Projecte ASIX 2k22

Escola Del Treball

2HISX 2021-2022

Aaron Andal & Cristian Condolo

CryptoSEC: "*Careful where you step in*"

> **Img Source**: *@Aaron & @Cristian 's GitHub*

Index

Que es el DNS?

El sistema de noms de **domini (DNS)** és l'agenda telefònica d'Internet. Permet associar noms de domini amb direccions IP per facilitar en gran mesura l'accés als hosts de la xarxa.

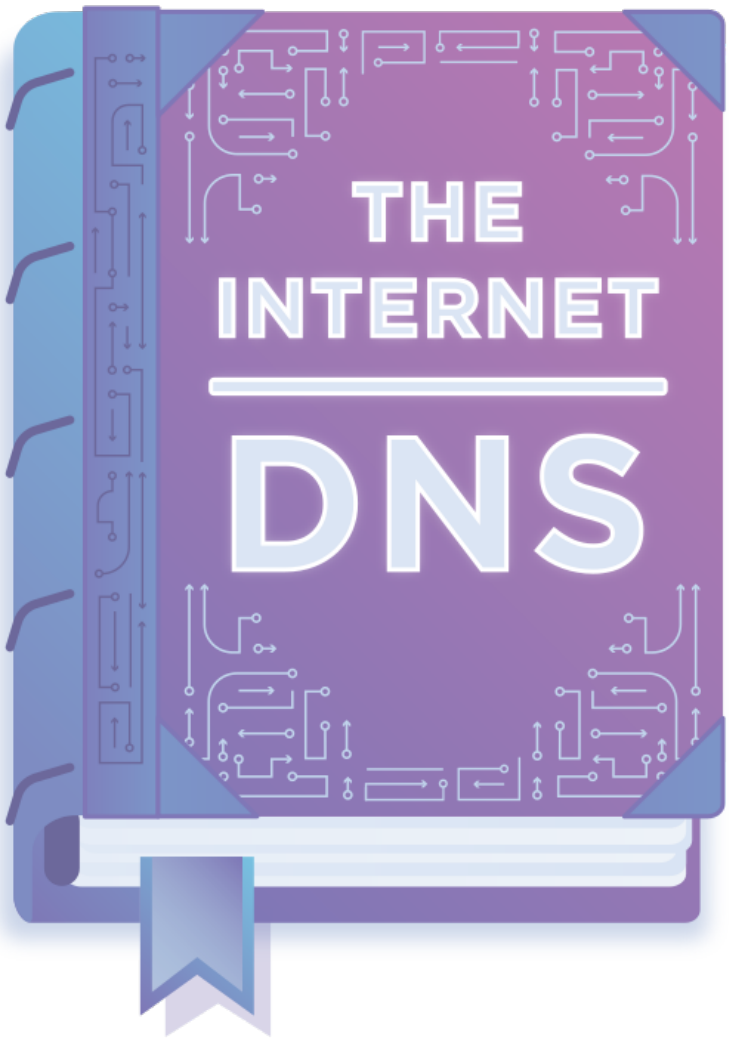
Els humans accedeixen a la informació en línia mitjançant **noms de domini**, com ara **nytimes.com** o **espn.com**.

Els navegadors web interactuen mitjançant adreces de **Protocol d'Internet (IP)**.

DNS *tradueix* els **noms de domini** a **adreces IP** perquè els navegadors puguin *carregar recursos d'Internet*.

Cada dispositiu connectat a **Internet** té una **adreça IP única** que altres màquines utilitzen per trobar el dispositiu.

Els servidors DNS eliminen la necessitat que els h___umans memoritzin___ adreces IP com ara **192.168.1.1** (en IPv4) o adreces IP alfanumèriques més complexes, com ara 2400:cb00:2048:1::c629:d7a2 (en IPv6).



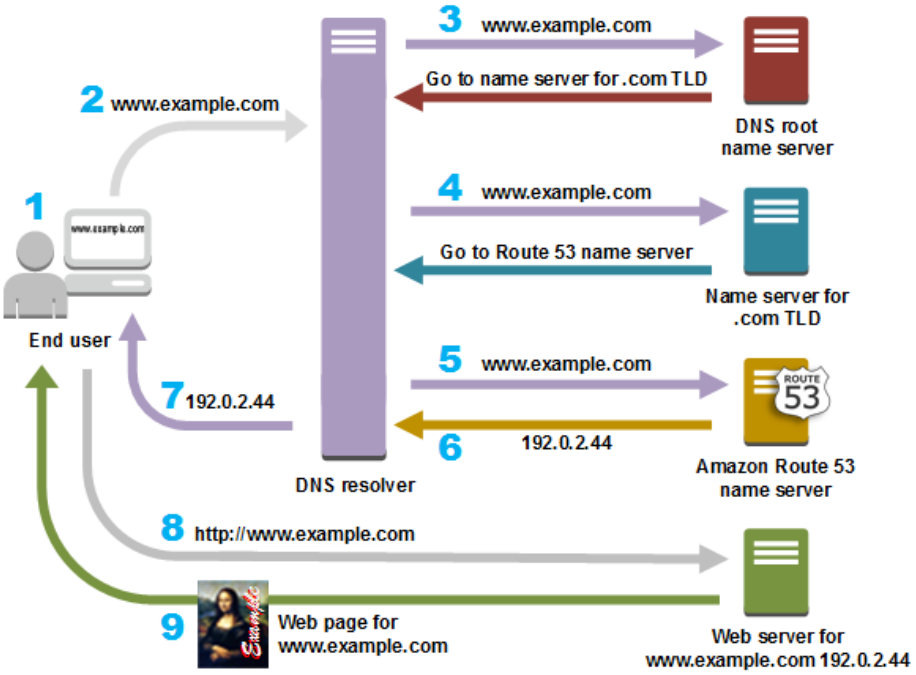
> **Img Source**: *@Aaron & @Cristian 's GitHub*

Com funciona el DNS

El procés de resolució de DNS implica convertir un nom d'**amfitrió** (com ara www.example.com) en una adreça IP compatible amb l'ordinador (com ara 192.168.1.1). Es dóna una adreça IP a cada dispositiu a **Internet**, i aquesta adreça és necessària per trobar el dispositiu d'Internet adequat, com si s'utilitza una **adreça** de carrer per trobar una casa determinada.

