Configuración DNS – Bind

VIII Jornadas de SL – GPUL 2008

Juan José Iglesias González

jiglesias@denodo.com

denodo technologies

Enterprise Data Mashups

Configuración Bind

Índice

- Internet y DNS
- Funcionamiento DNS
- Bind
- Configuración básica Bind
- Bind avanzado

Configuración Bind

- Fichero HOSTS.TXT

```
www.google.com.   66.249.93.99
a.l.google.com.   209.85.139.9
b.l.google.com.   64.233.179.9
...
```

- Mantenido por SRI Network Information Center (the NIC)

Problemas:

- Tráfico y carga
- Colisiones de nombres
- Consistencia

El sistema no escalaba

Configuración Bind

Internet y DNS: Alternativa DNS

Paul Mockapetris 1984: RFC 882 y 883 (sustituidos por RFC 1034 y 1035)

Idea clave: BD distribuida

Estructura jerárquica.

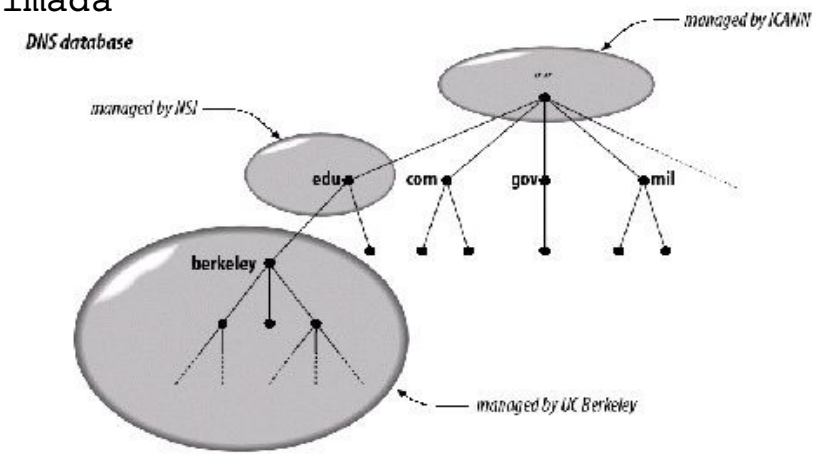
Cada organización gestiona su espacio de nombres a través de su propio servidor de nombres (NS).

Delegar adeministración de subdominios a NS más “próximos”.

Devolver la respuesta más “aproximada”

Cachés para evitar búsquedas.

El sistema si escala



Configuración Bind

Funcionamiento DNS: Vocabulario

Árbol de nombres de dominio DNS.
¡No confundir con árbol NIS o AD!

Dominio y subdominio: subárbol. TLD: com, org, ..., es, us, ..., info, biz, ...

Zonas: (hay delegación)

Etiquetas y nombres de host

Resource Records

clases: Internet y algunas raras (ChaosNet, Hesiod, a olvidar...)

tipos:

SOA	CNAME
NS	TXT
MX	HINFO
A	
PTR	

Configuración Bind

Funcionamiento DNS: Agentes DNS

Primary Master Nameserver ("master")
lee la información desde el fichero de la zona.

Secondary Master Nameserver ("slave")
lee la información desde otro NS (primary o no)

