

# Práctica 2 de Administración de Sistemas

Paloma Pérez de Madrid Laguna

1. Comenzamos con la máquina VM1. Realizar peticiones DNS utilizando las utilidades dig y/o nslookup, tanto en resolución directa como inversa, sobre servidores de DNS locales y remotos (servidores de Internet). Llevar a cabo manualmente el proceso iterativo de búsqueda de un recurso de Internet desde los servidores raíz hasta el servidor con autoridad en el dominio a consultar (también puede usar la opción +trace de dig).

## Servidor Local

Resolución directa: para obtener una dirección IP a partir de un nombre

- dig @servidor (-t tipo) \_\_dominio\_\_

# Dig @localhost [www.constanzalaguna.com](http://www.constanzalaguna.com)

```
; <>> DIG 9.18.18-0ubuntu0.22.04.2-Ubuntu <>> @localhost www.constanzalaguna.com
; (1 server found)
;: global options: +cmd
;: Got answer:
;: -->HEADER<<- opcode: QUERY, status: NOERROR, id: 34980
;: flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;: OPT PSEUDOSECTION:
;: EDNS: version: 0, flags:; udo: 1232
;: COOKIE: fa306d2b4456a3fd0100000065eadccb0770e18d21d890f0 (good)
;: QUESTION SECTION:
;: www.constanzalaguna.com.      IN      A
;: ANSWER SECTION:
www.constanzalaguna.com. 300 IN      A      104.21.25.127
www.constanzalaguna.com. 300 IN      A      172.67.134.61

;: Query time: 388 msec
;: SERVER: 127.0.0.1#53(localhost) (UDP)
;: WHEN: Fri Mar 08 09:39:23 UTC 2024
;: MSG SIZE rcvd: 112

root@server:/#
```

```
www.constanzalaguna.com. 300 IN      A      172.67.134.61
www.constanzalaguna.com. 300 IN      A      104.21.25.127
;; Received 84 bytes from 108.162.192.244#53(rihana.ns.cloudflare.com) in 7 ms

root@server:/var/named#
```

Resolución inversa: para obtener el dominio a través de una dirección IP

dig @servidor -x \_\_dirección\_IP\_\_ # Dig @localhost -t 172.67.134.61

```
i.root-servers.net. 450537 IN      A      192.36.148.17
j.root-servers.net. 450537 IN      A      192.58.128.30
k.root-servers.net. 450537 IN      A      193.0.14.129
l.root-servers.net. 450537 IN      A      199.7.83.42
m.root-servers.net. 450537 IN      A      202.12.27.33
a.root-servers.net. 450537 IN      AAAA   2001:508:b3e::2:30
b.root-servers.net. 450537 IN      AAAA   2801:1b8:10::b
c.root-servers.net. 450537 IN      AAAA   2001:500:2::c
d.root-servers.net. 450537 IN      AAAA   2001:500:2d::d
e.root-servers.net. 450537 IN      AAAA   2001:500:a8::e
f.root-servers.net. 450537 IN      AAAA   2001:500:2f::f
g.root-servers.net. 450537 IN      AAAA   2001:500:12::d0d
h.root-servers.net. 450537 IN      AAAA   2001:500:1::53
i.root-servers.net. 450537 IN      AAAA   2001:7fe::53
j.root-servers.net. 450537 IN      AAAA   2001:503:c27::2:30
k.root-servers.net. 450537 IN      AAAA   2001:7fd::1
l.root-servers.net. 450537 IN      AAAA   2001:500:9f::42
m.root-servers.net. 450537 IN      AAAA   2001:dc3::35

;: Query time: 0 msec
;: SERVER: 127.0.0.1#53(localhost) (UDP)
;: WHEN: Fri Mar 08 09:41:39 UTC 2024
;: MSG SIZE rcvd: 851

root@server:/#
```

## Servidores Remoto

Servidor remoto de mi máquina Windows:

```
Servidores DNS. . . . . : 10.80.200.12
                        10.80.200.13
```

