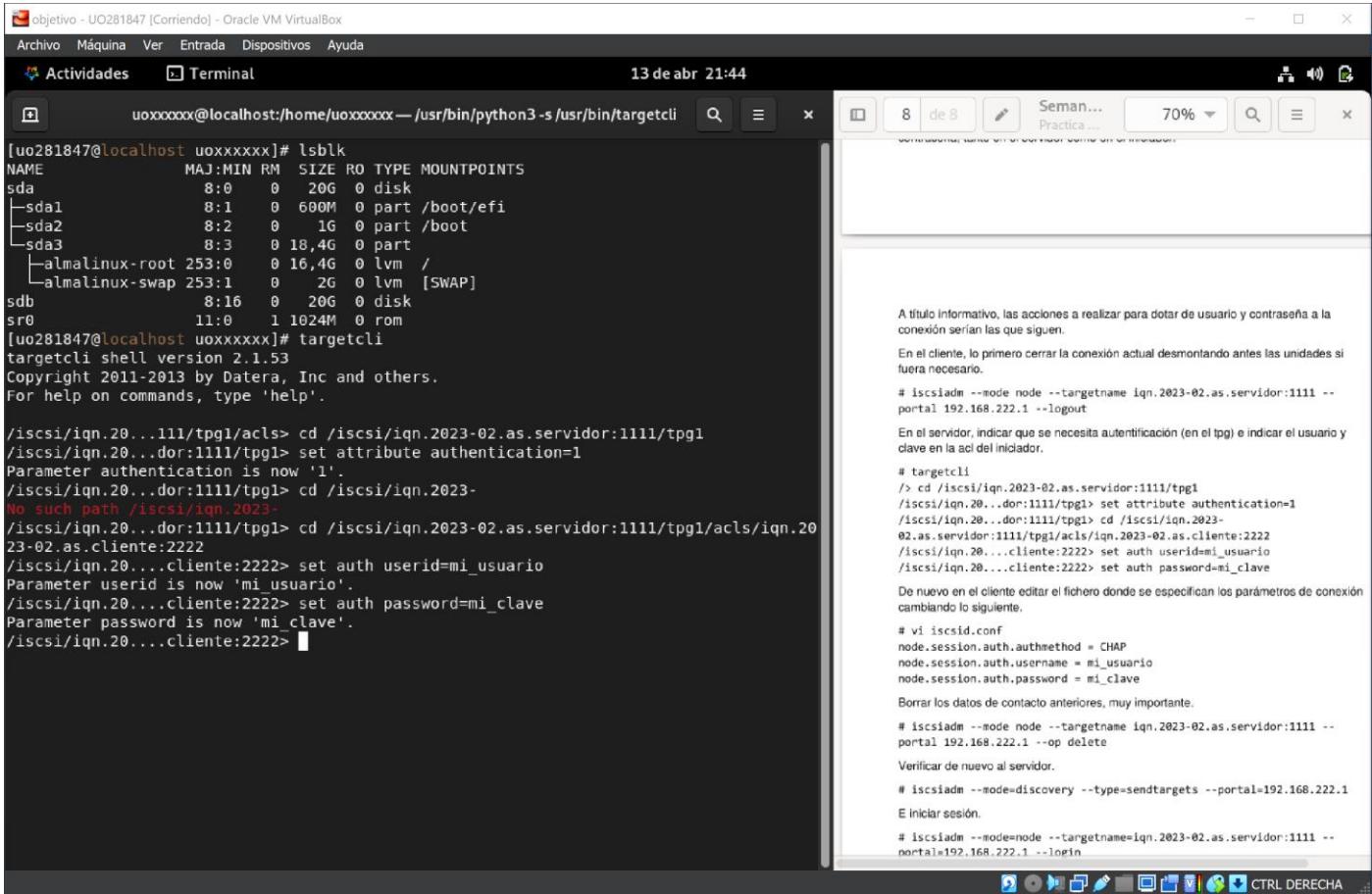
The terminal window also displays a status bar with system information and a note in the top right corner:

Hágalo así con ambas particiones y reinicie el sistema. Compruebe que se realiza todo de forma automática en el iniciador y que ha arrancado correctamente el demonio iscsi con: # systemctl status iscsi

Además una captura de pantalla de la orden # df y de la # cat /proc/scsi/scsi

Consideraciones de seguridad: aunque no entra en el ámbito de esta asignatura debería permitirse el acceso con # targetcli solo a la dirección IP del servidor deseada y se debería poner una ACL con las especificaciones necesarias. También debería abrirse el cortafuegos solo para el iniciador y debería añadirse un nombre de usuario CHAP y contraseña, tanto en el servidor como en el iniciador.