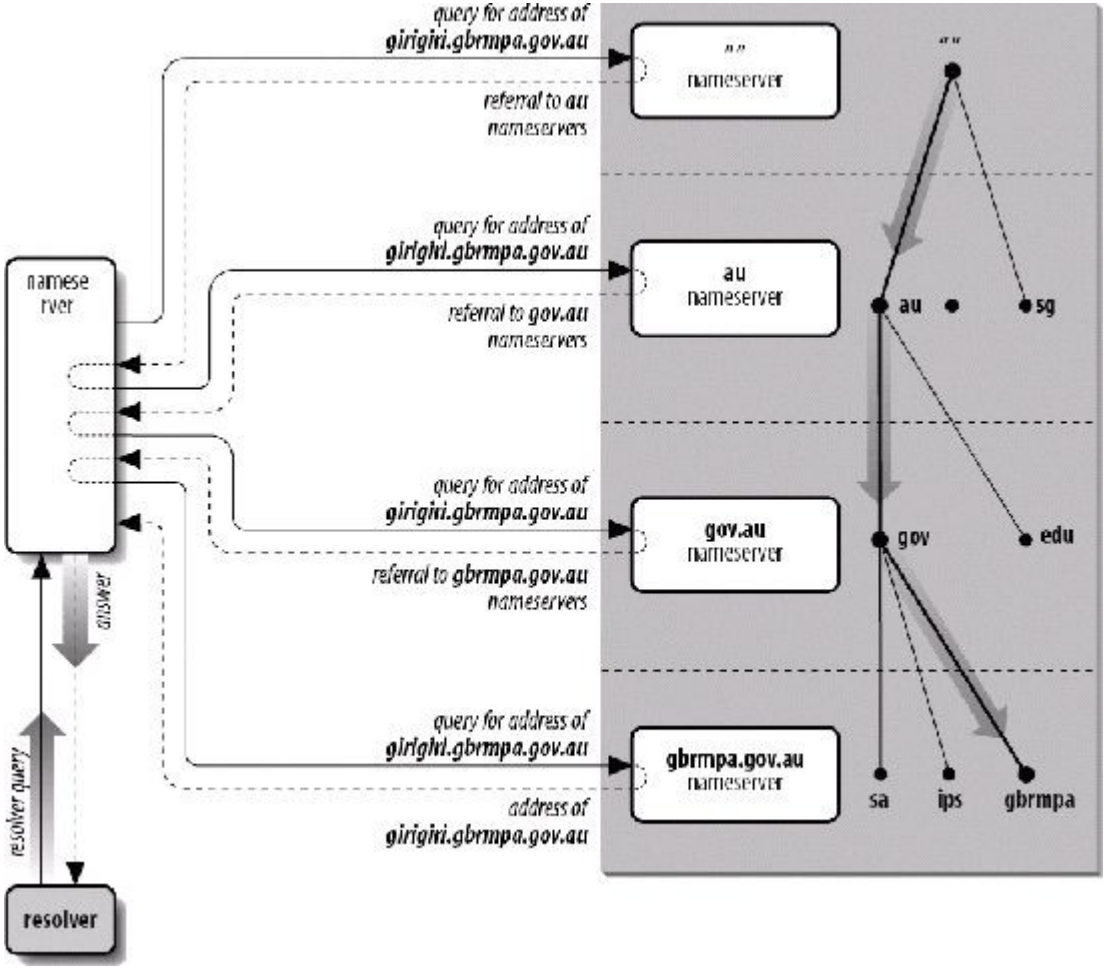
Cache Nameserver
responde a las consultas de los "resolvers"

Resolvers
recibe consultas del software de cliente

biblioteca a linkar con programa cliente (unix/linux)
programa independiente (windows)
puede tener cachés individuales
incluso realizar su propia "resolución"

Configuración Bind

Funcionamiento DNS: Resolución



Configuración Bind

Funcionamiento DNS: Tipos de consultas, herramienta dig

Recursivas

devuelve respuesta exacta o error

- devuelve respuesta porque está en sus zonas
- devuelve respuesta en cache
- reenvía la consulta recursiva (forward).
- resuelve realizando múltiples iterativas.

```
dig @ns.example.com dominio.tld A
```

Iterativas

puede devolver una respuesta aproximada.

- respuesta exacta si está en caché o sus zonas
- referral a un subdominio (delegación)
- referral a un dominio padre (no sabe nada)

```
dig @ns.example.com dominio.tld +norec NS
```