# Dig @10.80.200.13 [www.constanzalaguna.com](http://www.constanzalaguna.com)

```
root@server:/# dig @10.80.200.13 www.constanzalaguna.com

<> DiG 9.18.18-0ubuntu0.22.04.2-Ubuntu <> @10.80.200.13 www.constanzalaguna.com
(1 server found)
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 44478
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
;; EDNS: version 0, flags:; udp: 4000
;; QUESTION SECTION:
;www.constanzalaguna.com.      IN      A

;; ANSWER SECTION:
www.constanzalaguna.com. 300     IN      A      104.21.25.127
www.constanzalaguna.com. 300     IN      A      172.67.134.61

;; Query time: 128 msec
;; SERVER: 10.80.200.13#53(10.80.200.13) (UDP)
;; WHEN: Fri Mar 08 09:46:12 UTC 2024
;; MSG SIZE rcvd: 84

root@server:/# _
```

```
# Dig @10.80.200.13 -x 172.67.134.61
```

```

a.root-servers.net.      1136   IN      A        198.41.0.4
a.root-servers.net.      1136   IN      AAAA     2001:503:ba3e::2:30
d.root-servers.net.      1136   IN      A        193.7.91.13
d.root-servers.net.      1136   IN      AAAA     2001:500:2d::d
c.root-servers.net.      1136   IN      A        192.33.4.12
c.root-servers.net.      1136   IN      AAAA     2001:500:2::c
b.root-servers.net.      1136   IN      A        170.247.170.2
b.root-servers.net.      1136   IN      AAAA     2801:1b8:10::b
j.root-servers.net.      1136   IN      A        192.58.128.30
j.root-servers.net.      1136   IN      AAAA     2001:503:c27::2:30
k.root-servers.net.      1136   IN      A        193.0.14.129
k.root-servers.net.      1136   IN      AAAA     2001:7fd::1
g.root-servers.net.      1136   IN      A        192.112.36.4
g.root-servers.net.      1136   IN      AAAA     2001:500:12::d0d
m.root-servers.net.      1136   IN      A        202.12.27.33
m.root-servers.net.      1136   IN      AAAA     2001:dc3::35
f.root-servers.net.      1136   IN      A        192.5.5.241
f.root-servers.net.      1136   IN      AAAA     2001:500:2::f

;; Query time: 116 msec
;; SERVER: 10.80.200.13#53(10.80.200.13) (UDP)
;; WHEN: Fri Mar 08 09:47:17 UTC 2024
;; MSG SIZE rcvd: 824

root@server:/# _

```

## Proceso Iterativo de Búsqueda con trace

```
# Dig @localhost www.constanzalaguna.com -trace
```

```

1 (<> Dig 9.18.18-Ubuntu22.04.2-Ubuntu <> @localhost www.constanzaiguazu.c
2 ns
3 (1 server found)
4 | Global options: +cmd
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 .
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 .
740 .
741 .
742 .
743 .
744 .
745 .
746 .
747 .
748 .
749 .
750 .
751 .
752 .
753 .
754 .
755 .
756 .
757 .
758 .
759 .
760 .
761 .
762 .
763 .
764 .
765 .
766 .
767 .
768 .
769 .
770 .
771 .
772 .
773 .
774 .
775 .
776 .
777 .
778 .
779 .
780 .
781 .
782 .
783 .
784 .
785 .
786 .
787 .
788 .
789 .
790 .
791 .
792 .
793 .
794 .
795 .
796 .
797 .
798 .
799 .
800 .
801 .
802 .
803 .
804 .
805 .
806 .
807 .
808 .
809 .
810 .
811 .
812 .
813 .
814 .
815 .
816 .
817 .
818 .
819 .
820 .
821 .
822 .
823 .
824 .
825 .
826 .
827 .
828 .
829 .
830 .
831
```

```

constanzalaguna.com. 172800 IN NS rihana.ns.cloudflare.com.
constanzalaguna.com. 172800 IN NS anirban.ns.cloudflare.com.
CKOP0JMG874LJREF7EFN8430QVIT8BSM.com. 86400 IN NSEC3 1 1 0 - CK0Q2D6NI4I7EQH8NA3
ONS6104GUL8G5 NS SOA RRSIG DNSKEY NSEC3PARAM
CKOP0JMG874LJREF7EFN8430QVIT8BSM.com. 86400 IN RRSIG NSEC3 13 2 86400 2024031305
2626 20240306041626 4534 com. vqYwZamvongqQ4TiNeNHJPd0qu8PyUA7F7EmE4aDXKskxZiirTW
RDK6Hr 0kJQ02XgsyGmYN9o4B9ZMgn2MrzKwA==
K90738C6JH7KR8C6L7M5VBQNNUAOR50C.com. 86400 IN NSEC3 1 1 0 - K907P20DTIA6KA2MT74
GT8B8HQRV5L1V NS DS RRSIG
K90738C6JH7KR8C6L7M5VBQNNUAOR50C.com. 86400 IN RRSIG NSEC3 13 2 86400 2024031205
5937 20240305044937 4534 com. Aws1GTTIB8pXUwb1zScKJS0gVgY/MudOk+PwVH0oz0QU1F87R1
KgoAN/ dQMcoSb4Mn1CwUusyP+GaZ1SwUwkcTQ==
;; Received 730 bytes from 192.26.92.30#53(c.gtld-servers.net) in 92 ms

;; UDP setup with 2a06:98c1:50::ac40:2140#53(2a06:98c1:50::ac40:2140) for www.co
nstanzalaguna.com failed: network unreachable.
www.constanzalaguna.com. 300 IN A 104.21.25.127
www.constanzalaguna.com. 300 IN A 172.67.134.61
;; Received 84 bytes from 108.162.192.244#53(rihana.ns.cloudflare.com) in 88 ms