17. En el servidor, indicar que se necesita autentificación (en el tpg) e indicar el usuario y clave en la acl del iniciador.



```

objetivo - UO281847 [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Actividades Terminal 13 de abr 21:44
[uo281847@localhost uoxxxxxx]# lsblk
NAME      MAJ:MIN RM  SIZE RO TYPE MOUNTPOINTS
sda        8:0    0  20G  0 disk
└─sda1     8:1    0 600M  0 part /boot/efi
sda2      8:2    0   1G  0 part /boot
sda3      8:3    0 18,4G  0 part
├─almalinux-root 253:0  0 16,4G  0 lvm /
└─almalinux-swap 253:1  0   2G  0 lvm [SWAP]
sdb        8:16   0  20G  0 disk
└─sdb1     8:17   1 1024M 0 rom
[uo281847@localhost uoxxxxxx]# targetcli
targetcli shell version 2.1.53
Copyright 2011-2013 by Datera, Inc and others.
For help on commands, type 'help'.
/iscsi/iqn.20...111/tpg1/acls> cd /iscsi/iqn.2023-02.as.servidor:1111/tpg1
/iscsi/iqn.20...dor:1111/tpg1> set attribute authentication=1
Parameter authentication is now '1'.
/iscsi/iqn.20...dor:1111/tpg1> cd /iscsi/iqn.2023-02.as.servidor:1111/tpg1/acls/iqn.2023-02.as.cliente:2222
/iscsi/iqn.20...cliente:2222> set auth userid=mi_usuario
Parameter userid is now 'mi_usuario'.
/iscsi/iqn.20...cliente:2222> set auth password=mi_clave
Parameter password is now 'mi_clave'.
/iscsi/iqn.20...cliente:2222> █

```

A título informativo, las acciones a realizar para dotar de usuario y contraseña a la conexión serían las que siguen.

En el cliente, lo primero cerrar la conexión actual desmontando antes las unidades si fuera necesario.

```

# iscsadm --mode node --targetname iqn.2023-02.as.servidor:1111 --portal 192.168.222.1 --logout

```

En el servidor, indicar que se necesita autentificación (en el tpg) e indicar el usuario y clave en la acl del iniciador.

```

# targetcli
/> cd /iscsi/iqn.2023-02.as.servidor:1111/tpg1
/iscsi/iqn.20...dor:1111/tpg1> set attribute authentication=1
/> cd /iscsi/iqn.20...dor:1111/tpg1> cd /iscsi/iqn.2023-02.as.servidor:1111/tpg1/acls/iqn.2023-02.as.cliente:2222
/iscsi/iqn.20...cliente:2222> set auth userid=mi_usuario
/iscsi/iqn.20...cliente:2222> set auth password=mi_clave

```

Do nuevo en el cliente editar el fichero donde se especifican los parámetros de conexión cambiando lo siguiente.

```

# vi iscsid.conf
node.session.auth.authmethod = CHAP
node.session.auth.username = mi_usuario
node.session.auth.password = mi_clave

```

Borrar los datos de contacto anteriores, muy importante.

```

# iscsadm --mode node --targetname iqn.2023-02.as.servidor:1111 --portal 192.168.222.1 --op delete

