Servidor DNS

Índex

Cicle formatiu: CFGM Sistemes Microinformàtics i Xarxes (SMX) / CFGS Administració de sistemes informàtics en xarxa (ASIX)

Mòdul: 0227 - Serveis de xarxa / 0375 - Serveis de xarxa i Internet

Sistema operatiu: Ubuntu Server 26.04 LTS

1. Introducció

El **DNS** (*Domain Name System*) és el servei fonamental d'Internet que tradueix noms de domini llegibles per humans (com `www.exemple.cat`) en adreces IP numèriques que entenen les màquines.

BIND9 (*Berkeley Internet Name Domain*) és el servidor DNS de codi obert més utilitzat al món i la implementació de referència dels estàndards DNS.

Figura 1: BIND9 logo

Escenari d'aquest document

Configurarem un servidor DNS per a la xarxa local fictícia **`thos.local`** `192.168.10.0/24`:

Rol	Nom FQDN	Adreça IP
Servidor DNS	`ns1.thos.local`	`192.168.10.1`
Servidor web	`www.thos.local`	`192.168.10.10`
Servidor de fitxers	`storage.thos.local`	`192.168.10.20`
Client de proves	`client01.thos.local`	`192.168.10.100`

2. Conceptes previs

2.1. Tipus de servidors DNS

Tipus	Descripció
Autoritatiu	Té la informació definitiva d'una zona DNS. Respon amb autoritat.
Recursiu / cau	Resol consultes en nom dels clients consultant altres servidors i guarda el resultat en cau.
Forwarder	Reenvia les consultes que no pot resoldre a un altre servidor DNS.

2.2. Tipus de registres DNS principals

Registre	Funció	Exemple
`A`	Nom → IPv4	`www IN A 192.168.10.10`
`AAAA`	Nom → IPv6	`www IN AAAA 2001:db8::1`
`PTR`	IP → Nom (invers)	`10 IN PTR www.thos.local.`
`NS`	Servidor de noms de la zona	`@ IN NS ns1.thos.local.`
`MX`	Servidor de correu	`@ IN MX 10 mail.thos.local.`
`CNAME`	Àlies cap a un altre nom	`ftp IN CNAME www.thos.local.`
`SOA`	Informació d'autoritat de zona	(vegeu més avall)
`TXT`	Text arbitrari (SPF, verificació…)	`@ IN TXT "v=spf1 mx ~all"`

2.3. Zones directa i inversa

- **Zona directa:** Tradueix noms → IP. Fitxer de zona per al domini `thos.local`.
- **Zona inversa:** Tradueix IP → noms. Fitxer de zona per a `10.168.192.in-addr.arpa`.

3. Instal·lació de BIND9

3.1. Actualitza el sistema

Actualitza la llista de paquets dels dipòsits

```
sudo apt update
```

Actualitza tots els paquets

```
sudo apt upgrade
```

3.2. Instal·la els paquets necessaris

```
sudo apt install bind9 bind9utils bind9-doc dnsutils
```

- `bind9` --- el servei principal
- `bind9utils` --- eines com `named-checkconf` i `named-checkzone`
- `bind9-doc` --- proporciona la documentació del servidor
- `dnsutils` --- eines de diagnòstic: `dig`, `nslookup`, `host`

3.3. Verifica la instal·lació

```
named -v
```

Sortida esperada:

```
BIND 9.20.18-1ubuntu2.1-Ubuntu (Stable Release) <id:>
```

3.4. Habilita iniciar el servei

Habilita perquè s'inicïi automàticament en cada arrencada del sistema:

```
sudo systemctl enable --now named
```

Comprova l'estat del servei:

```
sudo systemctl status named
```

El servei ha d'aparèixer com **`active (running)`**.

```
● named.service - BIND Domain Name Server
```

```
     Loaded: loaded (/usr/lib/systemd/system/named.service; enabled;
↪  preset: enabled)
     Active: active (running) since Tue 2026-06-30 13:42:12 UTC; 5min
↪  ago
Invocation: 14537caa82cb4eaea3cc72f75195d32a
       Docs: man:named(8)
   Main PID: 9215 (named)
     Status: "running"
      Tasks: 8 (limit: 1718)
     Memory: 10M (peak: 10.3M)
        CPU: 146ms
     CGroup: /system.slice/named.service
             └─9215 /usr/sbin/named -f -u bind
```