```

## 2. Instalar el servidor de DNS Bind 9.

Apt-get install bind9

```

root@server:~# apt-get install bind9

```

( Si no funciona hacer primero apt update y luego apt-get install bind9)

Para buscar archivos que terminen en .service → find . -type f -name '\*.service'

## 3. Configuración del servidor Bind:

- Estudiar el contenido y la ubicación de named.conf  
/etc/bind/named.conf

```

// This is the primary configuration file for the BIND DNS server named.
//
// Please read /usr/share/doc/bind9/README.Debian.gz for information on the
// structure of BIND configuration files in Debian, *BEFORE* you customize
// this configuration file.
//
// If you are just adding zones, please do that in /etc/bind/named.conf.local
include "/etc/bind/named.conf.options";
include "/etc/bind/named.conf.local";
include "/etc/bind/named.conf.default-zones";
~

```

La configuración está distribuida en tres secciones:

- Local
- Options
- Default-zones

Cuando añadamos nuestras zonas en el futuro es importante escribirlas a continuación del include

- Arrancar servicio named

[netstat -utlp] → Systemctl start named → [netstat -utlp]

```
root@server:~# netstat -utlp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
PID/Program name
tcp        0      0 0.0.0.0:ssh             0.0.0.0:*               LISTEN
784/sshd: /usr/sbin
tcp        0      0 localhost:domain       0.0.0.0:*               LISTEN
639/systemd-resolve
tcp6       0      0 [::]:ssh               [::]:*                  LISTEN
784/sshd: /usr/sbin
udp        0      0 localhost:domain       0.0.0.0:*               LISTEN
639/systemd-resolve
udp        0      0 server:bootpc          0.0.0.0:*
541/systemd-network
root@server:~#
```

```
root@server:~# systemctl start named
root@server:~# netstat -utlp
tcp6       0      0 ip6-localhost:953      [::]:*                  LISTEN
2341/named
tcp6       0      0 ip6-localhost:953      [::]:*                  LISTEN
2341/named
udp        0      0 server:domain          0.0.0.0:*
2341/named
udp        0      0 server:domain          0.0.0.0:*
2341/named
udp        0      0 localhost:domain       0.0.0.0:*
2341/named
udp        0      0 localhost:domain       0.0.0.0:*
2341/named
udp        0      0 localhost:domain       0.0.0.0:*
639/systemd-resolve
udp        0      0 server:bootpc          0.0.0.0:*
541/systemd-network
udp6       0      0 ip6-localhost:domain   [::]:*
2341/named
udp6       0      0 ip6-localhost:domain   [::]:*
2341/named
udp6       0      0 server:domain          [::]:*
2341/named
udp6       0      0 server:domain          [::]:*
2341/named
root@server:~#
```

- El servidor deberá estar escuchando el puerto 53/UDP de todas las direcciones y atender peticiones DNS desde cualquier dirección de origen

[named.conf.options]

- Permitir que escuche desde el puerto 53 a todas las direcciones: *listen-on port 53 { any; };*
  - Atender peticiones desde cualquier puerto: *allow-query { any; };*
- Trabaja en modo recursivo
  - *recursion yes;*

```
// If your ISP provided one or more IP addresses for stable
// nameservers, you probably want to use them as forwarders.
// Uncomment the following block, and insert the addresses replacing
// the all-0's placeholder.

// forwarders {
//     0.0.0.0;
// };

// =====

// If BIND logs error messages about the root key being expired,
// you will need to update your keys. See https://www.isc.org/bind-keys
// =====

dnssec-validation auto;

listen-on-v6 { any; };
listen-on port 53 { any; };
allow-query { any; };
recursion yes;

};
-- INSERTAR --
```

- a) Comprobar que el servidor mantiene una caché de últimos accesos realizados (para eliminar el contenido de la caché se puede utilizar el comando `rndc flush`)

`Rndc dumpdb -cache` (vocaldo por defecto al archivo  
`/var/named/data/cache_dump.db`)

```
root@server:/etc/bind# rndc dumpdb -cache
root@server:/etc/bind#
```