Quan un usuari vol **carregar** una **pàgina web**, s'ha de produir una traducció entre el que un usuari escriu al seu navegador web (**example.com**) i l'adreça adaptada a la màquina necessària per localitzar la pàgina web **example.com**.

Per entendre el procés darrere de la *resolució DNS*, és important conèixer els diferents components de maquinari entre els quals ha de passar una consulta DNS. Per al navegador web, la cerca de DNS es produeix "darrere de l'escenari" i no requereix cap interacció de l'ordinador de l'usuari a part de la sol · licitud inicial.



> **Img Source**: *https://d1.awsstatic.com/Route53/how-route-53-routes-traffic.8d313c7da075c3c7303aaef32e89b5d0b7885e7c.png*

Tipus de DNS "4 servidors DNS implicats en la càrrega d'una pàgina web":

Tots els **servidors DNS** es divideixen en una d'aquestes quatre categories: **Resolvers recursius**, **Root Servers** , **Servidor de noms TLD** i **State Of Authority**.

En una cerca DNS típica (quan no hi ha **memòria cau** en joc), aquests quatre servidors DNS treballen junts en harmonia per completar la tasca de lliurar l' adreça IP d'un domini especificat al client (el client sol ser un solucionador de talons, un senzill resolutor integrat en un sistema operatiu).

Resolver de DNS Recursiu

1. **DNS Recursor (Servidor DNS Recursiu)** : És com un **bibliotecari** a la qual se li demana que busqui un llibre determinar a la biblioteca. El **recurs DNS** és un **servidor** dissenyat per rebre consultes de les màquines client mitjançant aplicacions com ara navegadors **web**. Normalment, el recurs és responsable de fer **peticions** addicionals per satisfer la **consulta DNS del client**.

És la *primera parada* d'una **consulta DNS**.

El *resolver* recursiu actua com a intermediari entre un client i un servidor de noms DNS.

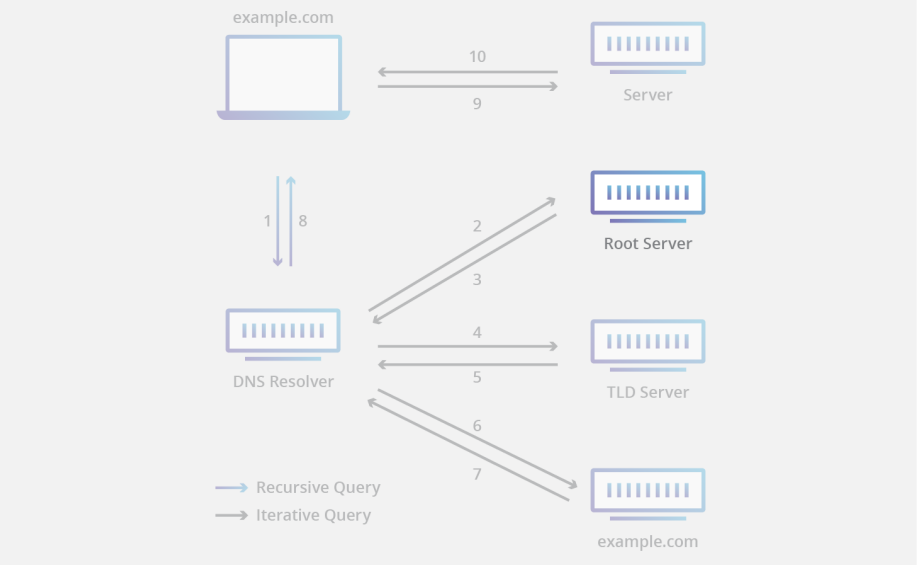
Després de rebre una consulta DNS d'un client web, un *resolver* recursiu respondrà amb dades emmagatzemades a la **memoria CAU** o enviarà una sol · licitud a un servidor de **noms arrel (Root Servers)**, seguida d'una altra sol · licitud a un servidor de noms TLD i després d'una última sol · licitud a un servidor de noms autoritzat.

Després de rebre una resposta del servidor de noms autoritzat que conté l'adreça IP sol · licitada, el resolutor recursiu envia una resposta al client.

Durant aquest procés, el solucionador recursiu guardarà a la **memòria cau** la informació rebuda dels servidors de noms autoritzats.

Quan un client nou sol · liciti l'adreça IP d'un nom de domini que ha estat sol · licitat recentment per un altre client, el *resolver* pot eludir el procés de comunicació amb els servidors de noms i només lliurar al client el registre sol · licitat de la seva memòria cau.

La majoria dels usuaris d'Internet utilitzen un solucionador recursiu proporcionat pel seu ISP, però hi ha altres opcions disponibles; per exemple , l'1.1.1.1 de Cloudflare .



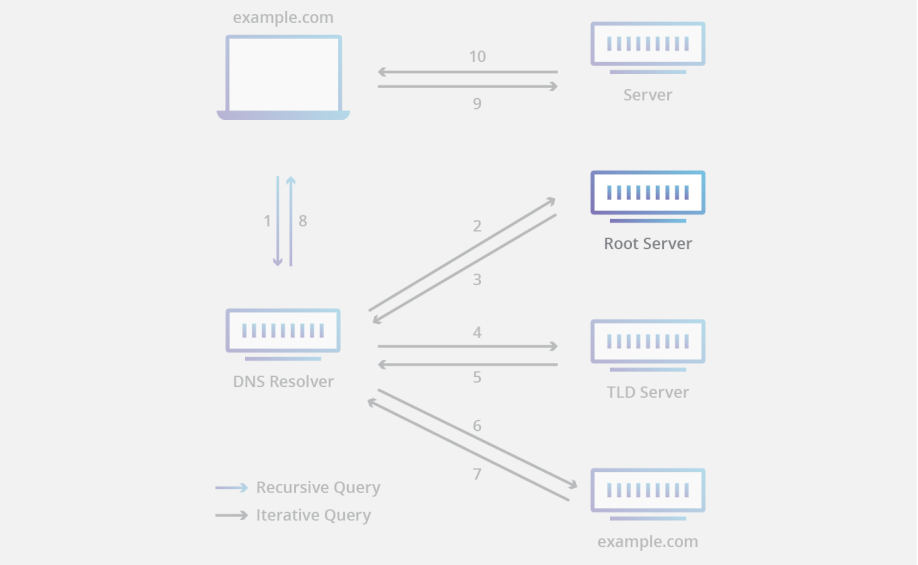
> **Img Source**: *https://www.cloudflare.com/img/learning/dns/dns-server-types/root-nameserver.png*

Root Servers

- **Root Servers** : El **servidor arrel** és el primer pas per traduir (resolució) noms d'amfitrió llegibles per humans a **adreces IP**. Es pot pensar com un **índex** en una **biblioteca** que apunta a **diferents bastidors** de llibres; normalment serveix com a referència a altres ubicacions més específiques.