```

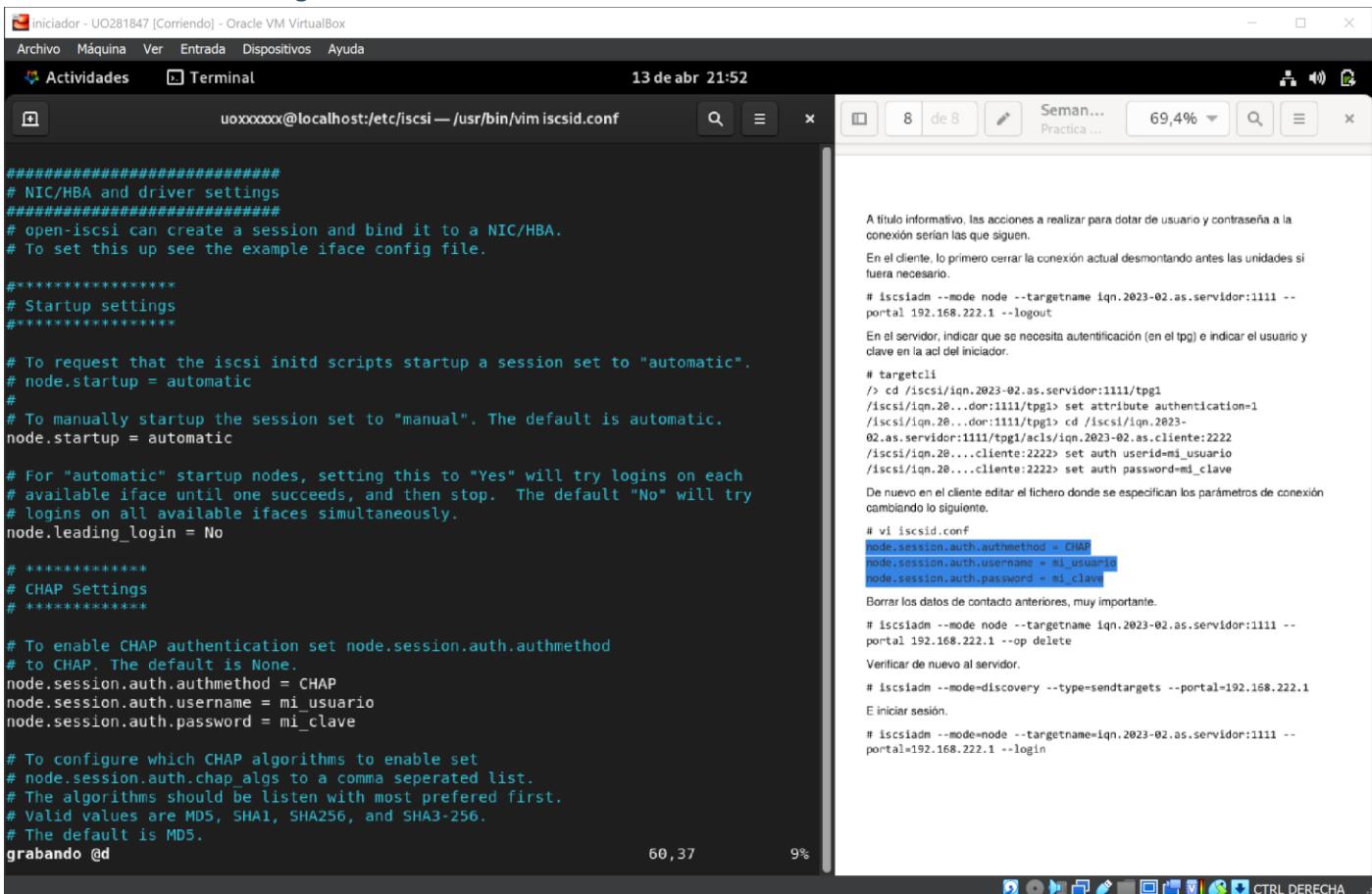
Verificar de nuevo al servidor.

```

# iscsadm --mode=discovery --type=sendtargets --portal=192.168.222.1
E iniciar sesión.
# iscsadm --mode=node --targetname=iqn.2023-02.as.servidor:1111 --portal=192.168.222.1 --login

```

18. De nuevo en el cliente editar el fichero donde se especifican los parámetros de conexión cambiando lo siguiente.



```

iniciador - UO281847 [Corriendo] - Oracle VM VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Actividades Terminal 13 de abr 21:52
[uoxxxxx@localhost /etc/iscsi]# /usr/bin/vim iscsid.conf
#####
# NIC/HBA and driver settings
#####
# open-iscsi can create a session and bind it to a NIC/HBA.
# To set this up see the example iface config file.

#####
# Startup settings
#####

# To request that the iscsi initd scripts startup a session set to "automatic".
# node.startup = automatic
#
# To manually startup the session set to "manual". The default is automatic.
node.startup = automatic

# For "automatic" startup nodes, setting this to "Yes" will try logins on each
# available iface until one succeeds, and then stop. The default "No" will try
# logins on all available ifaces simultaneously.
node.leading_login = No

#####
# CHAP Settings
#####

# To enable CHAP authentication set node.session.auth.authmethod
# to CHAP. The default is None.
node.session.auth.authmethod = CHAP
node.session.auth.username = mi_usuario
node.session.auth.password = mi_clave

# To configure which CHAP algorithms to enable set
# node.session.auth.chap_algs to a comma separated list.
# The algorithms should be listed with most preferred first.
# Valid values are MD5, SHA1, SHA256, and SHA3-256.
# The default is MD5.
grabando @d