Configuración Bind

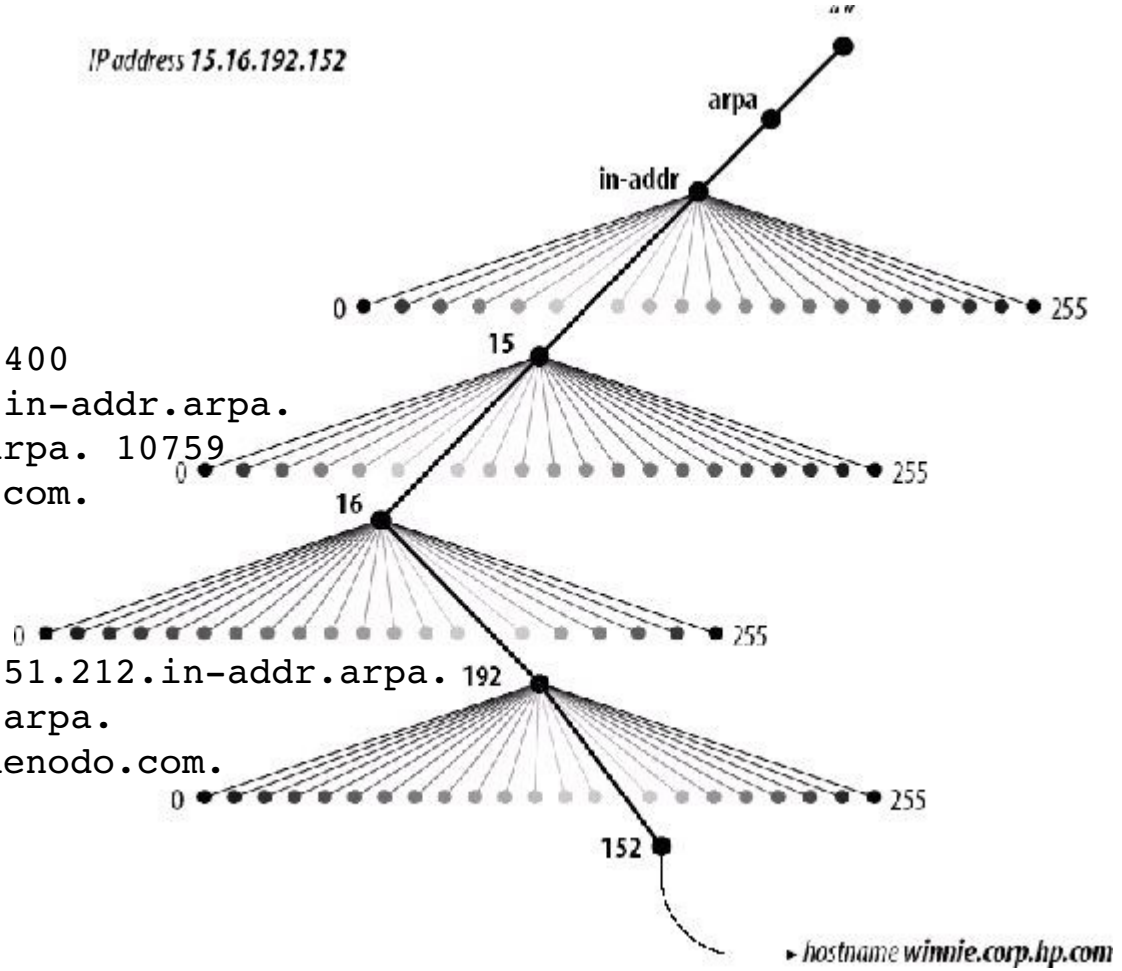
Funcionamiento DNS: Resolución inversa

RFC 1912:
un PTR debe coincidir con un A

Espacios de direcciones CIDR

```
dig -x 212.51.33.56
;; ANSWER SECTION:
56.33.51.212.in-addr.arpa. 86400
IN CNAME 56.denodo.33.51.212.in-addr.arpa.
56.denodo.33.51.212.in-addr.arpa. 10759
IN PTR cor056.housing.denodo.com.

dig -x 212.51.61.198
198.61.51.212.in-addr.arpa.
86400 IN CNAME 198.192/26.61.51.212.in-addr.arpa.
198.192/26.61.51.212.in-addr.arpa.
10800 IN PTR cor198.network.denodo.com.
```



Configuración Bind

Paul Mockapetris implementó DNS con JEEVES.

Bind: Berkeley Internet Name Domain

Kevin Dunlap para Berkeley's 4.3 BSD Unix.

Mantenido por Internet System Consortium.
http://www.isc.org/sw/bind/

Estándar "de facto" en Unix y Linux. Portado a Windows, ...

Alternativas:

DJBDNS (D.J. Bernstein)

Windows Server DNS

Configuración Bind

Configuración básica BIND: zona ejemplo

```
127.0.0.1       localhost

192.168.1.101   cronos.billenet.com
192.168.1.101   cronos-1.billenet.com

192.168.201.1   cronos-201.billenet.com
192.168.201.1   cronos.billenet.com
192.168.201.10  hercules.billenet.com
192.168.201.11  ajax.billenet.com
192.168.201.13  helena.billenet.com
192.168.201.15  pandora.billenet.com

www             hercules.billenet.com
mail            ajax.billenet.com
smtp            ajax.billenet.com
pop             ajax.billenet.com
imap            ajax.billenet.com
shared          helena.billenet.com
```