Hi han 13 servidors de noms d'arrel DNS, són coneguts per tots els *resolvers recursius* i són la primera parada en la recera de registres DNS d'un *resolver recursiu*.

Un servidor arrel accepta la consulta d'un resolutor recursiu que inclou un nom de domini, i el servidor de noms arrel respon dirigint el resolutor recursiu a un **servidor de noms TLD**, en funció de l'extensió d'aquest domini **(.com, .net, .org, etc.)**.



> **Img Source**: *https://www.cloudflare.com/img/learning/dns/dns-server-types/root-nameserver.png*

Servidor DNS - TLD

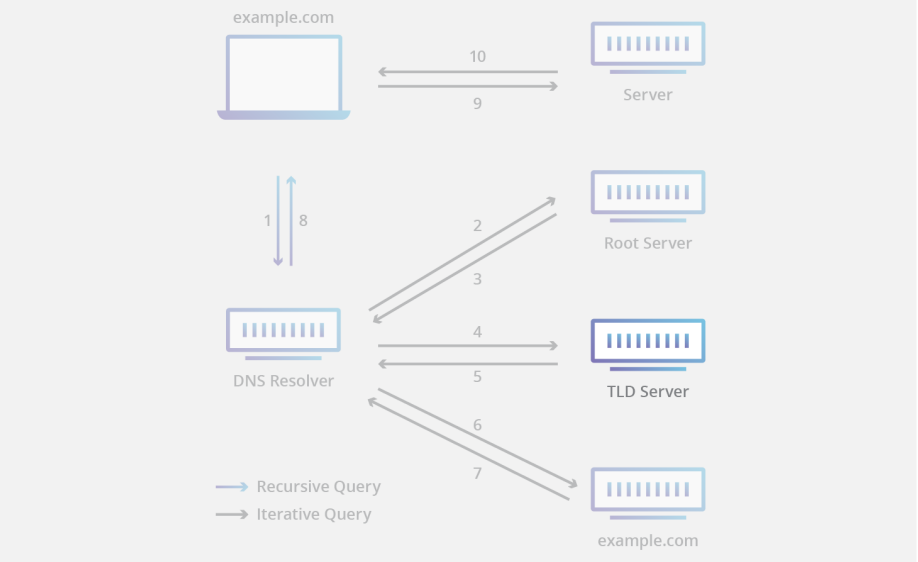
- **Servidor DNS - TLD** : El servidor de domini de **primer nivell** (TLD = Top Layer Domain) es pot considerar com un *lloc específic* de llibres d'una biblioteca. Aquest servidor de noms és el següent pas en la cerca d'una adreça IP específica i allotja l'última part d'un nom d'amfitrió (a example.com, el servidor TLD és "com").

Un **servidor de noms TLD** manté la informació de tots els noms de domini que comparteixen una extensió de domini comuna, com ara .com, .net o qualsevol que vingui després de l'últim punt d'una URL.

Per exemple, un servidor de noms TLD **.com** conté informació per a cada lloc web que acabi en **".com"**.

Si un usuari estava cercant **google.com**, després de rebre una resposta d'un servidor de noms arrel, el solucionador recursiu enviaria una consulta a un servidor de noms TLD .com, que respondria apuntant al servidor de noms autoritzat (vegeu més avall) per a aquest domini.

- Dominis genèrics de **primer nivell**: són dominis que no són específics d'un país, alguns dels TLD genèrics més coneguts inclouen **.com, .org, .net, .edu i .gov.**
- Dominis de **nivell superior** de codi de país: inclouen tots els dominis específics d'un país o estat. Alguns exemples inclouen **.uk, .us, .ru i .jp**.



> **Img Source**: *https://www.cloudflare.com/img/learning/dns/dns-server-types/tld-nameserver.png*

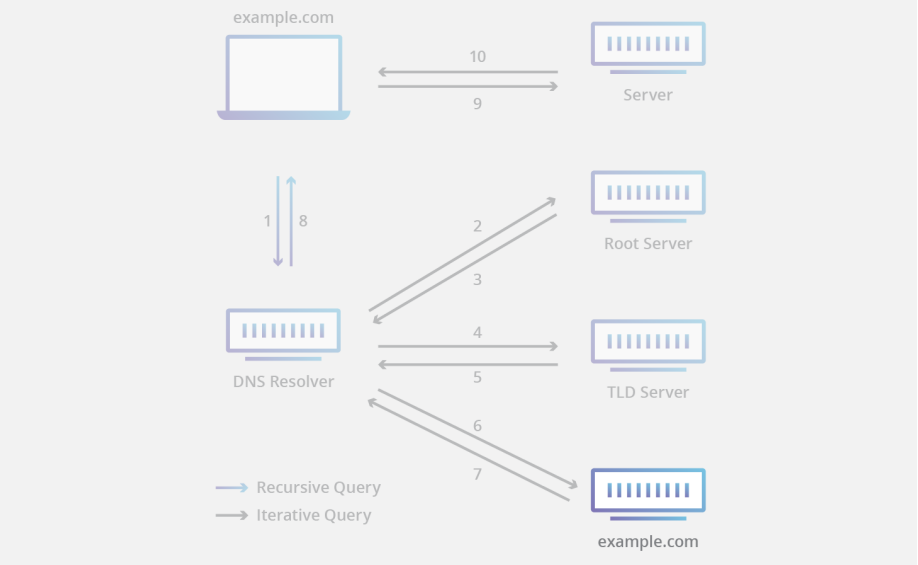
Servidor DNS Authoritative

- **Servidor de noms autoritzat (Authoritative DNS Server)** : Es pot interpretar com un diccionari en una **prestatgeria de llibres**, on es pot consultar la **definició** d'un **nom específic**. Aquest servidor de noms autoritzat és **l'última parada** de la consulta del servidor de noms. Si el servidor de noms autoritzat té accés al registre sol · licitat, retornarà l'adreça IP del nom d'amfitrió sol · licitat al recurs DNS **(el bibliotecari)** que va fer la sol · licitud inicial.