```

A título informativo, las acciones a realizar para dotar de usuario y contraseña a la conexión serían las que siguen.

En el cliente, lo primero cerrar la conexión actual desmontando antes las unidades si fuera necesario.

```

# iscsadm --mode node --targetname iqn.2023-02.as.servidor:1111 --portal 192.168.222.1 --logout

```

En el servidor, indicar que se necesita autentificación (en el tpg) e indicar el usuario y clave en la acl del iniciador.

```

# targetcli
/> cd /iscsi/iqn.2023-02.as.servidor:1111/tpg1
/iscsi/iqn.20...dor:1111/tpg1> set attribute authentication=1
/> cd /iscsi/iqn.20...dor:1111/tpg1> cd /iscsi/iqn.2023-02.as.servidor:1111/tpg1/acls/iqn.2023-02.as.cliente:2222
/iscsi/iqn.20...cliente:2222> set auth userid=mi_usuario
/iscsi/iqn.20...cliente:2222> set auth password=mi_clave

```

Do nuevo en el cliente editar el fichero donde se especifican los parámetros de conexión cambiando lo siguiente.

```

# vi iscsid.conf
node.session.auth.authmethod = CHAP
node.session.auth.username = mi_usuario
node.session.auth.password = mi_clave

```

Borrar los datos de contacto anteriores, muy importante.

```

# iscsadm --mode node --targetname iqn.2023-02.as.servidor:1111 --portal 192.168.222.1 --op delete

```

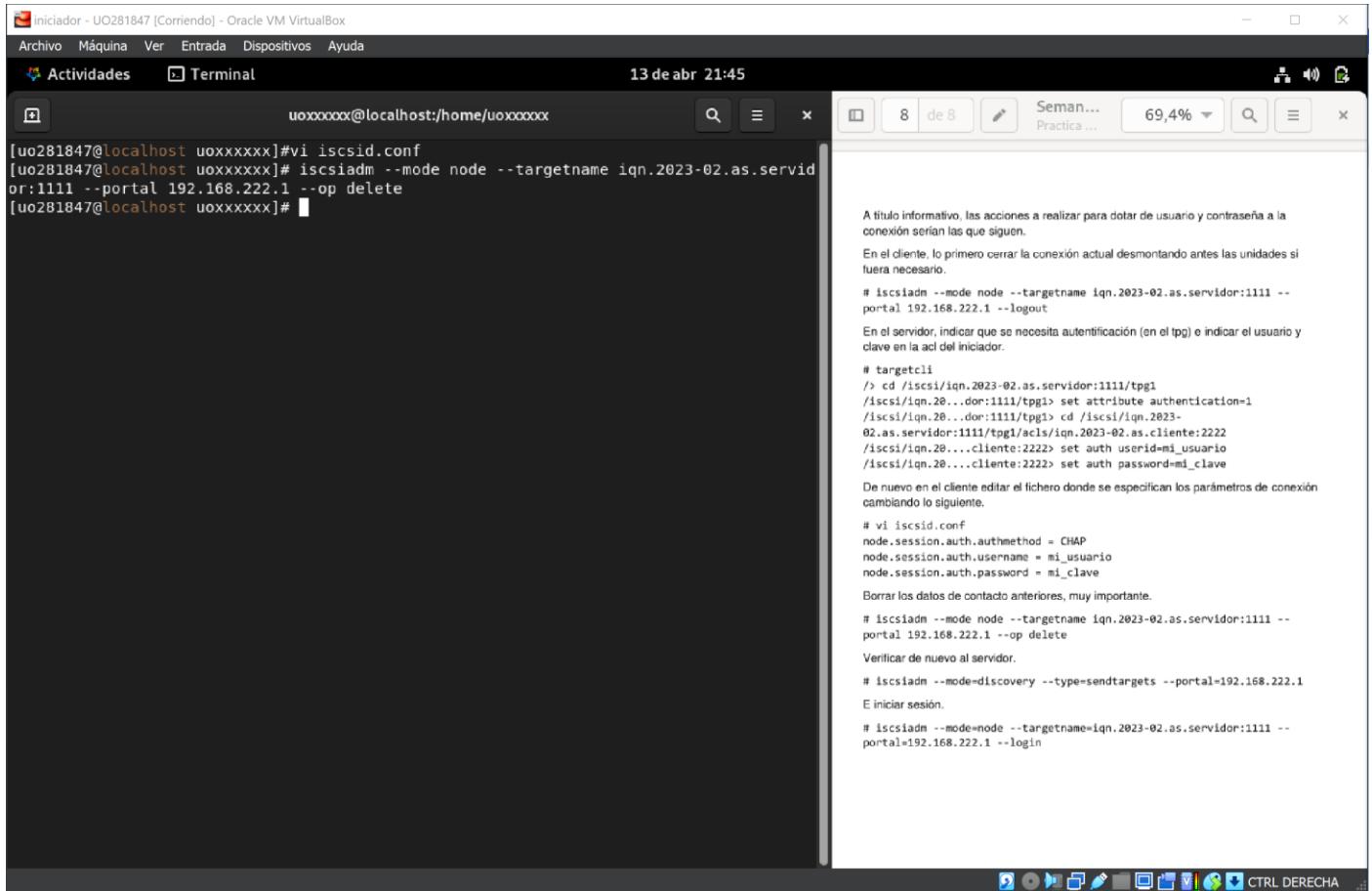
Verificar de nuevo al servidor.

```

# iscsadm --mode=discovery --type=sendtargets --portal=192.168.222.1
E iniciar sesión.
# iscsadm --mode=node --targetname=iqn.2023-02.as.servidor:1111 --portal=192.168.222.1 --login