1. `dig @127.0.0.1 www.hola.com` (1º consulta)

```
<<>> DiG 9.18.18-0ubuntu0.22.04.2-Ubuntu <<>> +stats @127.0.0.1 www.hola.com
(1 server found)
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 47490
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:;, udp: 1232
;; COOKIE: d8b85288d547118b0100000065e8ae4fd6a6efb995d4d6f2 (good)
;; QUESTION SECTION:
;; www.hola.com.                IN      A
;; ANSWER SECTION:
www.hola.com.                300     IN      CNAME   www.hola.com.edgekey.net.
www.hola.com.edgekey.net.    21600   IN      CNAME   e13750.a.akamaiedge.net.
e13750.a.akamaiedge.net.    20      IN      A       92.122.236.114
;; Query time: 1440 msec
;; SERVER: 127.0.0.1#53(127.0.0.1) (UDP)
;; WHEN: Wed Mar 06 17:56:31 UTC 2024
;; MSG SIZE rcvd: 160
```

2. `dig @127.0.0.1 www.hola.com` (2º consulta)

```
<<>> DiG 9.18.18-0ubuntu0.22.04.2-Ubuntu <<>> +stats @127.0.0.1 www.hola.com
(1 server found)
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 52168
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:;, udp: 1232
;; COOKIE: 47f0735857fb15d70100000065e8ae660e2b206029307d1c (good)
;; QUESTION SECTION:
;; www.hola.com.                IN      A
;; ANSWER SECTION:
www.hola.com.                277     IN      CNAME   www.hola.com.edgekey.net.
www.hola.com.edgekey.net.    21577   IN      CNAME   e13750.a.akamaiedge.net.
e13750.a.akamaiedge.net.    20      IN      A       92.122.236.114
;; Query time: 12 msec
;; SERVER: 127.0.0.1#53(127.0.0.1) (UDP)
;; WHEN: Wed Mar 06 17:56:54 UTC 2024
;; MSG SIZE rcvd: 160
root@server:/etc/bind#
```

Si la vuelvo a ejecutar veo que tarda mucho menos porque la busca en la caché

3. Elimino el contenido de la caché: `rndc flush`  
4. Vuelvo a ejecutar `dig @127.0.0.1 www.hola.com`

```
<<>> DiG 9.18.18-0ubuntu0.22.04.2-Ubuntu <<>> +stats @127.0.0.1 www.hola.com
(1 server found)
;; global options: +cmd
;; Got answer:
;; ->HEADER<<- opcode: QUERY, status: NOERROR, id: 8377
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1
;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:;, udp: 1232
;; COOKIE: 275a5e4be1e47bfe0100000065e8aebfc87f60fb83191253 (good)
;; QUESTION SECTION:
;; www.hola.com.                IN      A
;; ANSWER SECTION:
www.hola.com.                300     IN      CNAME   www.hola.com.edgekey.net.
www.hola.com.edgekey.net.    21600   IN      CNAME   e13750.a.akamaiedge.net.
e13750.a.akamaiedge.net.    20      IN      A       92.122.236.114
;; Query time: 1560 msec
;; SERVER: 127.0.0.1#53(127.0.0.1) (UDP)
;; WHEN: Wed Mar 06 17:58:23 UTC 2024
;; MSG SIZE rcvd: 160
root@server:/etc/bind#
```

Tarda mucho más, tiene que realizar la consulta directa en lugar de obtenerla de la caché

- b) Creación de zonas primarias. Supondremos un dominio ficticio midominio.net, que administra direcciones en el rango 160.50.40.0/24. Configurar dos zonas primarias para administrar las resoluciones directa e inversa.

- En /etc/bind/named.conf → crear zona
5. Cambiamos /etc/bind/named.conf e incluimos las zonas DIRECTA e INVERSA

```
include "/etc/bind/named.conf.options";
include "/etc/bind/named.conf.local";
include "/etc/bind/named.conf.default-zones";

zone "midominio.net"{
    type master;
    file "/etc/bind/midominio.net.hosts";
};

zone "40.50.160.in-addr.arpa"{
    type master;
    file "/etc/bind/40.50.160.in-addr.arpa";
};
```

(Importante que estén las zonas debajo de include)

6. Creamos los archivos los archivos de zona.

```
zone "localhost" {
    type master;
    file "/etc/bind/db.localhost";
};

zone "127.in-addr.arpa" {
    type master;
    file "/etc/bind/db.127";
};

zone "0.in-addr.arpa" {
    type master;
    file "/etc/bind/db.0";
};

zone "255.in-addr.arpa" {
    type master;
    file "/etc/bind/db.255";
};
```