Quan un *resolver recursiu* rep una resposta d'un servidor de noms TLD, aquesta resposta es dirigirà directament a un servidor DNS autoritatiu *(Authoritative DNS Server)*.

El servidor de noms autoritatiu conté la informació específica del nom de domini a la qual serveix.

Pot proporcionar una **solució recursiva** amb l'adreça IP d'aquest servidor que es troba al registra **DNS A** o si té un alias registre **CNAME**, que proporcionarà al *resolver recursiu* un domini d'àlies.



> **Img Source**: *https://www.cloudflare.com/img/learning/dns/dns-server-types/authoritative-nameserver.png*

Diferencia entre "Authoritative DNS Server" i "Recursive DNS Resolver"

Els dos conceptes es refereixen a servidors (O grups de servidors) que estàn *"integrals"* a la infraestructura DNS, però cadascun realitza un paper diferent. Es troba en diferents ubicacions dins del trajecte d'una consulta de DNS. Una manera d'entendre la diferència és que el *"Recursive Resolver"* és a l'inici de la consulta DNS i el *"Athoritative Nameserver"* (servidor de noms autoritatiu) al final.

Recursive DNS Resolver

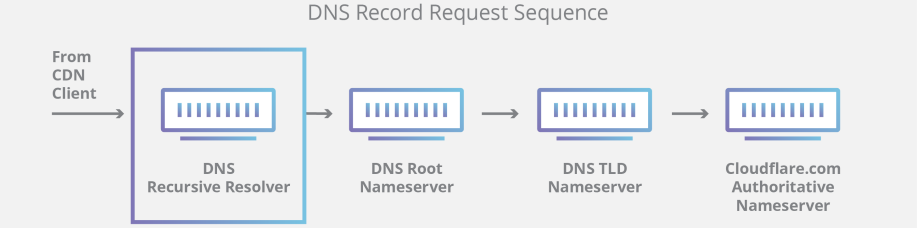
El *"Recursive DNS Resolver"* és el servidor que respon a una solicitud recursiva del client i dedica temps a detectar el **registre DNS**.

Ho fa mitjançant una **sèrie de sol · licituds** fins que arriba al servidor de noms DNS autoritatiu *(Authoritative DNS Server)* per al registre DNS sol · licitat (o es torna inactiu o torna un error si no es troba cap registre).

Amb altres paraules, el client que fa una petició per anar a *www.exemple.com*, el *"Recursive DNS Resolver"* respon la petició i va preguntant a altres *servidors* quina IP es la *www.exemple.com* fins que arriba al servidor DNS autoriratiu *(Authoritative DNS Server)* que conté la zona *www.exemple.com* en els seus registres.

Afortunadament, els *"Recursive DNS Resolver"* **no** sempre han de fer diverses sol · licituds per inspeccionar els registres necessaris per respondre a un client.

L' emmagatzematge en **memòria cau** és un procés d'agilització de procés en la *busca* del registre DNS que ajuda a **saltar-se** les sol · licituds *necessàries* servint abans el registre del recurs sol · licitat a la cerca DNS.



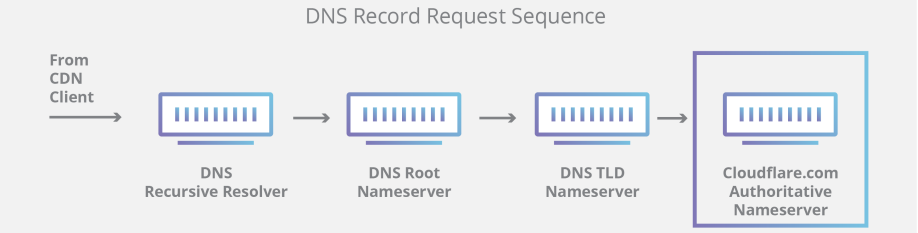
> **Img Source**: *https://www.cloudflare.com/img/learning/dns/what-is-dns/dns-record-request-sequence-1.png*

Authoritative DNS Server

Un servidor DNS autoritatiu *(Authoritative DNS Server)* és un servidor que allotja realment registres de recursos DNS i n'és responsable.

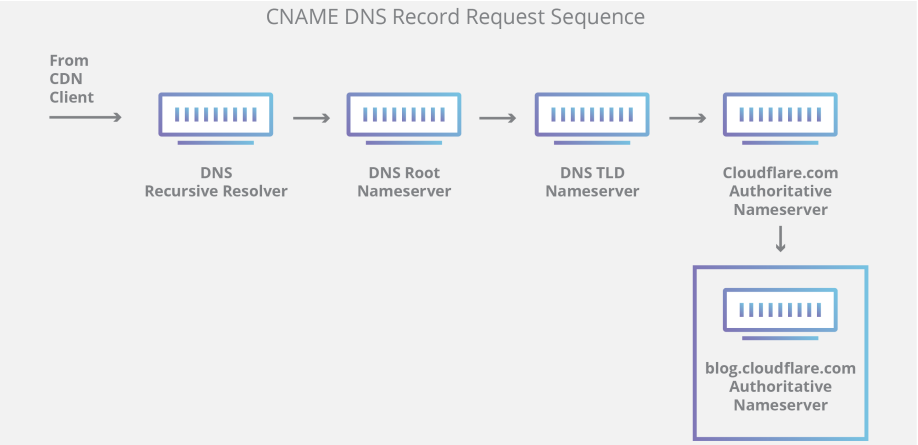
Aquest és el **servidor al final** de la cadena de cerca de DNS que respondrà amb el registre DNS del recurs consultat, permetent finalment que el **navegador web** faci la sol · licitud per arribar a **l'adreça IP** necessària per accedir a un **lloc web** o altres **recursos web**.

