

# DNS LINUX BIND

 [Descargar PDF](#)

## ▼ DNS LINUX BIND

- INTRODUCCIÓN
- INSTALACIÓN
- ▼ ARCHIVOS DE CONFIGURACIÓN
  - NAMED.CONF
  - NAMED.CONF.OPTIONS
  - NAMED.CONF.LOCAL
  - DB.ZONA
- ▼ ZONAS
  - ▼ RESOLUCIÓN
    - DIRECTAS
    - INVERSAS
  - ▼ TIPO
    - MASTER
    - SLAVE
    - STUB
    - FORWARD
  - ▼ REGISTROS DE RECURSOS
    - ESQUEMA RR
    - DIRECTIVAS
    - ▼ TIPOS DE REGISTROS
      - SOA
      - NS
      - A
      - AAAA
      - PTR
      - CNAME
      - MX
  - ▼ OPCIONES
    - ACL
    - DIRECTORY
    - FORWARDERS
    - LISTEN-ON
    - RECURSION
    - ALLOW-RECURSION
    - ALLOW-QUERY-CACHE
    - CACHE
    - ALLOW-QUERY
  - DELEGACIÓN DE DOMINIOS

▼ TRANSFERENCIAS DE ZONAS

- ALLOW-TRANSFER
- CLAVES TSIG
- NOTIFY
- BALANCEO DE CARGA
- DNSSEC
- DDNS

▼ FICHEROS DE LOG

- RSYSLOGD
- JOURNALD
- CLAUSULA LOGGING

# INTRODUCCIÓN

Los sistemas Linux incorporan en sus repositorios los paquetes `dnsmasq` y `bind9` para implementar servidores DNS, siendo `bind9` el servidor más utilizado por su potencia y versatilidad.

## INSTALACIÓN

Podemos instalar BIND en prácticamente cualquier distribución Linux, nosotros nos centraremos en las distribuciones Linux Alpine y Linux Debian.

### Instalación

En un sistema Linux Alpine

```
root@pc~# apk update && apk add bind
root@pc~# apk update && apk add bind-tools
```

En un sistema Linux Debian

```
root@pc~# apt update && apt install bind9 -y
root@pc~# apt update && apt install dnsutils -y
```

Para comprobar la versión instalada ejecutar el siguiente comando.

```
#Ejemplo salida named-v
named -v
BIND 9.16.50
```

Los archivos ejecutables instalados son:

Comando	Ruta más común	Descripción
<code>named</code>	<code>/usr/sbin/</code>	servidor DNS
<code>named-checkconf</code>	<code>/usr/sbin/</code>	verifica fichero de configuracion
<code>named-checkzone</code>	<code>/usr/sbin/</code>	verifica fichero de zona
<code>named-compilezone</code>	<code>/usr/sbin/</code>	verifica y convierte en binario un archivo de zona
<code>rndc</code>	<code>/usr/sbin/</code>	control del servicio named

Las utilidades instaladas son:

Comando	Ruta más común	Descripción
<code>dig</code>	<code>/usr/bin/</code>	consultas y diagnostico detallado de DNS
<code>nslookup</code>	<code>/usr/bin/</code>	consultas básicas de DNS

Comando	Ruta más común	Descripción
host	/usr/bin/	consultas rápidas y simples de DNS

Los servicios instalados son:

Sistemas	Servicio
System V	/etc/init.d/named
SystemD	/lib/systemd/system/named.service

Linux Debian utiliza System V o SystemD dependiendo de la versión del sistema. Los sistemas Linux Alpine utilizan OpenRC una versión ampliada de System V.

Para forzar que el servicio se ejecute solo usando la pila IPv4 debemos modificar los parametros de llamada al servicio y añadir la opción `-4`.

### named IPv4

En un servidor DNS sobre un sistema Linux con SystemD se quiere configurar BIND para utilizar solamente la pila de protocolos IPv4.

```
#parar el servicio
systemctl stop named

#editar fichero de opciones del servicio y modificar OPTIONS
nano /etc/default/named
....
OPTIONS="-u bind -4"
....

#iniciar el servicio
systemctl start named
```

Las acciones más comunes para gestionar el servicio DNS son:

Acción	System V	SystemD	OpenRC
Habilitar	update-rc.d named defaults	systemctl enable named	rc-update add named default
Deshabilitar	update-rc.d -f named remove	systemctl disable named	rc-update del named
Iniciar	service named start	systemctl start named	rc-service named start
Parar	service named stop	systemctl stop named	rc-service named stop
Reiniciar	service named restart	systemctl restart named	rc-service named restart
Estado	service named status	systemctl status named	rc-service named status

# ARCHIVOS DE CONFIGURACIÓN

Los archivos de configuración se almacenan en la carpeta `/etc/bind/`. A continuación se describen los principales archivos de configuración que permiten una configuración modular y flexible:

## NAMED.CONF

El archivo `named.conf` es el archivo de configuración general e incorpora una serie de cláusulas `include` que especifican archivos que configuran distintos aspectos del servidor.

### named.conf

```
//use this file for global options
include "/etc/bind/named.conf.options";
//use this file for local zones
include "/etc/bind/named.conf.local";
//default zones do not modify
include "/etc/bind/named.conf.default-zones";
```

**Nota:** la cláusula `include` se puede utilizar en cualquier archivo de configuración. Por ejemplo, podríamos poner dentro del archivo `named.conf.options` una cláusula `include` al archivo `named.conf.acl` utilizado para definir reglas de acceso.

**Nota:** el archivo `named.conf.default-zones` incluye las zonas por defecto en BIND y no se debe modificar.

### named.conf.default.zones

```
//root-servers
zone "."{
    type hint;
    file "/usr/share/dns/root.hints";
};
//RFC 1912
//localhost
zone "localhost"{
    type master;
    file "/etc/bind/db.local";
};
//localhost inverse
zone "127.in-addr.arpa"{
    type master;
    file "/etc/bind/db.127";
};
//net inverse
zone "0.in-addr.arpa"{
    type master;
    file "/etc/bind/db.0";
};
//broadcast inverse
zone "255.in-addr.arpa"{
    type master;
    file "/etc/bind/db.255";
};
```