En Ubuntu todo va en la misma carpeta. Si entramos en named.conf.default-zones vemos que todos los archivos de zonas se guardan ahí. Luego escribiremos los archivos en la carpeta /etc/bind

midominio.net.hosts:

```
$TTL 86400
@ IN SOA ns1.midominio.net. admin.midominio.net. (
    2024030801
    3600      ; Tiempo de reintento
    1800      ; caducidad
    604800
    86400 )

@ IN NS ns1.midominio.net.

ns1 IN A 160.50.40.1
ordenador_orianna IN A 160.50.40.2
ordenador_carlos IN A 160.50.40.3
ordenador_maria IN A 160.50.40.4
```

40.50.160.in-addr.arpa

```
$TTL 86400
@ IN SOA ns1.midominio.net. admin.midominio.net. (
    2024030801
    3600
    1800
    604800
    86400 ) |

@ IN NS ns1.midominio.net.

1 IN PTR ns1.midominio.net.
2 IN PTR ordenador_orianna.midominio.net.
3 IN PTR ordenador_carlos.midominio.net.
4 IN PTR ordenador_maria.midominio.net.
```

- Systemctl restart name

- c) Mantenimiento de zonas primarias. Añadir los siguientes registros a las zonas creadas: A (zipi, 160.50.40.1), A (zape, .2), A (mortadelo, .4), A (correo, .50), A (dns1, nuestra propia dirección IP), A (www, a las direcciones 160.50.40.200 y 160.50.40.201), NS (dns1), CNAME (aplicaciones -> mortadelo), MX (correo, prioridad 20). Todos los registros de tipo A deben tener asociado su correspondiente registro PTR. Verificar su funcionamiento con el cliente de DNS (dig o nslookup)

named.conf de VM2:

```
zone "midominio.net" IN {
    type slave;
    file "/etc/bind/midominio.net.hosts";
    masters { 192.168.119.137; };
    allow-notify { 192.168.119.137; };
    allow-transfer {none; };
};
```

Agregamos los registros a midominio.net.hosts:

```
$TTL 86400
@ IN SOA ns1.midominio.net. admin.midominio.net. (
    2022103062
    86400 ; Tiempo de refresco
    7200 ; Tiempo de reintento
    3600000 ; Caducidad
    86400 ) ; TTL min

@ IN NS dns1

zipi IN A 160.50.40.1
zape IN A 160.50.40.2
mortadelo IN A 160.50.40.4
correo IN A 160.50.40.50
dns1 IN A 192.168.119.137
www IN A 160.50.40.200

aplicaciones IN CNAME mortadelo
correo IN MX 20 correo
```

Agregamos registros a 40.50.160.in-addr.arpa

```
$TTL 86400
@ IN SOA dns1.midominio.net. admin.midominio.net. (
    2022143063
    86400
    7200
    3600000
    86400 )

@ IN NS dns1.midominio.net.

1 IN PTR zipi.midominio.net.
2 IN PTR zape.midominio.net.
4 IN PTR mortadelo.midominio.net.
50 IN PTR correo.midominio.net.
200 IN PTR www.midominio.net.
201 IN PTR www.midominio.net.
```

Reiniciamos el servicio “named” y comprobamos

```
root@server:/etc/bind# dig @localhost zape.midominio.net

; <<>> DiG 9.18.18-0ubuntu0.22.04.2-Ubuntu <<>> @localhost zape.midominio.net
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 36910
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 972b79ba159bfa880100000065eaf21e07f947925e57be58 (good)
;; QUESTION SECTION:
;zape.midominio.net.          IN      A

;; ANSWER SECTION:
zape.midominio.net.          86400   IN      A           160.50.40.2

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(localhost) (UDP)
;; WHEN: Fri Mar 08 11:10:22 UTC 2024
;; MSG SIZE rcvd: 91
```

```
root@server:/etc/bind# dig @localhost -x 160.50.40.1

; <<>> DiG 9.18.18-0ubuntu0.22.04.2-Ubuntu <<>> @localhost -x 160.50.40.1
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 27704
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: b1d243fe39df48740100000065eaf3bd638c350076553dd2 (good)
;; QUESTION SECTION:
;1.40.50.160.in-addr.arpa.    IN      PTR

;; ANSWER SECTION:
1.40.50.160.in-addr.arpa.    86400   IN      PTR           zipi.midominio.net.

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(localhost) (UDP)
;; WHEN: Fri Mar 08 11:17:17 UTC 2024
;; MSG SIZE rcvd: 113
```



- d) Sincronización primaria-secundarias. Vamos a replicar la zona midominio.net en otro servidor de DNS secundario. Arrancar la segunda máquina virtual (VM2) e instalar nuevamente el servidor Bind 9. A continuación establecer una zona secundaria del dominio midominio.net. En el servidor maestro añadir otra entrada NS (dns2) apuntando a la dirección IP del nuevo servidor. Configurar en ambos servidores los parámetros que permitirán la transferencia de la zona. Reiniciar ambos servidores y comprobar que el secundario mantiene una copia de la zona. Llevar a cabo algún cambio en la zona maestra incrementando su número de serie. Reiniciar el servidor y verificar que se actualiza la zona secundaria. Nota: se recomienda configurar la notificación explícita a las secundarias (notify explicit) y la directiva also-notify con la dirección IP del servidor secundario. Delegación de un subdominio