Un servidor DNS autoritatiu *(Authoritative DNS Server)* pot oferir sol · licituds a partir de les seves pròpies dades sense necessitat de consultar altres recursos *(recursive)*, ja que és la font final de veritat per a **certs registres DNS**.



> **Img Source**: *https://www.cloudflare.com/img/learning/dns/what-is-dns/dns-record-request-sequence-2.png*

Convé indicar que en els casos de *consultes relatives* a **subdominis**, com ara *foo.exemple.com* o *blog.cloudflare.com* , s'afegirà un servidor de noms addicional a la seqüència després del servidor de noms autoritatiu, que és el responsable d'emmagatzemar el registre **CNAME** del subdomini.



> **Img Source**: *https://www.cloudflare.com/img/learning/dns/what-is-dns/dns-record-request-sequence-3.png*

Hi ha una diferencia fundamental entre molts serveis de DNS i el que ofereix Cloudfare per exemple. Hi han diferents *"Recursive DNS Resolver"* com Google DNS, OpenDNS o proveïdors com Comcast mantenen instal · lacions de centre de dades de *"Recursive DNS Resolver"*.

Aquests *"Resolvers"* permeten consultes rapides i senzilles mitjaçant clusters optimitzats de sistemes informàtics optimitzats per a DNS. Però son bàsicament diferents servidors de noms allotjats en servidors com per exemple Cloudflare.

Procediment per fer un "lookup" de DNS

En la majoria de situacions, DNS fa referència a un **nom de domini** que s'està traduint a l'adreça IP.

Sovint, la informació de cerca de DNS s'emmagatzemarà a la memòria **cau local** dins del servidor que realitzi la **consulta** o en **remot** a la *infraestructura* de DNS.

Generalment, hi ha 8 passos en una cerca DNS.

Quan la informació de DNS s'emmagatzema en memòria cau, s'ometen els passos del procés de cerca DNS, cosa que ho fa més ràpid. L'exemple descriu els 8 passos necessaris quan no s'ha emmagatzemat res a la memòria cau.

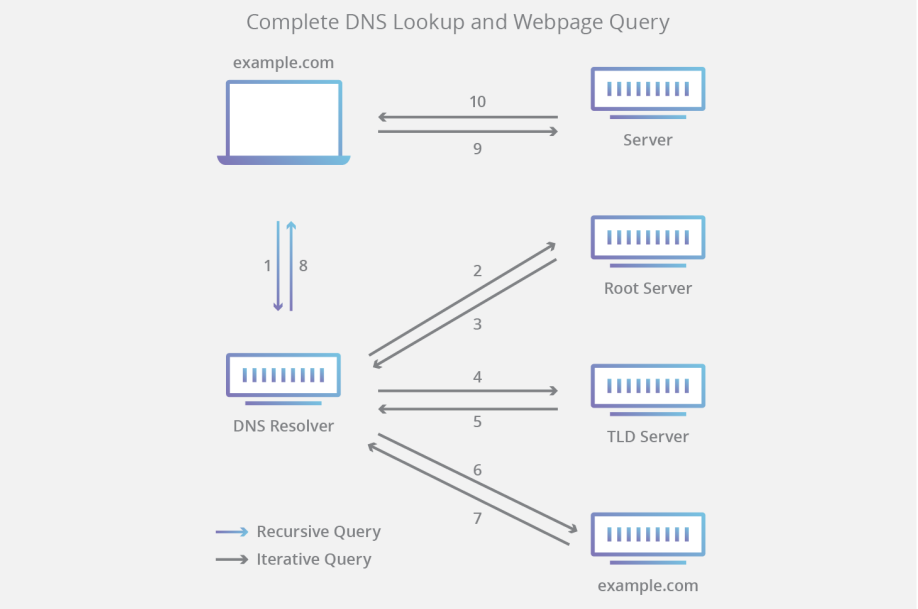
Els 8 passos d'un "lookup" de DNS

1. Un usuari escriu "exemple.com" en un navegador web i la consulta recorre Internet i és rebuda per un *"resolutor recursiu de DNS (Recursive DNS Resolver)"*.

2. El *resolver* consulta a continuació un servidor de *noms d'arrel de DNS (Root Servers) (.)* = Internet.
3. El servidor arrel *(Root Servers)* respon a continuació al *resolver* amb l'adreça d'un servidor de *DNS de domini* de **primer nivell** (TLD = Top Level Domain) (p.ex. .com o .net), que emmagatzema la informació per als vostres dominis. En cercar "*exemple.com*", la nostra sol · licitud es dirigeix al TLD **.com**.
4. El *resolver* farà a continuació una sol · licitud al domini de **primer nivell** .___com___.
5. El **servidor TLD** respondrà a continuació amb l'adreça IP del servidor de noms del domini autoriratiu *(Authoritative DNS Server)*: **exemple.com**.
6. Finalment, el *resolver recursiu* envia una consulta al *servidor de noms del domini autoritatiu* **(Authoritative DNS Server)**.
7. Per exemple, l'adreça IP es retornarà al *resolver* desde del *servidor de noms*.
8. El *resolver de DNS* respondrà a continuació al *navegador web* amb **l'adreça IP del domini** sol · licitat inicialment.

Un cop els 8 passos de la cerca del DNS han tornat l'adreça IP per exemple.com, el navegador podrà fer la sol · licitud per a la *pàgina web*:

9. El navegador farà una sol · licitud **d'HTTP** a l'adreça IP.
10. El servidor en aquesta adreça IP torna la **pàgina web** perquè es processi al navegador (pas 10).



> **Img Source**: *https://www.cloudflare.com/img/learning/dns/what-is-dns/dns-lookup-diagram.png*

Què és un *"resolver"* de DNS

El **resolver de DNS** és la **primera parada** de la recerca de DNS i s'encarrega de tractar amb el **client** que va fer la **sol · licitud inicial**.