# NAMED.CONF.OPTIONS

El archivo `named.conf.options` es el archivo en el que se **definen las opciones globales** de configuración del servidor DNS, como pueden ser los reenviadores (forwarders), listas de control de acceso (ACL), modo de resolución (recursivo o iterativo), la seguridad avanzada (DNSSEC) o la actualización dinámica (DDNS). Las opciones globales se definen dentro de la cláusula `options`. Evidentemente, existen numerosas opciones globales que modifican el comportamiento de BIND y se pueden encontrar en la documentación oficial de BIND.

```
1  named.conf.local
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
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
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1190
1191
1192
1193
1194
1195
1196
1197
1198
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1290
1291
1292
1293
1294
1295
1296
1297
1298
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1389
1390
1391
1392
1393
1394
1395
1396
1397
1398
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1790
1791
1792
1793
1794
1795
1796
1797
1798
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1890
1891
1892
1893
1894
1895
1896
1897
1898
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2079
2080
2081
2082
2083
2084
2085
2086
2087
2088
2089
2090
2091
2092
2093
2094
2095
2096
2097
2098
2099
2100
2101
2102
2103
2104
2105
2106
2107
2108
2109
2110
2111
2112
2113
2114
2115
2116
2117
2118
2119
2120
2121
2122
2123
2124
2125
2126
2127
2128
2129
2130
2131
2132
2133
2134
2135
2136
2137
2138
2139
2140
2141
2142
2143
2144
2145
2146
2147
2148
2149
2150
2151
2152
2153
2154
2155
2156
2157
2158
2159
2160
2161
2162
2163
2164
2165
2166
2167
2168
2169
2170
2171
2172
2173
2174
2175
2176
2177
2178
2179
2180
2181
2182
2183
2184
2185
2186
2187
2188
2189
2190
2191
2192
2193
2194
2195
2196
2197
2198
2199
2200
2201
2202
2203
2204
2205
2206
2207
2208
2209
2210
2211
2212
2213
2214
2215
2216
2217
2218
2219
2220
2221
2222
2223
2224
2225
2226
2227
2228
2229
2230
2231
2232
2233
2234
2235
2236
2237
2238
2239
2240
2241
2242
2243
2244
2245
2246
2247
2248
2249
2250
2251
2252
2253
2254
2255
2256
2257
2258
2259
2260
2261
2262
2263
2264
2265
2266
2267
2268
2269
2270
2271
2272
2273
2274
2275
2276
2277
2278
2279
2280
2281
2282
2283
2284
2285
2286
2287
2288
2289
2290
2291
2292
2293
2294
2295
2296
2297
2298
2299
2300
2301
2302
2303
2304
2305
2306
2307
2308
2309
2310
2311
2312
2313
2314
2315
2316
2317
2318
2319
2320
2321
2322
2323
2324
2325
2326
2327
2328
2329
2330
2331
2332
2333
2334
2335
2336
2337
2338
2339
2340
2341
2342
2343
2344
2345
2346
2347
2348
2349
2350
2351
2352
2353
2354
2355
2356
2357
2358
2359
2360
2361
2362
2363
2364
2365
2366
2367
2368
2369
2370
2371
2372
2373
2374
2375
2376
2377
2378
2379
2380
2381
2382
2383
2384
2385
2386
2387
2388
2389
2390
2391
2392
2393
2394
2395
2396
2397
2398
2399
2400
2401
2402
2403
2404
2405
2406
2407
2408
2409
2410
2411
2412
2413
2414
2415
2416
2417
2418
2419
2420
2421
2422
2423
2424
2425
2426
2427
2428
2429
2430
2431
2432
2433
2434
2435
2436
2437
2438
2439
2440
2441
2442
2443
2444
2445
2446
2447
2448
2449
2450
2451
2452
2453
2454
2455
2456
2457
2458
2459
2460
2461
2462
2463
2464
2465
2466
2467
2468
2469
2470
2471
2472
2473
2474
2475
2476
2477
2478
2479
2480
2481
2482
2483
2484
2485
2486
2487
2488
2489
2490
2491
2492
2493
2494
2495
2496
2497
2498
2499
2500
2501
2502
2503
2504
2505
2506
2507
2508
2509
2510
2511
2512
2513
2514
2515
2516
2517
2518
2519
2520
2521
2522
2523
2524
2525
2526
2527
2528
2529
2530
2531
2532
2533
2534
2535
2536
2537
2538
2539
2540
2541
2542
2543
2544
2545
2546
2547
2548
2549
2550
2551
2552
2553
2554
2555
2556
2557
2558
2559
2560
2561
2562
2563
2564
2565
2566
2567
2568
2569
2570
2571
2572
2573
2574
2575
2576
2577
2578
2579
2580
2581
2582
2583
2584
2585
2586
2587
2588
2589
2590
2591
2592
2593
2594
2595
2596
2597
2598
2599
2600
2601
2602
2603
2604
2605
2606
2607
2608
2609
2610
2611
2612
2613
2614
2615
2616
2617
2618
2619
2620
2621
2622
2623
2624
2625
2626
2627
2628
2629
2630
2631
2632
2633
2634
2635
2636
2637
2638
2639
2640
2641
2642
2643
2644
2645
2646
2647
2648
2649
2650
2651
2652
26
```

## file define registro de recursos

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

zone "192.168.1.in-addr.arpa." {
    type master;
    file "/etc/bind/db.192.168.1.in-addr.arpa";
};
```

Podemos comprobar la sintaxis de un archivo de configuración mediante el comando `named-checkconf` y la sintaxis de un archivo de recursos de una zona mediante el comando `named-checkzone`.

### Comprobación de archivos

```
#comprobar archivo de configuracion opciones globales
named-checkconf /etc/bind/named.conf.options

#comprobar archivo de configuracion de zonas
named-checkconf /etc/bind/named.conf.local

#comprobar fichero de recursos de zona ser.smr
named-checkzone ser.smr /etc/bind/db.ser.smr
```

# ZONAS

## RESOLUCIÓN

En cuanto a la **resolución del nombre** tenemos 2 tipos de zonas:

### DIRECTAS

Son aquellas zonas cuyos registros resuelven la relación Nombre - IP. Es decir, son aquellas zonas a las que se les pregunta el nombre y devuelven la IP correspondiente. Se definen usando el siguiente esquema:

```
//zona directa
zone <dominio.> {
    type {master,slave,stub} ;
    file "/etc/bind/db.<dominio>"
    [opciones]
};
```

### Definición zona directa

```
//zona directa para el nombre ser.smr
zone "ser.smr." {
    type master;
    file "/etc/bind/db.ser.smr";
};
```

## INVERSAS

Son aquellas zonas cuyos registros resuelven la relación IP - Nombre. Es decir, son aquellas zonas a las que se les pregunta por una IP y devuelven el nombre correspondiente. **Como nombre de zona se utiliza la inversa de la IP de red y el sufijo in-addr.arpa.** Se definen usando el siguiente esquema:

```
//zona inversa
zone <net.in-addr.arpa.> {
    type {master,slave,stub} ;
    file "/etc/bind/db.<net.in-addr.arpa>"
    [opciones]
};
```

### Definición zona inversa

```
//zona inversa para la red 192.168.1.0/24
zone "1.168.192.in-addr.arpa."{
    type master;
    file "/etc/bind/db.1.168.192.in-addr.arpa";
};
```

## TIPO

En cuanto al **tipo de zona** (opción `type`) tenemos 4 tipos de zonas:

### MASTER

Una zona master define una **zona principal** o primaria sobre la que el servidor DNS tiene **autoridad**. Se definen usando el siguiente esquema:

```
//zona directa
zone <dominio.> {
    type master;
    file "/etc/bind/db.<dominio>";
    [opciones]
};

//zona inversa
zone <net.in-addr.arpa.> {
    type master;
    file "/etc/bind/db.<net.in-addr.arpa>";
    [opciones]
};
```

### Zonas Master

Un servidor DNS define la zona ser.smr para la red 192.168.1.0/24. La definición de la zona master directa e inversa sería:



```

zone "ser.smr." {
    type master;
    file "/etc/bind/db.ser.smr";
};

zone "1.168.192.in-addr.arpa." {
    type master;
    file "/etc/bind/db.1.168.192.in-addr.arpa";
};

```

## SLAVE

Una zona slave define una **zona esclava** o secundaria de una zona master sobre la que el servidor DNS tiene **autoridad**. Las zonas esclavas son una **copia completa de una zona master** y por tanto son autoritativas. El proceso por el cual la zona esclava realiza la copia o sincronización de la zona master se denomina **transferencia de zona**. Se ha de asegurar que los archivos de recursos de las zonas slave tengan los permisos necesarios para poder ser escritos tras las transferencias de zonas. El directorio `/var/lib/bind/` tiene los permisos adecuados y suele ser el utilizado para guardar estas zonas slaves. El esquema de definición de las zonas slaves es el siguiente:

```

//zona directa
zone <dominio.> {
    type slave;
    file "/var/lib/bind/db.<dominio>";
    masters { <IP-master> ; <IP-master> };
    [opciones]
};

//zona inversa
zone <net.in-addr.arpa.> {
    type slave;
    file "/var/lib/bind/db.<net.in-addr.arpa>";
    masters { <IP-master> ; <IP-master> };
    [opciones]
};

```

### Zonas Slave

Un servidor DNS define la zona esclava ser.smr que esta definida en el servidor 192.168.1.254. La definición de la zona slave directa e inversa sería:

```

zone "ser.smr." {
    type slave;
    file "/var/lib/bind/db.ser.smr";
    masters { 192.168.1.254; };
};

zone "1.168.192.in-addr.arpa." {
    type slave;
    file "/var/lib/bind/db.1.168.192.in-addr.arpa";
    masters { 192.168.1.254; };
};

```

Los archivos de registros de las zonas transferidas se guardan en formato RAW para agilizar la carga por parte del servidor DNS, podemos convertirlos a texto usando la utilidad `named-compilezone` .

### RAW a TXT

```
#named-compilezone -f raw -F text -o <fichero.txt> <zona> <fichero.raw>
named-compilezone -f raw -F text -o db.ser.smr.txt ser.smr /var/lib/bind/db.ser.smr.saved
```

## STUB

Una zona stub define una **zona esclava** o secundaria de una zona master sobre la que el servidor DNS tiene **autoridad**. Las zonas stub son una **copia parcial de una zona master**. Estas zonas solo copian los registros SOA y NS del archivo de resolución de la zona master y se utilizan fundamentalmente para facilitar la resolución recursiva de nombres en otra zona sin transferir toda la base de datos de esa zona. Permite que el servidor sepa qué servidores son autoritativos para dicha zona. El esquema de definición es el siguiente.

```
//zona directa
zone <dominio.> {
    type stub;
    file "/var/lib/bind/db.<dominio>";
    masters { <IP-master> ; <IP-master> };
    [opciones]
};
//zona inversa
zone <net.in-addr.arpa.> {
    type stub;
    file "/var/lib/bind/db.<net.in-addr.arpa>";
    masters { <IP-master> ; <IP-master> };
    [opciones]
};
```

## FORWARD

Una zona forward define una **zona de reenvío** de otra zona definida en un servidor DNS. Estas zonas no responden autoritativamente ya que no definen la zona sino que reenvían las peticiones a otros servidores que si las definen. No se hace forwarding para zonas inversa. El esquema de definición es el siguiente.

```
//zona directa
zone <dominio.> {
    type forward;
    forwarders { <IP-fowarder> ; <IP-fowarder> };
    forward only;
    [opciones]
};
```



### Zona Foward

Un servidor DNS define la zona forward ser.smr que esta definida en el servidor 192.168.1.254. La definición de la zona de forwarding sería:

```
zone "ser.smr." {
    type forward;
    forwarders { 192.168.1.254; };
    forward only;
};
```

# REGISTROS DE RECURSOS

Los archivos de resolución de nombres ( `db.<zona>` ) consisten en una colección de elementos llamados **RR** o **registros de recurso** (*resource records*). Los registros de recurso **son las unidades de consulta**, es decir, son los registros que un servidor DNS devuelve cuando se le realiza una consulta.

Los registros de recursos tienen 5 campos, algunos de ellos opcionales. Los campos que no se especifican toman un valor por defecto.

## ESQUEMA RR

Nombre	TTL	Clase	Tipo	Datos
--------	-----	-------	------	-------

- **Nombre**

Nombre DNS del recurso. Puede ser un nombre fqdn (Fully Qualified Domain Name), o un nombre corto o no fqdn.



### Ejemplo fqdn y no fqdn

```
ser.smr.    ; es un nombre fqdn ya que acaba en . ,es decir, en la raíz.  
ns          ; es un nombre no fqdn  
www.ser     ; es un nombre no fqdn
```

- **TTL (time to live)**

**Tiempo en segundos** que un registro de recurso **permanece** en la **memoria caché** de un cliente. Puede especificarse en semanas ( `w` ) días ( `d` ), horas ( `h` ), minutos ( `m` ) o segundos ( `s` ), si no se especifica unidad de tiempo se suponen segundos. Si el valor es 0, el registro no se guarda en la memoria caché.



### TTL

```
1h30m      ; TTL de 1 hora y 30 minutos  
86400      ; TTL de 1 día por defecto en segundos  
3600s      ; TTL de 1 hora expresado en segundos
```

- **Clase**

Espacio de nombres a los que pertenece el registro. Aunque existen varios espacios hoy solo se usa el de Internet, el resto están en desuso. Su valor es el siguiente:

- **IN** Internet
- CH Chaos (diagnóstico)
- HS Hesiod (MIT)

- **Tipo**

Identifica el tipo de registro de recurso. Algunos valores habituales son: SOA, NS, A, AAAA, PTR, MX, CNAME, etc.

- **Datos**

Datos del registro. Dependen del tipo de registro.

# DIRECTIVAS

Para mejorar la legibilidad de los archivos de resolución de zonas se suelen definir las siguientes **directivas**:

- **\$ORIGIN**

Define el **nombre fqdn de la zona** que se configura en el archivo. La directiva \$ORIGIN es **usada** por BIND **para completar los nombres de registro no fqdn**. El caracter @ se utiliza para expandir el valor de esta directiva en el campo nombre de los RR. Además si en un RR no se especifica nombre (espacio en blanco) se sustituye por el nombre del registro anterior. Si en un fichero `db` no se define la directiva entonces su valor por defecto es el nombre de la zona, sin embargo, por legibilidad se suele recomendar definirla.

## Ejemplo \$ORIGIN

En el archivo `db.ser.smr` que define la zona `ser.smr` se define la siguiente directiva \$ORIGIN