```

19. Borrar los datos de contacto anteriores, muy importante.



iniciador - UO281847 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Actividades Terminal 13 de abr 21:45

u0xxxxxx@localhost:~

```
[u0281847@localhost u0xxxxxx]# vi iscsid.conf
[u0281847@localhost u0xxxxxx]# iscsiadm --mode node --targetname iqn.2023-02.as.servidor:1111 --portal 192.168.222.1 --op delete
[u0281847@localhost u0xxxxxx]#
```

A título informativo, las acciones a realizar para dotar de usuario y contraseña a la conexión serían las que siguen.

En el cliente, lo primero cerrar la conexión actual desmontando antes las unidades si fuera necesario.

```
# iscsiadm --mode node --targetname iqn.2023-02.as.servidor:1111 --portal 192.168.222.1 --logout
```

En el servidor, indicar que se necesita autenticación (en el tpg) e indicar el usuario y clave en la acl del iniciador.

```
# targetcli
/> cd /iscsi/iqn.2023-02.as.servidor:1111/tpg1
/iscsi/iqn.2023-02.as.servidor:1111/tpg1> set attribute authentication=1
/iscsi/iqn.2023-02.as.servidor:1111/tpg1> cd /iscsi/iqn.2023-02.as.servidor:1111/tpg1/acls/iqn.2023-02.as.cliente:2222
/iscsi/iqn.2023-02.as.servidor:1111/tpg1/acls/iqn.2023-02.as.cliente:2222> set auth userid=mi_usuario
/iscsi/iqn.2023-02.as.servidor:1111/tpg1/acls/iqn.2023-02.as.cliente:2222> set auth password=mi_clave
```