4. Estructura de fitxers de BIND9

Després de la instal·lació, els fitxers principals es troben a:

```
/etc/bind/
├── named.conf              # Fitxer principal (inclou els altres)
├── named.conf.options      # Opcions globals del servidor
├── named.conf.local        # Zones locals (les que definirem
↪  nosaltres)
├── named.conf.default-zones # Zones per defecte (localhost, etc.)
├── db.local                # Zona localhost (exemple)
├── db.127                  # Zona inversa 127.x.x.x
└── zones/                  # Directori recomanat per als fitxers de
↪  zona
```

CONSELL

Bones pràctiques: Crea el directori `/etc/bind/zones/` per guardar els fitxers de zona personalitzats.

AVÍS

Si tens la intenció de configurar DDNS és preferible crear les zones al directori `/var/lib/bind/zones` per una qüestió de permisos i propietari. `/etc/bind` sol pertànyer a `root:bind` amb permisos pensats perquè `named` llegeixi la configuració (`named.conf*`), no perquè hi escrigui. `/var/lib/bind` pertany a `bind:bind` amb permisos d'escriptura per al dimoni. Aquí `named` pot crear i actualitzar fitxers sense problemes de permisos.

```
sudo mkdir -p /etc/bind/zones

# o si vols configurar posteriorment DDNS
sudo mkdir -p /var/lib/bind/zones
```

5. Configura com a DNS cau/recursiu

Editarem `named.conf.options` per configurar el comportament general del servidor.

```
sudo nano /etc/bind/named.conf.options
```

Contingut recomanat:

```
options {
    directory "/var/cache/bind";

    // Adreces des de les quals s'accepten consultes recursives
    // Canvia "192.168.10.0/24" per la teva xarxa local
    allow-recursion {
        localhost;
        192.168.10.0/24;
    };

    // Forwarders: a qui reenviem si no podem resoldre localment
    forwarders {
        8.8.8.8;    // Google DNS
        1.1.1.1;    // Cloudflare DNS
    };

    // Millora la seguretat: no retornis la versió de BIND
    version "not disclosed";

    // Escolta a totes les interfícies (o especifica la IP del
 ↪  servidor)
    listen-on { any; };
    listen-on-v6 { any; };

    // Permet consultes des de la xarxa local i localhost
    allow-query {
        localhost;
        192.168.10.0/24;
    };

    // Desactiva transferències de zona per defecte
    allow-transfer { none; };

    dnssec-validation auto;
};
```

PRECAUCIÓ

Mai posis `allow-recursion { any; };` en un servidor públic. Podries convertir-te en amplificador d'atacs DDoS.

Comprova la sintaxi:

```
sudo named-checkconf
```

Si no retorna cap sortida, la configuració és correcta. Reinicia el servei:

```
sudo systemctl restart named
```

6. Configura com a DNS autoritatiu (zona directa)

6.1. Declara la zona a `named.conf.local`

```
sudo nano /etc/bind/named.conf.local
```

Afegeix:

```
// Zona directa per al domini thos.local
zone "thos.local" {
    type master;
    file "/etc/bind/zones/db.thos.local";
    allow-update { none; };
};

// Zona inversa per a la xarxa 192.168.10.0/24
zone "10.168.192.in-addr.arpa" {
    type master;
    file "/etc/bind/zones/db.192.168.10";
    allow-update { none; };
};
```