```
$ORIGIN ser.smr. ; acaba en . -> fqdn
...
;nombre ttl  clase  tipo  dato
@      1h   IN      NS    ns.ser.smr. ; @=$ORIGIN=ser.smr.
ns     1h   IN      A     192.168.1.254 ; ns.ser.smr.
      1h   IN      A     192.168.1.253 ; espacio=ns.ser.smr.
...
```

- **\$TTL (time to live)**

Define el **tiempo** en segundos que **por defecto** que un registro DNS permanece en la **caché**. Este valor se aplica a aquellos registros de recursos que no definan su propio TTL. Si no se define esta directiva su valor por defecto es 1 hora. Para definir el tiempo se puede usar el valor en segundos o bien los símbolos w (week), h (hour), m (minute), s (second).

## Ejemplo \$TTL

En el archivo `db.ser.smr` que define la zona `ser.smr` se define la siguiente directiva \$TTL

```
$TTL 1h30m
...
;nombre ttl  clase  tipo  dato
@      2h   IN      NS    ns.ser.smr. ; TTL 2h
ns     IN    A      192.168.1.254 ; TTL=$TTL=1h30m
...
```

# TIPOS DE REGISTROS

## SOA

Define las características globales de la zona como por ejemplo el servidor que la define o la sincronización con zonas esclavas. En cada archivo `db` solamente puede existir un registro SOA y es el primer registro que se debe definir en la zona. Se define con el siguiente esquema

```

<nombre> <t1> IN SOA <server> <email> (
    <serial>
    <refresh>
    <retry>
    <expire>
    <nxdomain>
)

```

campo	descripción
<nombre>	Nombre fqdn de la zona. Si se ha definido directiva \$ORIGIN su valor suele ser @.
<t1>	TTL del registro. Si se omite su valor será \$TTL.
IN	Clase del registro Internet
SOA	Tipo de Registro Start Of Authority
<server>	Nombre fqdn del servidor que define la zona
<email>	Dirección de correo del administrador de la zona. Como las direcciones de correo tienen la forma usuario@servidor y la @ es un símbolo reservado se utiliza el carácter "." en lugar de arroba. Por ejemplo, si el email es <a href="mailto:admin@google.com">admin@google.com</a> se escribe <a href="mailto:admin.google.com">admin.google.com</a>
<serial>	Se utiliza en la sincronización con las zonas esclavas. Cuando una zona esclava solicita transferencia de zona comprueba el serial, si este es mayor que el de la zona esclava entonces se produce la transferencia de zona. Como número serial se suele utilizar la fecha en formato americano seguido de un valor secuencial de dos dígitos. Por ejemplo, si se ha modificado la zona el 15 de Diciembre de 2025 por segunda vez en el día su serial sería 2025121502.
<refresh>	Se utiliza en la sincronización con las zonas esclavas. Tiempo de espera de las zonas esclavas para volver a sincronizar la zona.
<retry>	Se utiliza en la sincronización con las zonas esclavas. Tiempo de espera de las zonas esclavas después de un fallo en la sincronización de la zona.
<expire>	Se utiliza en la sincronización con las zonas esclavas. Tiempo máximo que una zona esclava puede seguir usando la zona sin sincronizarse.
<nxdomain>	TTL que un registro nxdomain (dominio no existe) de esta zona debe ser almacenado en la cache

**Nota:** Los tiempos se expresan en segundos aunque se pueden usar las unidades w,h,m,s de forma similar a los TTL.

## SOA

Ejemplo registro SOA para el dominio ser.smr.

```

$ORIGIN ser.smr.
$TTL 2d

@ IN SOA ns.ser.smr. admin.ser.smr. (
    2025121502      ; serial
    1d              ; refresh
    3h              ; retry
    1w              ; expire
    1h              ; nxdomain
)

```

## NS

Define los servidores autorizados para la zona. Es un registro obligatorio. Puede existir más de un registro NS, por ejemplo, cuando una zona esta definida en otros servidores que definen la zona como esclava. Se define con el siguiente esquema:

```
<nombre> <ttl> IN NS <server>
```

campo	descripción
<nombre>	Nombre fqdn de la zona. Si se ha definido directiva \$ORIGIN su valor suele ser @.
<ttl>	TTL del registro. Si se omite su valor será \$TTL.
IN	Clase del registro Internet
NS	Tipo de Registro Name Server
<server>	Nombre fqdn del servidor que define la zona

## NS

Ejemplo registro NS para el dominio ser.smr.

```

$ORIGIN ser.smr.
$TTL 2d
....
@ IN NS ns.ser.smr. ;server master
  IN NS nss.ser.smr. ;server slave
....

```

## A

Define la IPv4 asociada a un nombre. Se utiliza en la resolución directa de un nombre. Se define con el siguiente esquema:

```
<nombre> <ttl> IN A <IPv4>
```

campo	descripción
<nombre>	Nombre

campo	descripción
<t1>	TTL del registro. Si se omite su valor será \$TTL.
IN	Clase del registro Internet
A	Tipo de Registro Address IPv4
<IPv4>	Dirección IPv4 asociada al nombre

## A

Ejemplo registros A para el dominio ser.smr.

```
$ORIGIN ser.smr.
$TTL 2d
....
ns IN A 192.168.1.254
nss IN A 172.10.10.254
www IN A 192.168.1.250
....
```

## AAAA

Define la IPv6 asociada a un nombre. Se utiliza en la resolución directa de un nombre. Se define con el siguiente esquema:

```
<nombre> <t1> IN AAAA <IPv6>
```

campo	descripción
<nombre>	Nombre
<t1>	TTL del registro. Si se omite su valor será \$TTL.
IN	Clase del registro Internet
AAAA	Tipo de Registro Address IPv6
<IPv6>	Dirección IPv6 asociada al nombre

## AAAA

Ejemplo registros A para el dominio ser.smr.

```
$ORIGIN ser.smr.
$TTL 2d
....
ns IN AAAA 2001:db8:a0b:12f0::10
nss IN AAAA 2001:aaa:bbb:ccc0::25
www IN AAAA 2001:db8:a0b:12f0::15
....
```

## PTR

Define el nombre asociado a una IP. Se utiliza en la resolución inversa. Se define con el siguiente esquema:

```
<IP> <ttl> IN PTR <nombre>
```

campo	descripción
<IP>	Dirección IP
<ttl>	TTL del registro. Si se omite su valor será \$TTL.
IN	Clase del registro Internet
PTR	Tipo de Registro Address IPv6
<nombre>	Nombre asociado a la IP. Debe ser siempre fqdn

### PTR

Ejemplo registros PTR para el dominio ser.smr.