- 1) Editar archivo named.conf.local (VM2):
- 2) Añade la entrada NS en el servidor maestro (VM1)
- 3) Configurar la transferencia de Zona
- 4) Reiniciar los servidores dns1 (VM1) y dns2 (VM2)
- 5) Verificar funcionamiento

#### *Máquina Virtual Ubuntu (VM1)*

named.conf

```
zone "midominio.net"{
    type master;
    file "/etc/bind/midominio.net.hosts";
    notify explicit;
    also-notify { 192.168.119.138; };
    allow-transfer { 192.168.119.138; };
};
```

Actualizar entradas NS:

```
$TTL 86400
@ IN SOA ns1.midominio.net. admin.midominio.net. (
    1000000003 ; Cambio para facilitar cambio de num serie
    86400
    7200
    3600000
    86400 )

@ IN NS dns1
@ IN NS dns2

zipi IN A 160.50.40.1
zape IN A 160.50.40.2
mortadelo IN A 160.50.40.4
correo IN A 160.50.40.50
dns1 IN A 192.168.119.137
dns2 IN A 192.168.119.138
www IN A 160.50.40.200

aplicaciones IN CNAME mortadelo
correo IN MX 20 correo
```

Cambiamos número de serie porque hemos cambiado el archivo

Reiniciamos servidor → systemctl restart named

### *Máquina Virtual Rocky (VM2)*

Arrancamos bind:

```
[root@server ~]# netstat -utlp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:ssh             0.0.0.0:*               LISTEN      36629/sshd: /usr/sb
tcp6       0      0 [::]:ssh                [::]:*                 LISTEN      36629/sshd: /usr/sb
udp        0      0 0.0.0.0:323             0.0.0.0:*               *          798/chronyd
udp6       0      0 localhost:323           [::]:*                 *          798/chronyd
[root@server ~]# systemctl start named
[root@server ~]# netstat -utlp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:ssh             0.0.0.0:*               LISTEN      36629/sshd: /usr/sb
tcp        0      0 localhost:domain        0.0.0.0:*               LISTEN      60433/named
tcp        0      0 localhost:rndc           0.0.0.0:*               LISTEN      60433/named
tcp6       0      0 [::]:ssh                [::]:*                 LISTEN      36629/sshd: /usr/sb
tcp6       0      0 localhost:domain        [::]:*                 LISTEN      60433/named
tcp6       0      0 localhost:rndc          [::]:*                 LISTEN      60433/named
udp        0      0 localhost:domain        0.0.0.0:*               *          60433/named
udp        0      0 localhost:323           0.0.0.0:*               *          798/chronyd
udp6       0      0 localhost:domain        [::]:*                 *          60433/named
udp6       0      0 localhost:323           [::]:*                 *          798/chronyd
[root@server ~]#
```

/etc/named.conf (VM2)

```
zone "midominio.net" IN {
    type slave;
    file "/etc/bind/midominio.net.hosts";
    masters { 192.168.119.137; };
    allow-notify { 192.168.119.137; };
    allow-transfer {none; };
};
```

### *Comprobación*

Funcionamiento VM1 sigue siendo el mismo:

```
root@server:/etc/bind# dig @localhost zape.midominio.net

; <<>> DiG 9.18.18-0ubuntu0.22.04.2-Ubuntu <<>> @localhost zape.midominio.net
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 4484
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 8c930b19f59b5b2b0100000065eb0a37353f7b906920d4a9 (good)
;; QUESTION SECTION:
;zape.midominio.net.          IN      A

;; ANSWER SECTION:
zape.midominio.net.          86400   IN      A          160.50.40.2

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(localhost) (UDP)
;; WHEN: Fri Mar 08 12:53:11 UTC 2024
;; MSG SIZE rcvd: 91
```

Desde VM2 podemos hacer dig a las zonas de VM1

```
[root@server etc]# dig @localhost zape.midominio.net

;<<>> DiG 9.16.23-RH <<>> @localhost zape.midominio.net
; (2 servers found)
; global options: +cmd
; Got answer:
;->HEADER<- opcode: QUERY, status: NOERROR, id: 42668
; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 1b686db18a83f5030100000065eb186797e4127f756c6ce5 (good)
;; QUESTION SECTION:
;zape.midominio.net.                IN      A

;; ANSWER SECTION:
zape.midominio.net.                86400   IN      A      160.50.40.2

;; Query time: 1 msec
;; SERVER: ::1#53(::1)
;; WHEN: Fri Mar 08 14:53:43 CET 2024
;; MSG SIZE rcvd: 91
```