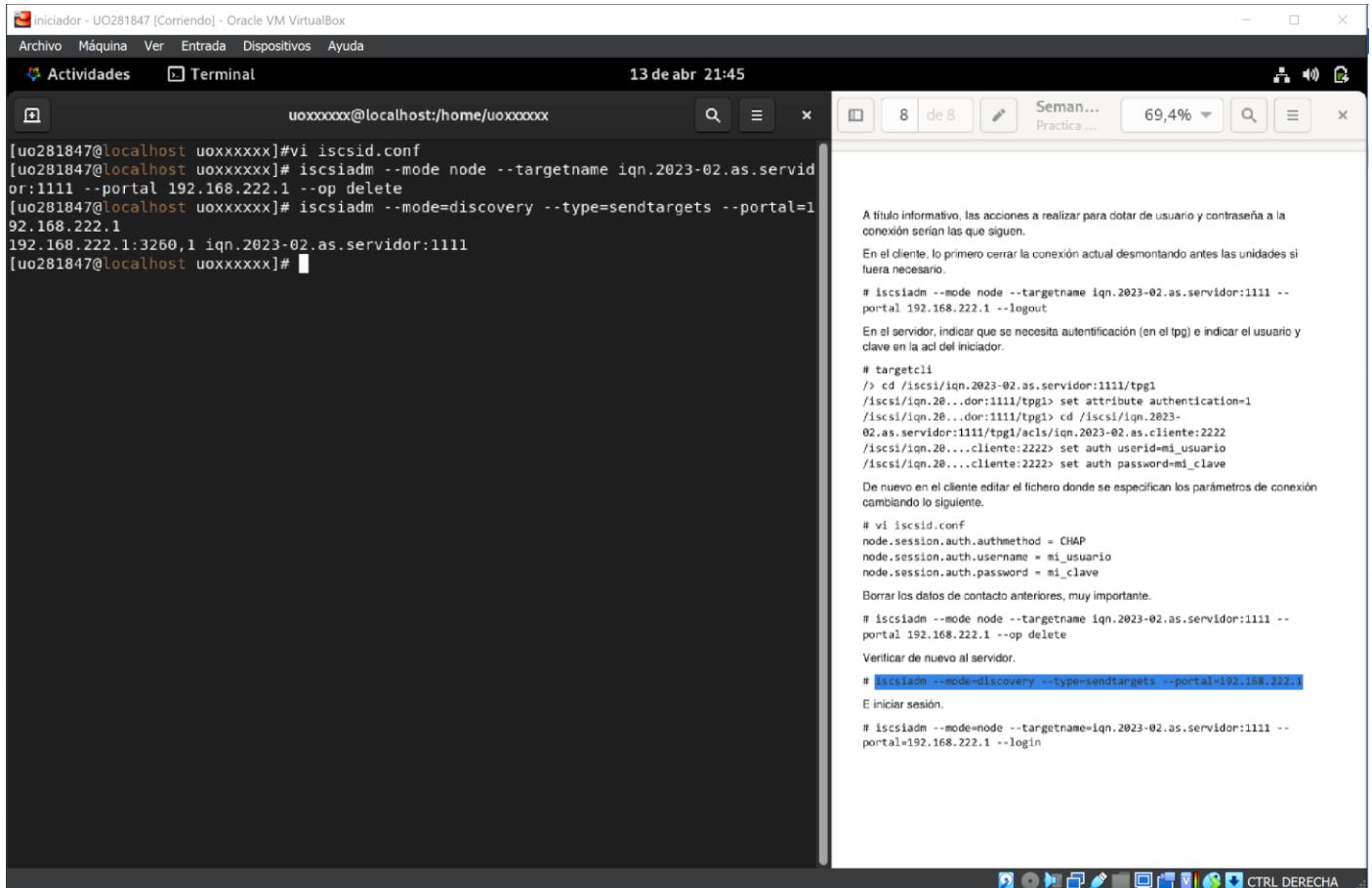
De nuevo en el cliente editar el fichero donde se especifican los parámetros de conexión cambiando lo siguiente.

```
# vi iscsid.conf
node.session.auth.authmethod = CHAP
node.session.auth.username = mi_usuario
node.session.auth.password = mi_clave
```

Borrar los datos de contacto anteriores, muy importante.

```
# iscsiadm --mode node --targetname iqn.2023-02.as.servidor:1111 --portal 192.168.222.1 --op delete
Verificar de nuevo al servidor.
# iscsiadm --mode=discovery --type-sendtargets --portal=192.168.222.1
E iniciar sesión.
# iscsiadm --mode=node --targetname=iqn.2023-02.as.servidor:1111 --portal=192.168.222.1 --login
```

20. Verificar de nuevo al servidor.



iniciador - UO281847 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Actividades Terminal 13 de abr 21:45

```
uoxxxxxx@localhost:~$ vi iscsid.conf
[...]
[uo281847@localhost uoxxxxxx]# iscsadm --mode node --targetname iqn.2023-02.as.servidor:1111 --portal 192.168.222.1 --op delete
[uo281847@localhost uoxxxxxx]# iscsadm --mode=discovery --type=sendtargets --portal=192.168.222.1
192.168.222.1:3260,1 iqn.2023-02.as.servidor:1111
[uo281847@localhost uoxxxxxx]#
```

A título informativo, las acciones a realizar para dotar de usuario y contraseña a la conexión serían las que siguen.