6.2. Crea el fitxer de zona directa

```
sudo nano /etc/bind/zones/db.thos.local
```

```
; Fitxer de zona directa per a thos.local
; Última modificació: 2026-06-16

$TTL    86400   ; Temps de vida per defecte: 1 dia (en segons)

; Registre SOA (Start of Authority)
@   IN  SOA     ns1.thos.local. admin.thos.local. (
                2026061601  ; Serial (format AAAAMMDDNN --- incrementa
 ↪  en cada canvi)
                3600        ; Refresh: cada quant el secundari comprova
 ↪  canvis (1h)
                900         ; Retry: si falla, torna a intentar-ho als
 ↪  15min
                604800      ; Expire: el secundari descarta la zona als
 ↪  7 dies sense resposta
```

```
                86400       ; Negative TTL: quant temps es guarda en
 ↪  cau una resposta NXDOMAIN
                )

; Servidors de noms de la zona
@       IN  NS      ns1.thos.local.

; Registres A (nom → IP)
ns1     IN  A       192.168.10.1
www     IN  A       192.168.10.10
storage IN  A       192.168.10.20
client01 IN A       192.168.10.100

; Àlies (CNAME)
ftp     IN  CNAME   www.thos.local.

; Servidor de correu (MX)
@       IN  MX  10  mail.thos.local.
mail    IN  A       192.168.10.30

; Registre TXT (exemple SPF)
@       IN  TXT     "v=spf1 mx ~all"
```

IMPORTANT

El **número de sèrie** (serial) ha d'incrementar-se **cada vegada que modifiquis el fitxer**. El format recomanat és `AAAAMMDDNN`, on `NN` és el número de revisió del dia.

6.3. Verifica el fitxer de zona directa

```
sudo named-checkzone thos.local /etc/bind/zones/db.thos.local
```

Sortida correcta:

```
zone thos.local/IN: loaded serial 2026061601
OK
```

7. Configuració de la zona inversa

7.1. Crea el fitxer de zona inversa

```
sudo nano /etc/bind/zones/db.192.168.10
```

```
; Fitxer de zona inversa per a 192.168.10.0/24
; Última modificació: 2026-06-16

$TTL    86400

; Registre SOA
@   IN  SOA     ns1.thos.local. admin.thos.local. (
                2026061601
                3600
                900
                604800
                86400
                )

; Servidor de noms
@       IN  NS      ns1.thos.local.

; Registres PTR (IP → nom)
; Nota: s'escriu només l'últim octet de l'adreça IP
1       IN  PTR     ns1.thos.local.
10      IN  PTR     www.thos.local.
20      IN  PTR     storage.thos.local.
30      IN  PTR     mail.thos.local.
100     IN  PTR     client01.thos.local.
```

7.2. Verifica el fitxer de zona inversa

```
sudo named-checkzone 10.168.192.in-addr.arpa
 ↪  /etc/bind/zones/db.192.168.10
```

Sortida correcta:

```
zone 10.168.192.in-addr.arpa/IN: loaded serial 2026061601
OK
```

7.3. Reinici i estat del servei

Reinicia el servei:

```
sudo systemctl restart named
```

Comprova l'estat:

```
sudo systemctl status named
```

```
● named.service - BIND Domain Name Server
     Loaded: loaded (/usr/lib/systemd/system/named.service; enabled;
 ↪  preset: enabled)
     Active: active (running) since Tue 2026-06-30 14:02:13 UTC; 1min
 ↪  16s ago
 Invocation: d75e0cbb344c4a91a6e17e96b6e30221
       Docs: man:named(8)
   Main PID: 11713 (named)
     Status: "running"
      Tasks: 8 (limit: 1718)
     Memory: 6.2M (peak: 6.5M)
        CPU: 24ms
     CGroup: /system.slice/named.service
             └─11713 /usr/sbin/named -f -u bind
```