Cambiaremos la IP de una dirección (y el número de serie) para comprobar que la máquina 2 también se actualiza.

```
# zipi      IN A 160.50.40.11
```

```
$TTL 86400
@      IN      SOA      ns1.midominio.net. admin.midominio.net. (
1000000004      ; Cambio para facilitar cambio de num serie
86400
7200
3600000
86400 )

@      IN      NS       dns1
@      IN      NS       dns2

zipi      IN      A      160.50.40.11
zape      IN      A      160.50.40.2
mortadelo IN      A      160.50.40.4
correo    IN      A      160.50.40.50
dns1      IN      A      192.168.119.137
dns2      IN      A      192.168.119.138
www       IN      A      160.50.40.200

aplicaciones IN CNAME mortadelo
correo      IN      MX      20 correo
```

(systemctl restart named)

```
[root@server etc]# dig @localhost zipi.midominio.net

;<<>> DiG 9.16.23-RH <<>> @localhost zipi.midominio.net
; (2 servers found)
; global options: +cmd
; Got answer:
;->HEADER<- opcode: QUERY, status: NOERROR, id: 2811
; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 0475e2a256986d650100000065eb1a5143c50d542438cd80 (good)
;; QUESTION SECTION:
;zipi.midominio.net.                IN      A

;; ANSWER SECTION:
zipi.midominio.net.                86400   IN      A      160.50.40.11

;; Query time: 1 msec
;; SERVER: ::1#53(::1)
;; WHEN: Fri Mar 08 15:01:53 CET 2024
;; MSG SIZE rcvd: 91
```

- e) Delegación de un subdominio. Crear una nueva zona maestra pruebas.com en el servidor VM2. Vamos a configurar la delegación de un subdominio (por ejemplo, ceu.pruebas.com), cuya **zona maestra se ubicará en el otro servidor de DNS (VM1)**. Para hacer las pruebas añadir algún registro A en el nuevo subdominio y verificar que una petición de resolución dirigida al servidor VM2 y relativa al subdominio, es reenviada y resuelta en el servidor VM1. Comprobar igualmente el efecto de la directiva recursión yes/no en el comportamiento del servidor que aloja el **dominio principal (VM2)**.

#### Ficheros de Zona y named.conf:

- Máquina VM2 (Rocky) – principal

# vim /var/named/pruebas.com.hosts

```
$TTL 86400
@      IN      SOA      ns1.pruebas.com. admin.pruebas.com. (
                                15
                                86400
                                7200
                                3600000
                                86400 )

@      IN      NS       ns1.pruebas.com.
ns1     IN      A        192.168.119.138
ceu     IN      NS       ns1.ceu
ns1.ceu IN      A        192.168.119.137
uhceu   IN      A        192.168.200.2
```

Hemos añadido la dirección uhceu para hacer pruebas.

```
zone "ceu.pruebas.com" {
    type master;
    file "/etc/bind/ceu.pruebas.com.hosts";
};
```

- Máquina VM1 (Ubuntu)

/etc/ceu.pruebas.com.hosts

```
$TTL 86400
@      IN      SOA      ns1.ceu.pruebas.com. admin.ceu.pruebas.com. (
                                10
                                86400
                                7200
                                3600000
                                86400 )

@      IN      NS       ns1.ceu.pruebas.com.
ns1     IN      A        192.168.119.137 ; IP de VM1
ade     IN      A        192.168.119.150
gisi    IN      A        203.0.113.1
teleco.ceu.pruebas.com. IN  A        192.168.119.151
```

Hemos añadido tres direcciones dentro del dominio de ceu.pruebas.com (teleco, gisi y ade)

```
zone "pruebas.com" IN {
    type master;
    file "/var/named/pruebas.com.hosts";
    notify explicit;
    allow-transfer {localhost; 192.168.119.137; };
    # also-notify { 192.168.119.137; };
};
```

## Configuración de Opciones:

- VM2 /etc/named.conf

```
listen-on-v6 { any; };
listen-on port 53 { any; };
allow-query {any; };
allow-transfer {192.168.119.138; };
recursion yes;
```

# *allow-query{any;};* → permite la consulta desde la propia máquina (localhost) y desde la red 192.168.119.0/24. Hemos activado las queries a todas las direcciones que empiezan por 192.168.119.\_\_\_\_ (Para las pruebas era lo más oportuno pues la direcciones IP de las máquinas solían cambiar)