En el cliente, lo primero cerrar la conexión actual desmontando antes las unidades si fuera necesario.

```
# iscsadm --mode node --targetname iqn.2023-02.as.servidor:1111 --portal 192.168.222.1 --logout
```

En el servidor, indicar que se necesita autenticación (en el tpg) e indicar el usuario y clave en la act del iniciador.

```
# targetcli
/> cd /iscsi/iqn.2023-02.as.servidor:1111/tpg1
/iscsi/iqn.20...:dor:1111/tpg1> set attribute authentication=1
/iscsi/iqn.20...:dor:1111/tpg1> cd /iscsi/iqn.2023-02.as.servidor:1111/tpg1/acls/iqn.2023-02.as.cliente:2222
/iscsi/iqn.20...:cliente:2222> set auth userid=mi_usuario
/iscsi/iqn.20...:cliente:2222> set auth password=mi_clave
```

De nuevo en el cliente editar el fichero donde se especifican los parámetros de conexión cambiando lo siguiente.

```
# vi iscsid.conf
node.session.auth.authmethod = CHAP
node.session.auth.username = mi_usuario
node.session.auth.password = mi_clave
```

Borrar los datos de contacto anteriores, muy importante.

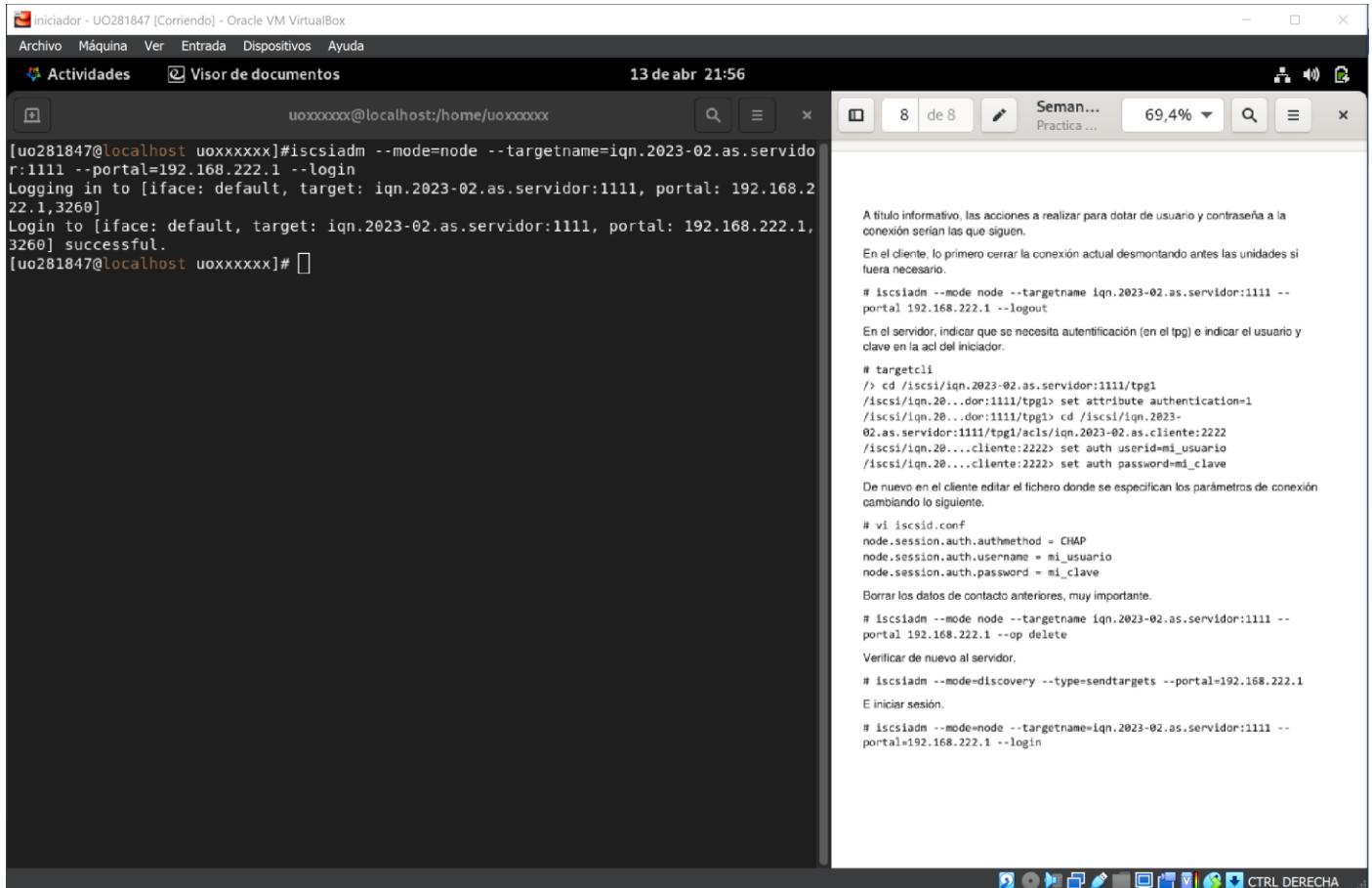
```
# iscsadm --mode node --targetname iqn.2023-02.as.servidor:1111 --portal 192.168.222.1 --op delete
```