8. Verificació i proves

8.1. Comprova que el port 53 és actiu

```
sudo ss -tulnp | grep named
```

Ha de mostrar el servei escoltant al port 53 per TCP i UDP.

```
udp   UNCONN 0      0                            192.168.10.1:53
 ↪  0.0.0.0:*    users:(("named",pid=11713,fd=43))
udp   UNCONN 0      0                            192.168.10.1:53
 ↪  0.0.0.0:*    users:(("named",pid=11713,fd=42))
udp   UNCONN 0      0                               127.0.0.1:53
 ↪  0.0.0.0:*    users:(("named",pid=11713,fd=29))
udp   UNCONN 0      0                               127.0.0.1:53
 ↪  0.0.0.0:*    users:(("named",pid=11713,fd=28))
tcp   LISTEN 0      10                           192.168.10.1:53
 ↪  0.0.0.0:*    users:(("named",pid=11713,fd=45))
tcp   LISTEN 0      10                           192.168.10.1:53
 ↪  0.0.0.0:*    users:(("named",pid=11713,fd=44))
tcp   LISTEN 0      10                              127.0.0.1:53
 ↪  0.0.0.0:*    users:(("named",pid=11713,fd=32))
```

```
tcp   LISTEN 0      10                                 127.0.0.1:53
 ↪  0.0.0.0:*    users:(("named",pid=11713,fd=30))
tcp   LISTEN 0      5                                  127.0.0.1:953
 ↪  0.0.0.0:*    users:(("named",pid=11713,fd=63))
```

8.2. Proves amb `dig`

Resolució directa (nom → IP):

```
dig @192.168.10.1 www.thos.local
```

Sortida esperada (fragment):

```
;; ANSWER SECTION:
www.thos.local.          86400   IN      A       192.168.10.10
```

Resolució inversa (IP → nom):

```
dig @192.168.10.1 -x 192.168.10.10
```

Sortida esperada:

```
;; ANSWER SECTION:
10.10.168.192.in-addr.arpa. 86400 IN PTR www.thos.local.
```

Consulta de registres NS:

```
dig @192.168.10.1 thos.local NS
```

Consulta de registres MX:

```
dig @192.168.10.1 thos.local MX
```

Comprovació d'un CNAME:

```
dig @192.168.10.1 ftp.thos.local
```

8.3. Proves amb `nslookup`

```
nslookup www.thos.local 192.168.10.1
nslookup 192.168.10.10 192.168.10.1
```

8.4. Proves amb `host`

```
host www.thos.local 192.168.10.1
host -t MX thos.local 192.168.10.1
```

8.5. Comprova els logs del servei

```
sudo journalctl -u named -f
```

9. Configuració del client

9.1. Ubuntu / Debian (amb systemd-resolved)

Edita la configuració de la interfície de xarxa amb Netplan:

```
sudo nano /etc/netplan/00-installer-config.yaml
```

```
network:
  version: 2
  ethernets:
    enp0s3:
      addresses:
      - 192.168.10.100/24
      nameservers:
        addresses:
        - 192.168.10.1
      search:
      - thos.local
      routes:
      - to: default
        via: 192.168.10.1
```

Aplica els canvis:

```
sudo netplan apply
```

Verifica la resolució de noms:

```
resolvectl status
dig www.thos.local
```

9.2. Comprova `/etc/resolv.conf`

```
cat /etc/resolv.conf
```

Ha de contenir:

```
nameserver 192.168.10.1
search thos.local
```

10. Resolució de problemes

10.1. El servei no arrenca

```
sudo journalctl -u named --no-pager | tail -30
sudo named-checkconf -z   # Comprova tota la configuració i zones
```

10.2. La zona no carrega

```
sudo named-checkzone thos.local /etc/bind/zones/db.thos.local
```

Errors habituals:

- **Punts finals omesos** en els noms FQDN (p. ex. `ns1.thos.local` en lloc de `ns1.thos.local.`)
- **Serial sense incrementar** en modificar el fitxer
- **Permisos incorrectes** als fitxers de zona

Corregeix els permisos:

```
sudo chown -R bind:bind /etc/bind/zones/
sudo chmod 640 /etc/bind/zones/*
```

10.3. El client no resol

```
# Comprova connectivitat bàsica al servidor DNS
ping 192.168.10.1

# Prova una consulta directa
dig @192.168.10.1 www.thos.local

# Si funciona amb @IP però no sense, el problema és la configuració
 ↪  del client
cat /etc/resolv.conf
```

10.4. Error de tallafocs

Si el servidor té `ufw` actiu, cal obrir el port 53:

```
sudo ufw allow 53/tcp
sudo ufw allow 53/udp
sudo ufw reload
```