```
$ORIGIN 1.168.192.in-addr.arpa.  
$TTL 2d  
....  
254 IN PTR ns.ser.smr.  
250 IN PTR www.ser.smr.  
....
```

## CNAME

Define el una alias para un nombre canónico, es decir, aquel que tiene asociado un registro A o AAA. Se utiliza en la resolución directa. Se define con el siguiente esquema:

```
<alias> <ttl> IN CNAME <nombre>
```

campo	descripción
<alias>	Nombre que se utilizará como alias
<ttl>	TTL del registro. Si se omite su valor será \$TTL.
IN	Clase del registro Internet
CNAME	Tipo de Registro Canonical Name
<nombre>	Nombre asociado a la IP. Debe ser siempre fqdn

### CNAME

Ejemplo registros CNAME para el dominio ser.smr.



```
$ORIGIN ser.smr.
$TTL 2d
....
ns IN A 192.168.1.254
nss IN A 172.10.10.254
www IN A 192.168.1.250
; alias
web IN CNAME www.ser.smr.
....
```

## MX

Define el nombre del servidor de correo que se encarga de gestionar los correos de la zona. Se define con el siguiente esquema:

```
<nombre> <ttl> IN MX <prioridad> <servidor>
```

campo	descripción
<nombre>	Nombre de la zona. Si se ha definido \$ORIGIN normalmente será @.
<ttl>	TTL del registro. Si se omite su valor será \$TTL.
IN	Clase del registro Internet
MX	Tipo de Registro Mail Exchanger
<prioridad>	Cuanto menor es el número mayor prioridad. Esto es debido a que se pueden definir varios servidores de correo para el dominio. De esta manera si el de mayor prioridad falla se puede usar el de siguiente prioridad.
<servidor>	Nombre del servidor de correo. Debe ser siempre fqdn

### MX

Ejemplo registros MX para el dominio ser.smr.

```
$ORIGIN ser.smr.
$TTL 2d
....
@ IN MX 10 mail.ser.smr.
  IN MX 20 aspmx.l.google.com.

;registro A del mail de la zona
mail IN A 192.168.1.201
; observar que aspmx.l.google.com. es externo
; a la zona y por tanto no hay que definir
; registro A
....
```

## OPCIONES

Las opciones permiten modificar le comportamiento del servidor. Algunas opciones sólo se pueden definir a nivel global ( `options` ) otras se pueden definir también a nivel de zona ( `zone` ).

# ACL

Las ACL (Access Control List) permiten definir mediante un nombre descriptivo un **grupo de direcciones IP o redes** para posteriormente utilizarlas dentro de alguna opción de configuración. Las ACL se evalúan desde la primera condición hasta que se cumpla alguna de sus condiciones. Existen varias **ACL** ya creadas **por defecto**:

ACL	descripción
none	Ninguna dirección IP
any	Cualquier dirección IP
localhost	Cualquier dirección IP configurada en el host
localnets	Cualquier dirección IP de la red o redes del host

Se pueden definir a nivel global y a nivel de zona siempre fuera de la cláusula option y/o zone. Es habitual definir las en su propio fichero de configuración, por ejemplo, `/etc/bind/named.conf.acl` para luego realizar un include en algún archivo de configuración o de zona. Su esquema es el siguiente:

```
acl "<nombre>" {  
    <IP>;           // IP aceptada  
    <IP>/<mascara>; // Red aceptada  
    "acl";         // ACL aceptada  
    !<IP>;         // IP rechazada  
    !<IP>/<mascara>; // Red rechazada  
    !"acl";        // ACL rechazada  
};
```

## ACL

Un servidor DNS quiere crear un ACL para permitir peticiones de cualquier IP menos de la red 172.20.20.0/24

```
// archivo /etc/bind/named.conf.options  
acl "query-net" {  
    !172.20.20.0/24;  
    any;  
};  
options {  
    allow-query { "query-net"; };  
};
```

# DIRECTORY

Permite definir el directorio en el que BIND buscará los archivos `db.zona` cuando no se utilicen path absolutos en la cláusula `file` de la definición de la zona. Se define a nivel global. Su esquema es el siguiente:

```
directory "directorio";
```

## directory

El servidor DNS grabará el archivo `db.ser.smr` en el directorio `/var/cache/bind`

```
// archivo /etc/bind/named.conf.options
options {
    directory "/var/cache/bind";
};
// archivo /etc/bind/named.conf.local
zone "ser.smr." {
    type master;
    file "db.ser.smr";
};
```

## FORWARDERS

Permite definir una lista de servidores DNS a los que reenviar las peticiones de resolución de nombres cuando no se pueden resolver en las zonas definidas en el propio servidor. En este caso, el servidor se comportará como un servidor DNS recursivo caché y responderá de manera no autoritativa para dichas peticiones. Se define a nivel global. Su esquema es el siguiente:

```
fowardsers { <IP-forward>; <IP-forward>; };
```

### DNS forwarder

Un servidor DNS con IP 192.168.1.254 define la zona ser.smr. , el resto de peticiones las reenvía al servidor 1.1.1.1.

```
// archivo /etc/bind/named.conf.options
options {
    fowardsers { 1.1.1.1; };
};
```

## LISTEN-ON

Permite definir las interfaces IPv4, IPv6 y puertos por los que se servirán las consultas DNS. Se puede usar **any** o **none** para indicar todas o ninguna interfaz. Se definen a nivel global. Su esquema es el siguiente:

```
listen-on [<port>] { <IPv4>; <IPv4>; };
listen-on-v6 [<port>] { <IPv6>; <IPv6>; };
```

### listen-on

Un servidor DNS con dos interfaces de red de direcciones 192.168.1.254 y 172.18.1.1.1 quiere escuchar peticiones DNS solo para la interfaz localhost y la interfaz de IP 192.168.1.254

```
// archivo /etc/bind/named.conf.options
options {
    listen-on {127.0.0.1; 192.168.1.254; };
    listen-on-v6 {none; };
};
```

# RECURSION

Configura al servidor para realizar resoluciones de nombres recursivas. Por defecto, es recursivo. Se define a nivel global. Su esquema es el siguiente:

```
recursion <yes|no>;
```

## ALLOW-RECURSION

Especifica que equipos podrán realizar consultas recursivas al servidor. Se define a nivel global. Por defecto, por motivos de seguridad, su valor es `{ localnets; localhost; }` por lo que solamente se permite recursión al propio equipo y a su red a no ser que se defina explícitamente. Su esquema es el siguiente:

```
allow-recursion { <IP>; <IP>/< mascara>; acl; };
```

### allow-recursion

Un servidor DNS quiere ser recursivo solo para las redes 172.16.16.0/24 y 192.168.1.0/24 además de para su propia red y él mismo.