- VM1 /etc/bind/named.conf.options

```
options {
    listen-on port 53 {any; };
    listen-on-v6 port 53 { any; };
    directory "/var/named";
    dump-file "/var/named/data/cache_dump.db";
    statistics-file "/var/named/data/named_stats.txt";
    memstatistics-file "/var/named/data/named_mem_stats.txt";
    secroots-file "/var/named/data/named.secroots";
    recursing-file "/var/named/data/named.recursing";
    allow-query { localhost; 192.168.119.0/24; };
    recursion yes;
```

# *allow-query { any; };* → Permite que cualquier host realice consultas DNS al servidor BIND.

# *allow-transfer { 192.168.119.138; };* → Permite transferencias de zona desde el servidor con la dirección IP `192.168.119.138` (VM2). Especifica que el servidor principal está autorizado para realizar transferencias de zona.

# *recursion yes;* → Habilita la recursión en el servidor BIND, permitiéndole realizar consultas recursivas en nombre de clientes.

¿Porqué no configuramos el servidor de subdominio como slave?

En el contexto de la delegación, se espera que el servidor que maneja el subdominio tenga control total sobre ese subdominio. La utilización de un tipo de zona `slave` implica que el servidor esclavo obtiene su información de zona directamente del servidor maestro. Si el tipo de zona fuera `slave`, la información de la zona estaría vinculada al servidor maestro, y cualquier cambio requeriría modificaciones en el servidor maestro.

Desde VM1 llamamos a VM2 y preguntamos por una IP del dominio ceu.pruebas.com.

```
root@server:/etc/bind# dig @192.168.119.138 gisi.ceu.pruebas.com

; <<>> DiG 9.18.18-0ubuntu0.22.04.2-Ubuntu <<>> @192.168.119.138 gisi.ceu.pruebas.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 33460
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 46b319be8b86421e0100000065ec83e0ca94e623c639dd83 (good)
;; QUESTION SECTION:
;gisi.ceu.pruebas.com.      IN      A

;; ANSWER SECTION:
gisi.ceu.pruebas.com.      86400   IN      A      203.0.113.1

;; Query time: 7 msec
;; SERVER: 192.168.119.138#53(192.168.119.138) (UDP)
;; WHEN: Sat Mar 09 15:44:32 UTC 2024
;; MSG SIZE rcvd: 93
```

Desde VM2 preguntamos en local por una IP del dominio ceu.pruebas.com

```
[root@server etc]# dig @localhost gisi.ceu.pruebas.com

; <<>> DiG 9.16.23-RH <<>> @localhost gisi.ceu.pruebas.com
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 2707
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: e31e93cb81c712720100000065ec844038ec800a18a89856 (good)
;; QUESTION SECTION:
;gisi.ceu.pruebas.com.      IN      A

;; ANSWER SECTION:
gisi.ceu.pruebas.com.      86304   IN      A      203.0.113.1

;; Query time: 1 msec
;; SERVER: ::1#53(::1)
;; WHEN: Sat Mar 09 16:46:08 CET 2024
;; MSG SIZE rcvd: 93
```

Comprobar igualmente el efecto de la directiva recursión yes|no en el comportamiento del servidor que aloja el dominio principal (VM2).

```
options {
    listen-on port 53 {any; };
    listen-on-v6 port 53 { any; };
    directory      "/var/named";
    dump-file       "/var/named/data/cache_dump.db";
    statistics-file "/var/named/data/named_stats.txt";
    memstatistics-file "/var/named/data/named_mem_stats.txt";
    secroots-file   "/var/named/data/named.secroots";
    recursing-file  "/var/named/data/named.recursing";
    allow-query     { localhost; 192.168.119.0/24; };
    recursion no;
```

VM2

```
[root@server etc]# systemctl restart named
[root@server etc]# dig @localhost gisi.ceu.pruebas.com

; <<>> DiG 9.16.23-RH <<>> @localhost gisi.ceu.pruebas.com
; (2 servers found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 50945
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 2
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
;; EDNS: version: 0, flags:; udp: 1232
;; COOKIE: a16882e6ee2740870100000065ec8e5a3dd910f9da47cd65 (good)
;; QUESTION SECTION:
;gisi.ceu.pruebas.com.      IN      A

;; AUTHORITY SECTION:
ceu.pruebas.com.          86400   IN      NS      ns1.ceu.pruebas.com.

;; ADDITIONAL SECTION:
ns1.ceu.pruebas.com.      86400   IN      A       192.168.119.137

;; Query time: 1 msec
;; SERVER: ::1#53(:1)
;; WHEN: Sat Mar 09 17:29:14 CET 2024
;; MSG SIZE rcvd: 111
```

Como se aprecia, no ha devuelto la dirección IP sino la IP del servidor que lleva el dominio ceu.pruebas.com (VM1, 192.168.119.137)