10.5. Taula de diagnosi ràpida

Símptoma	Ordre de diagnosi	Solució probable
`SERVFAIL`	`journalctl -u named`	Error al fitxer de zona
`NXDOMAIN`	`named-checkzone`	Registre no definit a la zona
`connection refused`	`ss -tulnp | grep named`	Servei aturat o no escolta
El client no resol	`cat /etc/resolv.conf`	DNS mal configurat al client
Canvis no reflectits	---	Serial no incrementat; reinicia `named`

11. Resum de fitxers modificats

Fitxer	Funció
`/etc/bind/named.conf.options`	Opcions globals: forwarders, ACL, recursió
`/etc/bind/named.conf.local`	Declaració de zones locals
`/etc/bind/zones/db.thos.local`	Fitxer de zona directa (nom → IP)
`/etc/bind/zones/db.192.168.10`	Fitxer de zona inversa (IP → nom)

Ordres de gestió del servei

```
sudo systemctl start named      # Iniciar
sudo systemctl stop named       # Aturar
sudo systemctl restart named    # Reiniciar (aplica canvis)
sudo systemctl reload named     # Recarregar zones sense reiniciar
sudo systemctl status named     # Estat del servei

sudo named-checkconf            # Verificar sintaxi de la configuració
sudo named-checkzone <zona> <fitxer>  # Verificar un fitxer de zona
```

12. Referències i recursos

Documentació oficial

Recurs	URL	Descripció
BIND 9 ARM (Administrator Reference Manual)	bind9.readthedocs.io	Manual de referència oficial i complet de BIND9 --- la font autoritativa
ISC BIND9	isc.org/bind	Pàgina oficial del projecte BIND a l'Internet Systems Consortium (ISC)
Ubuntu Server Docs --- DNS	documentation.ubuntu.com/server/.. dns	Guia oficial d'Ubuntu per instal·lar i configurar BIND9
RFCs DNS a IETF	datatracker.ietf.org	Estàndards tècnics originals del DNS (RFC 1034, RFC 1035, etc.)

RFCs fonamentals del DNS

RFC	Títol	Rellevància
RFC 1034	*Domain Names --- Concepts and Facilities*	Conceptes generals del DNS
RFC 1035	*Domain Names --- Implementation and Specification*	Implementació i formats de registres
RFC 2308	*Negative Caching of DNS Queries*	Comportament del TTL negatiu (NXDOMAIN)
RFC 4034	*Resource Records for the DNS Security Extensions*	Base de DNSSEC

NOTA

Els RFCs es poden consultar a datatracker.ietf.org o a rfc-editor.org.

Tutorials i guies addicionals

Recurs	URL	Descripció
DNS for Rocket Scientists	zytrax.com/books/dns	Llibre en línia gratuït i molt complet sobre DNS i BIND --- molt recomanat
LinuxTechi --- BIND9 Ubuntu	linuxtechi.com/…	Guia pràctica d'instal·lació a Ubuntu 24.04 / 22.04
AlphaVPS --- BIND9 Ubuntu 24.04	blog.alphavps.com/…	Configuració de BIND9 com a servidor autoritatiu

Eines de diagnosi en línia

Eina	URL	Funció
MXToolbox DNS Lookup	mxtoolbox.com/DNSLookup.aspx	Consultes DNS (A, MX, NS, PTR…) des del navegador
DNSChecker	dnschecker.org	Comprova la propagació DNS des de múltiples ubicacions
intoDNS	intodns.com	Anàlisi completa de la configuració DNS d'un domini
RIPE WHOIS	apps.db.ripe.net	Informació de registres d'IP i dominis a Europa

Seguretat DNS

Recurs	URL	Descripció
NIST DNS Deployment Guide	csrc.nist.gov	Guia de bones pràctiques de seguretat DNS del NIST
ISC Security Advisories	kb.isc.org/docs/security-advisories	Avisos de seguretat oficials per a BIND9

Índex de figures

Versions d'aquest document

- HTML
- PDF
- ODT
- MD