Configuración Bind

Configuración básica BIND: zona bind (db.com.billenet.2008041400)

```
$TTL    3h
billenet.com. IN SOA hercules.billenet.com. jiglesias.billenet.com. (
        2008041400      ; serial
        3h              ; refresh after 3 hours
        1h              ; retry after 1 hour
        1w              ; expire after 1 week
        1h              ; negative caching TTL
billenet.com.    IN NS hercules.billenet.com.
billenet.com.    IN NS ajax.billenet.com.
billenet.com.    IN MX 10 192.168.201.11
billenet.com.    IN A 192.168.1.101

cronos.billenet.com.      IN A 192.168.1.101
cronos-1.billenet.com.    IN A 192.168.1.101

cronos.billenet.com.      IN A 192.168.201.1
cronos-201.billenet.com.  IN A 192.168.201.1
hercules.billenet.com.    IN A 192.168.201.10
ajax.billenet.com.        IN A 192.168.201.11
helena.billenet.com.      IN A 192.168.201.13

www.billenet.com.         IN CNAME billenet.com.
mail.billenet.com.        IN CNAME ajax.billenet.com.
```

Configuración Bind

Configuración básica BIND: zona bind (db.com.billenet.2008041400)

```
; EJEMPLO DE DELEGACIÓN
; Glue records
ad.billenet.com. 86400 IN NS helena.billenet.com
helena.billenet.com. IN A 192.168.201.13
```

Configuración Bind

Configuración básica BIND: zona bind (db.192.168.201.0.2008041400)

```
$TTL 3h
201.168.192.in-addr.arpa. IN SOA hercules.billenet.com.
jiglesias.billenet.com. (2008041400 3h 1h  1w 1h)

201.168.192.in-addr.arpa. IN NS hercules.billenet.com.
201.168.192.in-addr.arpa. IN NS ajax.billenet.com.

10.201.168.192.in-addr.arpa. IN PTR hercules.billenet.com.
11.201.168.192.in-addr.arpa. IN PTR ajax.billenet.com.
13.201.168.192.in-addr.arpa. IN PTR helena.billenet.com.
```

Configuración Bind

Configuración básica BIND: zona bind (db.127.0.0.0.2008041400)

```
$TTL 3h
0.0.127.in-addr.arpa. IN SOA hercules.billenet.com.
jiglesias.billenet.com. (1 3h 1h 1w 1h)

0.0.127.in-addr.arpa.  IN NS  hercules.billenet.com.
0.0.127.in-addr.arpa.  IN NS  ajax.billenet.com.

1.0.0.127.in-addr.arpa.  IN PTR localhost.
```

Configuración Bind

Configuración básica BIND: zona raiz (db.cache)

```
.                       3600000  IN  NS    A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET.     3600000      A     198.41.0.4
A.ROOT-SERVERS.NET.     3600000      AAAA  2001:503:BA3E::2:30
;
; formerly NS1.ISI.EDU
;
.                       3600000      NS    B.ROOT-SERVERS.NET.
B.ROOT-SERVERS.NET.     3600000      A     192.228.79.201
;
; formerly C.PSI.NET
;
.                       3600000      NS    C.ROOT-SERVERS.NET.
C.ROOT-SERVERS.NET.     3600000      A     192.33.4.12
;
; formerly TERP.UMD.EDU
;
.                       3600000      NS    D.ROOT-SERVERS.NET.
D.ROOT-SERVERS.NET.     3600000      A     128.8.10.90
;
```

Configuración Bind

Configuración básica BIND: fichero de configuración bind cache (named.conf)

```
options {
        directory “/var/named”; };

zone "0.0.127.in-addr.arpa" in {
        type master;
        file "db.127.0.0"; };

zone "." in {
        type hint;
        file "db.cache"; };
```

Configuración Bind

Configuración básica BIND: fichero de configuración bind (named.conf)

```
options {
        directory “/var/named”; };

zone “billenet.com” {
        type master;
        file “db.billenet.com”; };

zone “201.168.192.in-addr.arpa” in {
        type master;
        file “db.192.168.201”; };

zone "0.0.127.in-addr.arpa" in {
       type master;
       file "db.127.0.0"; };

zone "." in {
       type hint;
       file "db.cache"; };
```

Configuración Bind

Configuración básica BIND: abreviaturas

El dominio de la zona se añade automáticamente:

```
ajax.billenet.com. IN A 192.168.201.11
          ajax IN A 192.168.201.11
11.201.168.192.in-addr.arpa. IN PTR ajax.billenet.com
          11 IN PTR ajax.billenet.com.
```

Notación @ (compartir SOA entre zonas)

```
@ IN SOA hercules.billenet.com. jiglesias.billenet.com. (...
```