Verificar de nuevo al servidor.

```
# iscsadm --mode=discovery --type=sendtargets --portal=192.168.222.1
E iniciar sesión.
```

```
# iscsadm --mode=node --targetname=iqn.2023-02.as.servidor:1111 --portal=192.168.222.1 --login
```

21. E iniciar sesión.



iniciador - UO281847 [Corriendo] - Oracle VM VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

Actividades Visor de documentos 13 de abr 21:56

```
uoxxxxxx@localhost:~$ iscsadm --mode=node --targetname=iqn.2023-02.as.servidor:1111 --portal=192.168.222.1 --login
Logging in to [iface: default, target: iqn.2023-02.as.servidor:1111, portal: 192.168.222.1,3260]
Login to [iface: default, target: iqn.2023-02.as.servidor:1111, portal: 192.168.222.1,3260] successful.
[uo281847@localhost uoxxxxxx]#
```

A título informativo, las acciones a realizar para dotar de usuario y contraseña a la conexión serían las que siguen.

En el cliente, lo primero cerrar la conexión actual desmontando antes las unidades si fuera necesario.

```
# iscsadm --mode node --targetname iqn.2023-02.as.servidor:1111 --portal 192.168.222.1 --logout
```

En el servidor, indicar que se necesita autenticación (en el tpg) e indicar el usuario y clave en la act del iniciador.

```
# targetcli
/> cd /iscsi/iqn.2023-02.as.servidor:1111/tpg1
/iscsi/iqn.20...:dor:1111/tpg1> set attribute authentication=1
/iscsi/iqn.20...:dor:1111/tpg1> cd /iscsi/iqn.2023-02.as.servidor:1111/tpg1/acls/iqn.2023-02.as.cliente:2222
/iscsi/iqn.20...:cliente:2222> set auth userid=mi_usuario
/iscsi/iqn.20...:cliente:2222> set auth password=mi_clave
```

De nuevo en el cliente editar el fichero donde se especifican los parámetros de conexión cambiando lo siguiente.

```
# vi iscsid.conf
node.session.auth.authmethod = CHAP
node.session.auth.username = mi_usuario
node.session.auth.password = mi_clave
```

Borrar los datos de contacto anteriores, muy importante.

```
# iscsadm --mode node --targetname iqn.2023-02.as.servidor:1111 --portal 192.168.222.1 --op delete
```

Verificar de nuevo al servidor.

```
# iscsadm --mode=discovery --type=sendtargets --portal=192.168.222.1
E iniciar sesión.
```

```
# iscsadm --mode=node --targetname=iqn.2023-02.as.servidor:1111 --portal=192.168.222.1 --login
```