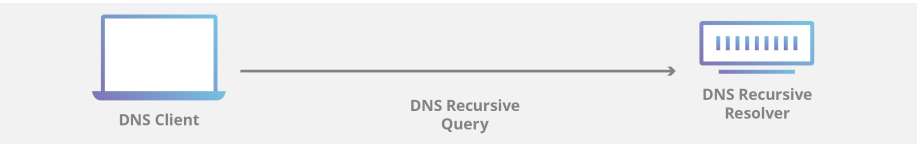
El solucionador inicia la seqüència de consultes que porten en última instància que l'URL es tradueixi a l'adreça IP necessària.

Nota: una cerca de DNS no emmagatzemada a la memòria cau inclourà consultes recursives i iteratives.

És important diferencia entre una *consulta* de *DNS recursiu* i un *resolver* de *DNS recursiu*.

La **consulta** fa referència a la sol · licitud feta a un solucionador de DNS que requereix la resolució de la consulta.

Un **resolver** de DNS recursiu és el servidor que accepta una **solució recursiva** i procesa la resposta fent les **sol · licituds necessàries**.



> **Img Source**: *https://www.cloudflare.com/img/learning/dns/what-is-dns/dns-*

recursive-query.png

Tipus de consultes DNS

En una busca DNS habitual es produeixen 3 tipus de consultes.

En utilitzar una combinació d'aquestes consultes, un procés optimitzat per la resolució de DNS es pot comportar una reducció de "salts". En una situació ideal, les dades de registra emmagatzemades a la memòria CAU estaran disponibles, la qual cosa permetrà que un servidor de noms DNS torni a una consulta no *recursiva*.

3 tipus de consultes DNS:

1. **Consulta recursiva**: En una consulta recursiva, un client DNS requereix que un servidor DNS (generalment un *resolver* de **DNS recursiu**) respongui al **client** amb el registre del recurs sol · licitat o un missatge d'error si el solucionador no pot trobar el registre.
2. **Consulta iterativa**: En aquesta situació, el *client DNS* permetrà que un **servidor DNS** retorni la **millor resposta** possible. Si el servidor DNS consultat no té el **nom** que ha demanat el client en la s eva consulta, el servidor DNS retornarà una referencia a un servidor DNS autoritatiu. El **client DNS** farà a continuació una consulta a **l'adreça de referència**. Aquest procés continua amb servidors DNS addicionals que segueixen a la cadena de consulta fins que es produeixi un error o se superi el temps despera.
3. **Consulta no recursiva**: Generalment es produeix quan un **client solucionador de DNS** consulta un **servidor DNS** per un registre al qual té **accés** perquè o bé **és autoritatiu** per al **registre** o el registre **existeix** dins de la seva memòria cau. Generalment, el servidor DNS emmagatzemarà a la memòria cau registres DNS per prevenir el consum d'amplada de banda addicional i la càrrega als servidors que precedeixen a la cadena.

Que es el emmagatzematge en caché de DNS?

L'objectiu de l'emmagatzematge a la memòria cau és guardar dades en una ubicació temporalment per aconseguir millores en el rendiment i fiabilitat en les sol · licituds de dades.

L'emmagatzematge en memòria cau de DNS guarda dades més a prop del client sol · licitant perquè la consulta DNS es pugui resoldre abans i les consultes addicionals que segueixen a la cadena de cerca DNS es puguin evitar, millorant així els temps de càrrega i reduint el consum d'amplada de banda/CPU.

Les dades de DNS es poden emmagatzemar en memòria cau en diverses ubicacions. Cadascuna guardarà els registres DNS durant una quantitat de temps establerta, determinada pel temps de vida (TTL) .

Que es un registre DNS?

Els registres DNS o també conegut con *arxius de zona* son instruccions radicades en servidors DNS autoritatius que proporcionen informacó sobre un domini, com l'adreça IP associada amb aquest i com gestionar sol · licituds dirigides a aquest domini.

Aquests registres consisteixen en una sèrie de fitxers de text escrits en el que es coneix com a sintaxi DNS. La sintaxi DNS és simplement una cadena de caràcters utilitzats com a ordres que diuen al servidor DNS què fer.

Exemple: **db.cryptosec.net** que es troba a **/etc/bind/**

Tots els registres DNS tenen també un " TTL “, que vol dir”time-to-live" i indica amb quina freqüència el servidor DNS actualitzarà aquest registre.

Tipus de registres DNS

MÉS COMUNS

- A: Conté l'adreça IP d'un domini.
- AAAA: Lo mateix que l'anterior pero per a Ipv6
- CNAME: Reenvia un domini o subdominis, es un alias, no proporciona una adreça IP.
- MX: Es dirigeix a un servidor de correu electrònic.
- TXT: Permet que un administrador pugui emmagatzemar notes de text al registre. Aquests registres se solen utilitzar per a la seguretat del correu electrònic.
- NS: Emmagatzema el servidor de noms per a una entrada DNS. Més info
- SOA: State of Authority. Emmagatzema la informació de l'administrador sobre un domini o zona. Més info
- SRV: Especifica un port per a serveis específics
- PTR: Proporciona un nom de domini a cerques inverses. Resolució inversa.

MÉNYS COMUNS

- SSHFP: Aquest registre emmagatzema les “empremtes digitals de la clau pública SSH”; SSH fa referència a “Secure Shell” i és un protocol de xarxa xifrat que permet la comunicació segura a una xarxa insegura.

- RP: Aquest és el registre de la "persona responsable" i emmagatzema l'adreça de correu electrònic de la persona responsable del domini.
- DCHID : el "identificador DHCP" emmagatzema informació per al protocol de configuració dinàmica de host (DHCP), un protocol de xarxa estandarditzat utilitzat a les xarxes IP.

DNSSEC

- CAA: És el registre d'"autorització d'autoritat de certificació"; permet que els propietaris d'un domini especifiquin quines autoritats de certificació poden emetre certificats per a aquest domini. Si no existeix cap registre CAA, aleshores qualsevol podrà emetre un certificat per a aquest domini. Aquests registres també els hereten els subdominis.
- DNSKEY: El ' Registre de Clau DNS ' conté una clau pública que es fa servir per verificar les signatures de l' Extensió de seguretat del sistema de noms de domini (DNSSEC) .
- CDNSKEY: És una còpia fill del registre DNSKEY destinada a transferir-se a un pare.
- CERT: El "registre de certificats" emmagatzema certificats de claus públiques.
- NSEC: El "següent registre segur" és part del DNSSEC i s'usa per demostrar que un registre de recursos DNS sol · licitat no existeix.
- RRSIG : el "registre de recursos de signatura" emmagatzema signatures digitals utilitzades per autenticar registres de conformitat amb el DNSSEC.