```
// archivo /etc/bind/named.conf.options
acl "recursive-net" {
    172.16.16.0/24;
    192.168.1.0/24;
    localhost;
    localnets;
};
options {
    recursion yes;
    allow-recursion { "recursive-net"; };
};
```

## ALLOW-QUERY-CACHE

Especifica que equipos podrán realizar consultas a la cache. Se define a nivel global. Por defecto, por motivos de seguridad, su valor es `{ localnets; localhost; }` Si se define allow-recursion entonces hereda el valor definido en dicha opción, por ese motivo, suele ser habitual definir solo allow-recursion y no esta clausula. De esta forma se evitan los ataques de envenamiento de cache o analicen el historial de tráfico DNS del servidor. Su esquema es el siguiente:

```
allow-query-cache { <IP>; <IP>/< mascara>; acl; };
```

## CACHE

Existen varias clausulas para controlar el comportamiento de la cache, entre ellas: `max-cache-size`, `max-cache-ttl` y `max-ncache-ttl`.

La clausula `max-cache-size` especifica el tamaño máximo de la memoria cache en RAM.

```
max-cache-size ( default | unlimited | <sizeval> | <percentage> );
```

Valor	Descripción
default	Depende del valor de <code>recursion</code> . Si <code>recursion yes</code> es el 90% del tamaño de la memoria del equipo. Si <code>recursion no</code> entonces es 2 MB.
unlimited	Hasta acabar con los recursos de memoria del servidor
<sizeval>	Valor en <code>k</code> iloBytes, <code>M</code> egaBytes, <code>G</code> igaBytes.
<percentage>	Valor en % sobre el total de la memoria

La clausula `max-cache-ttl` especifica el tiempo máximo que un registro permanece en la cache. Se pueden especificar con w,d,h,m,s como \$TTL. El valor por defecto es 1w y no se puede poner a 0.

```
max-cache-ttl <duration>;
```

La clausula `max-ncache-ttl` especifica el tiempo máximo que un registro no resuelto (NXDOMAIN) permanece en la cache. Se pueden especificar con w,d,h,m,s como \$TTL. El valor por defecto es 3h y su valor máximo es 7d;

```
max-ncache-ttl <duration>;
```



## Configuración cache

Un servidor DNS recursivo quiere restringir el tamaño de su memoria cache a 512 MB, que el tiempo máximo de los registros resueltos sea de 3 días y de los no resueltos de 1 hora.

```
// archivo /etc/bind/named.conf.options
options {
    max-cache-size 512M;
    max-cache-ttl 3d;
    max-ncache-ttl 1h;
};
```

## ALLOW-QUERY

Especifica que equipos podrán realizar consultas al servidor. Se define a nivel global o de zona. Por defecto, su valor es `{ any; }` por lo se permite la consulta a cualquier equipo. Su esquema es el siguiente:

```
allow-query { <IP>; <IP>/< mascara>; acl; };
```



## allow-recursion

Un servidor DNS quiere permitir consultas solo a las redes 172.16.16.0/24 y 192.168.1.0/24 además de su propia red y él mismo.

```
// archivo /etc/bind/named.conf.options
acl "query-net" {
    172.16.16.0/24;
    192.168.1.0/24;
    localhost;
    localnets;
};
options {
    allow-query { "query-net"; };
};
```

## DELEGACIÓN DE DOMINIOS

La delegación de dominios es el mecanismo de DNS que permite que la autoridad sobre un dominio o subdominio pase a otros servidores DNS sin perder la jerarquía sobre dicho dominio. La delegación de dominios es la piedra de toque en la que se basa todo el sistema de distribución de la base de datos de DNS.

La delegación de dominio se realiza fundamentalmente mediante la definición de los registros NS que permiten alcanzar dichos dominios. Veamoslo con un ejemplo.

### Delegación de dominios

Un servidor DNS de nombre ns.ser.smr e IP 192.168.1.254 define el dominio ser.smr y delega los subdominio ga y gb en los servidores ns.ga.ser.smr y ns.gb.ser.smr que tienen IP 192.168.2.254 y 192.168.3.254 respectivamente.

```
$ORIGIN ser.smr.
$TTL 1d
@ IN SOA ns.ser.smr. admin.ser.smr. (
    2025121502 ; serial
    1d ; refresh
    3h ; retry
    1w ; expire
    1h ; nxdomain
)

@ IN NS ns.ser.smr.
ga IN NS ns.ga.ser.smr. ;delegacion
gb IN NS ns.gb.ser.smr. ;delegacion

ns IN A 192.168.1.254
ns.ga IN A 192.168.2.254 ;delegacion
ns.gb IN A 192.168.3.254 ;delegacion

www IN A 192.168.1.250
ftp IN A 192.168.1.249
```

## TRANSFERENCIAS DE ZONAS

Las transferencias de zonas es el mecanismo que utilizan las zonas master y slave para transferirse los registros de recursos. Básicamente el mecanismo de transferencias de zona es el siguiente:

Cuando un administrador modifica una zona master aumenta el `serial` definido en el registro SOA de la zona. El servidor que contiene la zona slave intenta sincronizarse periódicamente, según el tiempo definido en `refresh`,

con la zona master. Si el `serial` de la zona master es superior al de la zona slave se producira la transferencia de zona y por tanto la sincronización de la zona.

Existen dos tipos de transferencia de zonas:

- **AXFR** (Asynchronous Full Transfer)

Se produce cuando la zona slave realiza una petición de sincronización con la zona master. La zona master envía todos los registros que definen la zona. Este tipo de transferencia se produce siempre la primera vez que se sincronizan las zonas master y slave y tambien cuando no se soporta el otro tipo de transferencia. El problema es que consume mucho ancho de banda y es algo lento ya que envía todos los registros de la zona.

- **IXFR** (Incremental Zone Transfer)

Se produce cuando la zona slave realiza una petición de sincronización con la zona master. La zona slave manda un número de serie indicando la ultima sincronización realizada, entonces la zona master envía sólo los registros que definen la zona y que se modificaron posteriormente a dicho número de serie. Las transferencias consumen menos ancho de banda y son más rápidas.

## ALLOW-TRANSFER

Es evidente que la seguridad de la base de datos de una zona se puede ver comprometida si algún "hacker" define un servidor DNS con una zona esclava apuntando a la dirección del servidor DNS master. Para evitar que cualquier servidor pueda apuntar a nuestras zonas se utiliza la clausula `allow-transfer`.

Pasos:

- 1.Servidor master. En la configuración global "bloqueamos" todas las transferencias.

```
//archivo named.conf.options
options {
...
    allow-transfer { none; };
...
};
```

- 2.Servidor master. En la configuración de la zona master "permitimos" las transferencias para los servidores secundarios que consideremos seguros.