Repetir último registro

```
@ IN SOA hercules.billenet.com. jiglesias.billenet.com. (...
          IN NS hercules.billenet.com.
          IN NS ajax.billenet.com.
          IN MX 10 ajax.billenet.com.
          IN A 192.168.1.101
```

$INCLUDE $ORIGIN

$GENERATE 192-255 $.61.51.212.in-addr.arpa IN NS ns.foo.com

Utilidades BIND: named-checkconf, named-checkzone

Configuración Bind

Configuración básica BIND: NS slave

```
options {
        directory “/var/named”; };

zone “billenet.com” {
        type slave;
        file “bak.billenet.com”;
        masters { 192.168.201.10; }; };

zone “201.168.192.in-addr.arpa” in {
        type slave;
        file “back.192.168.201”;
        masters { 192.168.201.10; }; };

zone "0.0.127.in-addr.arpa" in {
       type master;
       file "db.127.0.0"; };

zone "." in {
       type hint;
       file "db.cache"; };
```

Configuración Bind

Configuración básica BIND: resolver

```
/etc/resolv.conf
search billenet.com ad.billenet.com
nameserver 192.168.201.10
nameserver 192.168.201.11

                domain billenet.com
                options
                        sortlist 192.168.1.0/255.255.255.0
                        ndots: 2
                        attempts: 4
                        timeout: 2
                        rotate

/etc/nsswitch.conf

                hosts: dns files
```

Resolver windows

```
                net stop dnscache
                ipconfig /displaydns
                ipconfig /flushdns
```

Configuración Bind

Temas avanzados BIND

Gestión RNDC (reload, refresh zone, retransfer zone, freeze zone, ...) y estadísticas

Email y DNS (Registros SPD, correspondencia PTR-A)

```
oreilly.com. IN TXT "v=spf1 +a:smtp1.oreilly.com +a:smtp2.oreilly.com -all"
```

Gestión Logs

```
logging { channel nombre {
          syslog daemon;      file "/tmp/nombre-log";
          severity info; };

          category xfer-out { nombre; }; };
```

Address Match List

```
acl "clients" { 192.168.201.0/24; };
predefinidas: none any localhost localnets
```

Vistas

```
view "internal" {
          match-clients {"clientes";}

          ; zonas
};
```

Configuración Bind

Temas avanzados BIND

Opciones para ajustar rendimiento

```
rrset-order { type A name "*.sample.edu" order cyclic; };

sort-list { 192.168.201/24; { 192.168.201/24; }; };
```

Opciones para control

```
black-hole { 10/8; 172.16/12; 192.168/16; };
listen on 5353 { IP; };
transfer-source IP;
```

Opciones para seguridad

```
key host.sample.com { algorithm hmac-md5; secret "abcd..."; };
server 192.168.201.10 { keys { host.sample.com.; }; };
zone sample.com {    type slave;
                     master { 192.168.201.10 key host.sample.com;};

master:
zone sample.com {    type master;
                     file "/var/named/db...";
                     allow-transfer { key host.sample.com; };
```

DNSSEC

IPV6

Configuración Bind

Bibliografía

- **DNS & Bind.** Paul Albitz; Cricket Liulbitz. O'Reilly 2006 (5Ed)
- **DNS & Bind Cookbook.** Cricket Liu. O'Reilly 2002.
- **The Concise Guide to DNS and Bind.** Nicolai Langfeldt. Que 2000.
- **Web Bind**: http://www.isc.org/index.pl?/sw/bind/index.php
- **RFC 1035** (Standard: STD 13) updated by RFCs 1101, 1122, 1183, 1706, 1876, 1982, 1995, 1996, 2136, 2137, 2181, 2308, 2535, 2782, 2845, 3425 and RFC 3658; obsoletes RFCs 882, 883 and 973: Domain Names--Implementation and Specification by P. Mockapetris
- **RFC 1034** (Standard: STD 13) updated by RFCs 1101, 1122, 1183, 1706, 1876, 1982, 2181, 2308 and 2535; obsoletes RFCs 882, 883 and 973 : Domain Names--Concepts and Facilities by P. Mockapetris Reference guide, covers just about everything.
- **RFC 1912** (Informational) obsoletes RFC 1537 Common DNS Operational and Configuration Errors by D. Barr Errors and common practice in operation of servers and format of data.
- **Listas correo Bind**: http://www.isc.org/index.pl?/sw/bind/bind-lists.php