Que es un DNS recursiu?

Una cerca de DNS recursiu és quan un servidor DNS es comunica amb altres servidors DNS per "trobar" una direcció IP i retornarla al client. Això es diferencia d'una consulta de DNS iterativa, en la que el client es comunica directament amb cada servidor DNS implicat en la cerca.

Exemple resumit de DNS

1. Un usuari escriu un nom de domini: **"cryptosec.net"** en el seu navegador, s'activa una **cerca de DNS**.
2. Una serie d'ordinadors en **remot coneguts** com **servidors DNS** troben la **direcció IP** d'aquell **domini** i la retornen a l'ordinador de l'usuari per a que pugui accedir al lloc **web correcte**.
3. Diferents tipus de **servidors DNS** han de treballar conjuntament per poder completar aquesta cerca de DNS.

4. Actuén:
    - Un solucionador o **resolver DNS**.
    - Un servidor **Root Server** (1.1.1.1 o 8.8.8.8 per exemple).
    - Un **servidor TLD** de DNS (de primer nivell, exemple: .net, .com. . .).
    - Un servidor de noms **autoritatiu** de DNS. Conté el **registre DNS**.
5. Pot haber un cas de **"caching"** que algun d'aquests servidors pot haber emmagatzemat la respostas de la consulta durant una cerca anterior, llavors el client, en lloc de recorrer i esperar molt, tindrà un temps de resposta menor.

Diferencia entre recursió i iteració

La **recursió** i la **iteració** son termes informàtics que descriuen dos mètodes diferents per resoldre un problema.

En la **recursió**, un programa es truca a **si mateix** fins a que **cumpleixi** una **condició**. Mentes que la iteració es repeteix un conjunt d'instruccions fins que es cumpleixi la condició.

Exemple: Jim ha perdut les seves claus de casa i les està buscant-la d'una forma sistemàtica.

```
Una solució recursiva seria que Jim no pararia de buscar les claus. Jim començarà a buscar,

Una solució iterativa seria que Jim faci una cerca en una habitació durant 5 minuts i despré
```

En un servidor DNS que faci la **recursió** seguirà consultant a altres servidors DNS fins que obtingui la direcció IP a la qual pugui retornar al client.

En un servidor DNS que faci una consulta **iterativa**, cada consulta DNS respon **directament al client** amb una direcció per a que un altre servidor DNS pregunti, i el client **seguirà preguntant** a altres servidors DNS fins que algú d'ells responda amb la IP i el domini correcte.

Iteració - Recursió / Resum:

El client delega una consulta a un DNS recursiu:

Recursiva: "Necessito la direcció IP d'aquest domini, per favor, trobala i no tornis a trucar-me fins que la trobis".

El client li diu al solucionador o *"resolver"* de DNS:

Iterativa: "Necessito la direcció IP d'aquest domini. Per favor, dona'm la direcció següent del servidor DNS en el procés de la recerca per a que jo mateix la pugui trobar".

Advantatges del DNS recursiu

Les consultes DNS recursives solen resoldre's més ràpid que les consultes iteratives. Això es degut al emmagatzematge **cache**. Un servidor DNs recursiu almacena en **caché** la resposta a cada consulta que realitza i guarda aquesta resposta final durant un temps determinar (TTL = Time to Live).

Quan un solucionador o *resolver* recursiu rep una consulta per a una adreça IP que tingui al seu caché, pot proporcionar ràpidament la resposta al caché al client sense comunicar-se amb cap altre servidor DNS. Servir ràpidament respostes des del caché és molt probable si a) el servidor DNS serveix a molts clients ob) el lloc web sol · licitat és molt popular.

Desaventatges del DNS recursiu

Desafortunadament, permetrà consultes de DNS recursives en servidors DNS oberts creant una vulnerabilitat de seguretat, ja que aquesta configuració pot permetre que els atacants portin a terme atacs d'amplificació de DNS i d'envergament de caché de DNS .

Servidors DNS recursius i atacs d'amplificació de DNS

En un atac d'amplificació de DNS, un atacant sol utilitzar un grup de màquines (que coneix com a botnet) per enviar un gran volum de consultes DNS mitjançant l'ús d'una adreça IP falsificada . Una direcció IP falsificada és com una direcció de retorn falsa; l'atacant envia sol · licituds des de la seva pròpia IP, però pide que les respostes van a la víctima.

Per agravar l'atac, l'atacant també utilitza una tècnica trucada amplificació, en la que la sol · licitud falsificada pide una resposta molt llarga. El servei víctima rebrà una allau de respostes de DNS llargues i no desitjades que poden interrompre o fins i tot fer els seus servidors. Aquest és un tipus d' atac DDoS.

És com si un grup d'adolescents bromistas llamara a una pizzeria i pidiera cada un una docena de pizzes. Al lloc de la seva pròpia direcció per a la entrega, a la direcció d'un veí despres. A la víctima, que rep una enorme quantitat de pizzes familiars que no ha fet cap comanda, probablement li pertorbirà el dia.

Necessiteu un servidor DNS que accepteu consultes recursives per dur a terme un tipus d'atac, ja que els paquets de DNS amplificats són respostes a consultes de DNS recursius.

Servidors DNS recursius i atacs d'envergament de caché de DNS

En un atac d'enverinament de caché de DNS, quan un servidor DNS recursiu sol · licita una adreça IP a un altre servidor DNS, un atacant intercepta la

sol · licitud i una resposta falsa, que sol · liciteu la direcció IP d'un lloc web maliciós.

El servidor DNS recursiu no només enviava al client original aquesta adreça IP, sinó que el servidor també guarda la resposta al seu caché.

Cal demanar usuari que sol · liciti una IP per al mateix nom de domini serà enviat al lloc web maliciós.

Si es tracta d'un nom de domini i un solucionador de DNS famosos, aquest atac podria arribar a afectar a milles d'usuaris.