```
//archivo named.conf.local
...
//zona master
zone "<dominio.>" {
...
    allow-transfer { IP-slave; IP-slave; };
...
};
```



### allow-transfer

Un servidor DNS define la zona master ser.smr y quiere permitir solo las transferencias de zona para los servidores esclavos con dirección 192.168.1.20 y 172.16.10.10:

```
//archivo named.conf.options
options {
    ...
    allow-transfer { none; };
    ...
};

//archivo named.conf.local
...
zone "ser.smr." {
    type master;
    file "/etc/bind/db.ser.smr";
    allow-transfer { 192.168.1.20; 172.16.10.10; };
};
...
```

## CLAVES TSIG

Aparentemente la protección mediante IP podría ser suficiente. Sin embargo, dista mucho de la realidad, cualquier "hacker" podría averiguar IPs en la red simplemente analizando el tráfico de las peticiones DNS el cual no es cifrado.

Un paso más en la seguridad de las transferencias entre zonas master y slaves es el uso de una clave simétrica para permitir las transferencias. Las claves **TSIG** (Transaction Signature) son claves simétricas compartidas por los servidores DNS, normalmente uno master y otro slave. Se usan para firmar criptográficamente los mensajes DNS y permite verificar:

- Autenticidad. El mensaje proviene de un servidor autorizado.
- Integridad. El mensaje no ha sido modificado.
- Fiabilidad. La comunicación es fiable.

Pasos:

- 1.Servidor master. Crear clave.

```
tsig-keygen -a hmac-sha256 clave > /etc/bind/tsig-clave.key
chmod 640 /etc/bind/tsig-clave.key
chown root:bin /etc/bind/tsig-clave.key
```

tsig-keygen habrá creado con el algoritmo hmac-sha256 una key de nombre clave que define una contraseña o secret. El archivo .key tiene la siguiente forma.

```
//archivo tsig-clave.key
key "clave" {
    algorithm hmac-sha256;
    secret "mXJ7p7b9zG+YxLQ8Q0dKxZQpXxK9WZP3R9uGZJ0sTn4=";
};
```

- 2.Servidor master. Incluir en el archivo de zonas la clave y asignarla a la zona que se desea proteger.



```
//archivo named.conf.local
...
include "/etc/bind/tsig-clave.key"
...
zone "<dominio.> {
    type master;
    file /etc/bind/db.dominio";
    allow-transfer { key clave; };
};
```

- 3.Servidores slave. Copiar el archivo .key a los servidores DNS slave que se desean puedan hacer transferencias de zonas.

```
cp tsig-clave.key /etc/bind/tsig-clave.key
```

- 4.Servidores slave. Incluir en el archivo de zonas la clave y asignarla a las zonas en las que se quiere realizar transferencias.

```
//archivo named.conf.local
...
include "/etc/bind/tsig-clave.key"
...
zone "<dominio.> {
    type slave;
    file /var/lib/bind/db.dominio";
    masters { <IP-master> key clave; };
};
```

## TSIG

Un servidor DNS con IP 192.168.1.254 define la zona master ser.smr y quiere permitir las transferencias de zona solo para los servidores esclavos que tengan la clave TSIG.

```
#1.Servidor master. Generar TSIG
tsig-keygen -a hmac-sha256 clave > /etc/bind/tsig-clave.key
chmod 640 /etc/bind/tsig-clave.key
chown root:bin /etc/bind/tsig-clave.key

#2.Servidor master. Incluir TSIG en la zona
//archivo named.conf.local
...
include "/etc/bind/tsig-clave.key"
...
zone "ser.smr." {
    type master;
    file /etc/bind/db.ser.smr";
    allow-transfer { key clave; };
};

#3.Servidores slave. Copiar tsig-clave.key
cp tsig-clave.key /etc/bind/tsig-clave.key

#4.Servidores slave. Incluir TSIG en la zona
//archivo named.conf.local
...
include "/etc/bind/tsig-clave.key"
...
zone "ser.smr." {
    type slave;
    file /var/lib/bind/db.ser.smr";
    masters { 192.168.1.254 key clave; };
};
```

## NOTIFY

Los servidores DNS BIND permiten no solo que el servidor slave inicie la sincronización con el servidor master, sino que sea el propio servidor master quien envíe notificaciones al servidor slave cuando haya realizado modificaciones en la zona para de este modo iniciar el proceso de sincronización. Se realiza mediante las cláusulas `notify`, `also-notify` y `allow-notify`

En la **zona master** usamos.

```
notify <yes | no | explicit>
```

valor	descripción
yes	Se envía notificación a todos los servidores esclavos definidos en los registros NS de la zona. Es el valor por defecto.
no	No se envía ninguna notificación
explicit	Se envía notificación sólo a los servidores esclavos definidos en la cláusula <code>also-notify</code>

```
also-notify { <IP-slave>; <IP-slave>; | <IP-slave> key <clave>; }
```

Lista de servidores slaves a los que se les pasa notificación, también se puede incluir una clave TSIG.

En la **zona slave**, usamos.

```
allow-notify { <IP-master>; <IP-master>; | key <clave>; }
```

Por defecto, si no se indica allow-notify es igual a la lista de masters definidos en la zona slave.

Por tanto, en BIND, por defecto se realizan notificaciones de las zonas master ( `notify yes` ) a las zonas slave definidas en los registros NS de la zona. Estas zonas slave aceptan notificaciones de los servidores master definidos ( `allow-notify = { masters; }` ).

## BALANCEO DE CARGA

En BIND podemos, por ejemplo, definir varios registros que apuntan a la misma dirección ( `A` ) o varios registros que definen un mismo dominio ( `ns` ). Por ejemplo:

```
$ORIGIN ser.smr.
$TTL 2d

@ IN SOA ns.ser.smr. admin.ser.smr. (
    2025121502    ; serial
    1d            ; refresh
    3h            ; retry
    1w            ; expire
    1h            ; nxdomain
)

@ IN NS  ns.ser.smr.
  IN NS  ns2.ser.smr.
  IN NS  ns3.ser.smr.

ns  IN A  192.168.1.254
ns2 IN A  192.168.1.253
ns3 IN A  192.168.1.252
www IN A  192.168.1.100
    IN A  192.168.1.101
    IN A  192.168.1.102
```

Por ejemplo, una consulta del registro `www` provocaría la contestación de un conjunto de registros de recursos ( `RRSet` ), en concreto 3 registros. Es muy importante el orden en que estos registros aparecen en la sección de respuesta del mensaje DNS ya que el cliente que ha realizado la consulta intentará la conexión en el orden propuesto. Variando el orden de la respuesta BIND puede **"balancear la carga"** sobre el servicio `www`, es decir, puede hacer que el orden varíe mejorando de esa manera la carga de trabajo de cada servidor `www`.

El balanceo de carga se puede configurar en la clausula `rrset-order` de las opciones globales de BIND.

```
rrset-order {
    [class <class_name>] [type <type_name>] [name "<domain_name>"] order <ordering>;
    [class <class_name>] [type <type_name>] [name "<domain_name>"] order <ordering>;
    [class <class_name>] [type <type_name>] [name "<domain_name>"] order <ordering>;
}
```

Valor	Descripción
<code>class</code>	Clase del registro. Si no se define es ANY
<code>type</code>	Tipo del registro. Si no se define es ANY
<code>nombre</code>	Nombre del registro. Si no se define es *
<code>order</code>	<code>fixed</code> según estan escritos en la zona <code>random</code> aleatorio

Valor	Descripción
	cyclic round-robin
	none indeterminado según la base de datos

Si no se configura `rrset-order`, el valor por defecto es `random` para todos los RRSets que se devuelvan. Si se configura `rrset-order` se aplican las reglas secuencialmente la primera que coincida se aplica.

### rrset-order

En un servidor DNS se quiere que los registros de direcciones correspondientes al nombre `www.ser.smr.` se devuelvan en orden round-robin y el resto de registros en orden random.

```
//archivo /etc/bind/named.conf.options
options {
    rrset-order {
        type A name www.ser.smr. order cyclic;
        order random;
    };
};
```

Para comprobar el orden en que nos devuelve la respuestas podemos usar la utilidad `dig`.

### dig y order

Para el servidor del ejemplo anterior se podrían realizar las siguientes consultas sobre `www` para comprobar la respuesta round-robin.

```
dig @127.0.0.1 www.ser.smr. +short
www 192.168.1.100
www 192.168.1.101
www 192.168.1.102
dig @127.0.0.1 www.ser.smr. +short
www 192.168.1.101
www 192.168.1.102
www 192.168.1.100
dig @127.0.0.1 www.ser.smr. +short
www 192.168.1.102
www 192.168.1.100
www 192.168.1.101
```

## DNSSEC

BIND permite el uso del protocolo DNSSEC para autenticar y mantener la integridad de los mensajes DNS.

La opción global `dnssec-validation` activa o desactiva el uso de DNSSEC y la verificación de firmas digitales en las consultas DNS. El objetivo es garantizar que los datos recibidos de la consulta no hayan sido manipulados por ningún atacante.

```
//archivo named.conf.options
options {
    ...
    dnssec-validation <yes | no | auto>;
    ...
};
```

valor	descripción
auto	El servidor utiliza DNSSEC con las <b>trust anchors</b> (claves de confianza) integradas en BIND para validar la zona raíz. La primera vez que conecta con los servidores raíz lo hace con la clave almacenada en <code>/etc/bind/bind.keys</code> , posteriormente la clave es actualizada mediante el módulo managed-keys en el archivo <code>/var/cache/bind/managed-keys.bind</code>
yes	El servidor utiliza DNSSEC pero requiere que el administrador configure manualmente las <b>trust anchors</b> (claves de confianza) para validar la zona raíz
no	El servidor desactiva DNSSEC y realiza consultas no seguras

**Nota:** En una red configurada sólo con IPv4 es necesario arrancar el servicio en modo IPv4 para que funcione dnssec.

**Nota:** Actualizar las claves de confianza integradas.

```
systemctl start named ; servidor en funcionamiento
rndc managed-keys refresh ; actualiza claves
rndc managed-keys status ; comprueba claves
rndc flush ; limpia cache
```

**Nota:** Forzar la carga de las claves de confianza.

```
systemctl stop named
rm -f /var/cache/bind/managed-keys.bind*
systemctl start named
```

Para comprobar el funcionamiento de DNSSEC se pueden realizar consultas mediante el comando `dig` o el comando `delv` diseñado por BIND para comprobar exclusivamente el funcionamiento de DNSSEC.

### Consulta DNSSEC

```
dig @127.0.0.1 google.com +dnssec
delv @127.0.0.1 google.com
```

## DDNS

DDNS (Dynamic DNS) permite realizar actualizaciones de los registros de recursos del servidor. BIND permite controlar DDNS mediante la clausula **allow-update** que se puede definir tanto a nivel global ( `options` ) como a nivel de zona ( `zone` ). Por defecto, su valor es `{ none; }` por lo no se permite la actualizacion a ningún equipo.

```
allow-update { <IP>; <IP>/< mascara>; acl; | key "clave"; };
```

Como se observa en la definición se puede usar una lista de IPs o bien una clave TSIG, método mucho más seguro.

### allow-update

Un servidor DNS quiere permitir actualizaciones de registros solo desde el equipo 192.168.1.250 y localhost.

```
// archivo /etc/bind/named.conf.options
acl "update-net" {
    192.168.1.250;
    localhost;
};
options {
    allow-update { "update-net"; };
};
```

## allow-update

Un servidor DNS quiere permitir actualizaciones de registros solo a los equipos que tengan la clave TSIG para la zona ser.smr.

```
// archivo /etc/bind/named.conf.local
include "/etc/bind/ddns.key"
zone "ser.smr." {
    type master;
    // el directorio debe tener permisos de escritura
    file "/etc/bind/db.ser.smr";
    allow-update { key "ddns"; }
}
```

## FICHEROS DE LOG

El servidor DNS BIND envía mensajes de log para indicar multiples situaciones, desde simples informaciones a notificaciones de error.

Hay 3 maneras de configurar y acceder a estos mensajes.

### RSYSLOGD

El daemon `rsyslogd` gestiona los mensajes de log mediante el protocolo SYSLOG y por defecto sus mensajes acaban en el archivo `/etc/log/syslog` donde se mezclan mensajes de diferentes servicios y aplicaciones. Para filtrar los mensajes del servicio DNS podremos ejecutar.

```
cat /var/log/syslog | grep named | more

fgrep named /var/log/syslog
```

### JOURNALD

El daemon `journald` se gestionan los mensajes de log enviandolos a un archivo binario que se puede consultar mediante la utilidad `journalctl`. Para filtrar los mensajes del servicio DNS podremos ejecutar.

```
journalctl -u named.service -xe
```

# CLAUSULA LOGGING

BIND9 permite mediante la clausula `logging` personalizar la salida de sus mensajes de log. Esta clausula se puede especificar por ejemplo en el archivo `/etc/bind/named.conf.options`. El sistema de logging se basa en los conceptos de canal y categoria.

- Canal  
Define donde se enviarán los mensajes de log. Puede ser un fichero, rsyslogd, la salida estandard, null, etc...
- Categoria  
Se refiere a categorias de mensajes de log. Por ejemplo: default, network, security, database,...La que más interesa es default que representa a todas las categorias.

El formato general de `logging` es:

```
logging {  
    category <categoria> { <canal>; };  
    channel <canal> {  
        <proceso_salida> <salida> [<opciones>];  
        [opciones print];  
    }  
}
```

## Logging

Se hará log de todos los mensajes (default) sobre un fichero de nombre `/var/lib/bind/bind.log` del que se guardarán hasta 3 versiones con un tamaño máximo de 100K. Además del mensaje se imprimirá en el archivo la hora, la gravedad del mensaje y su categoria.

```
logging {  
    category default { "canal-log"; };  
    channel "canal-log" {  
        file "/var/lib/bind/bind.log" versions 3 size 100k;  
        print-time yes;  
        print-severity yes;  
        print-category yes;  
    };  
};
```