En una consulta de DNS iterativa, el client pide directament la resposta a cada servidor DNS.

Inclós si un atacant és capaç d'enviar una resposta falsificada a la consulta, només afectarà a un únic client, el que no mereixi el temps de l'atacant.

Configuració DNS CryptoSEC

Instal · lació

S'instal · la amb la comanda `apt-get install bind9`, el fitxer de configuració es troba a `/etc/bind`.

El servidor DNS Autoritatiu

Tindrà els registres de la zona **"cryptosec.net"**. És un servidor autoritari que rebrà les peticions DNS d'un forwarder.

Arxiu de d'opcions de les zones

El fitxer `/etc/bind/named.conf.options`.

```
        // 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-enable yes;
        dnssec-validation yes;
        dnssec-lookaside auto;

        listen-on-v6 { any; };
};
```

Conté:

1. La declaració del directori on es guardaran els arxius de zona: **/etc/bind**
2. La declaració, per defecte desactivada, dels servidors de reenviament: secció forwarders {...}

Si no s'utilitzen forwarders, el servidor DNS anirà als servidors arrel per iniciar les resolucions de les consultes que no estiguin en memòria cau ni a cap de les seves zones. Quan s'utilitzen servidors de reenviament es consultarà aquests servidors.

Arxiu de dades per especificar la zona

És un servidor SOA, State of Authority

El fitxer `/etc/bind/named.conf.default-zones`:

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

Cada zona (directa o inversa) tindrà:

1. La declaració amb la directiva zoneon s'indica el domini o l'adreça de xarxa a les zones inverses.
2. Una directiva typeindicant si és una zona mestra (escrita per l'administrador) o esclava (descarregada automàticament d'un servidor mestre).
3. Una directiva fileindicant el fitxer de respatller (que es trobarà a /var/cache/bind)

Arxiu de dades per a una zona directa "*cryptosec.net*"

Cada zona necessita un fitxer de dades on desar els registres de la zona. Per a una zona directa com `cryptosec.net` el fitxer de zona pot ser `/etc/bind/db.cryptosec.net` i contenir:

```
$TTL    604800
@       IN      SOA     cryptosec.net. mail.cryptosec.net. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL

@       IN      NS      cryptosec.net.
@       IN      A       192.168.0.164
```

```
www     IN      CNAME   cryptosec.net.
;@      IN      A       10.200.243.164
;@      IN      A       192.168.31.164
$INCLUDE "/etc/bind/keys/zsk/Kcryptosec.net.+007+53495.key"
$INCLUDE "/etc/bind/keys/ksk/Kcryptosec.net.+007+07353.key"
```

NOTE: $INCLUDE "/etc/bind/keys/zsk/Kcryptosec.net.+007+53495.key" / $INCLUDE "/etc/bind/keys/ksk/Kcryptosec.net.+007+07353.key" son lés claus de **DNSSEC**. Vegeu la documentació de **DNSSEC**.

En aquest arxiu de zona cal notar:

- El caràcter @equival al domini que estigui definint acabat en punt. Aquí `cryptosec.net.`
- El camp `mail.cryptosec.net.` correspon al correu de contacte per indicar errors a la zona i s'interpreta com `cryptosec.net.`
- És important incrementar el valor Serial cada cop que es fa una modificació.

El servidor DNS Forwarder

És un servidor DNS que s'encarregarà d'encaminar les peticions DNS dels seus clients al SOA.

Arxiu de d'opcions de les zones

El fitxer `/etc/bind/named.conf.options`.

```
forwarders {
// CLASE
        10.200.243.164;
};
dnssec-validation no;
querylog yes;
recursion yes;
```

Conté:

1. La declaració del directori on es guardaran els arxius de zona: **/etc/bind**
2. La declaració, està activada, reenviarà els paquets al **SOA**: secció forwarders {...}

Arxiu de dades per especificar el forwarding a la zona "*cryptosec.net*"

És un servidor SOA, State of Authority

El fitxer `/etc/bind/named.conf.default-zones`:

```
zone "cryptosec.net" {
        type forward;
```

```
// CLASSE
        forwarders { 10.200.243.164; };
};
```

Cada zona (directa o inversa) tindrà:

1. La declaració amb la directiva zoneon s'indica el domini o l'adreça de xarxa a les zones inverses.
2. Una directiva typeindicant si és una zona mestra (escrita per l'administrador) o esclava (descarregada automàticament d'un servidor mestre).
3. Una directiva fileindicant el fitxer de respatller (que es trobarà a /var/cache/bind)

Comandes de verificació

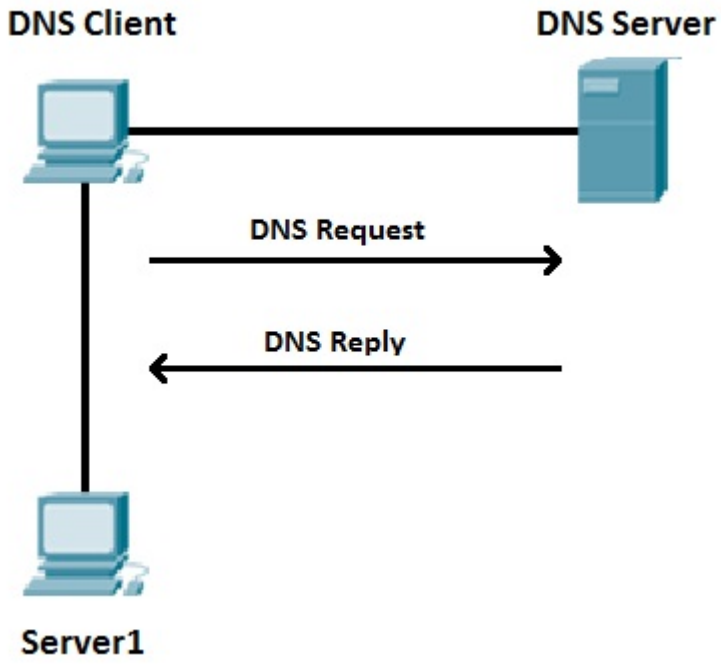
- `journalctl -u named -f &`: Mostra els logs del servei Bind9 en temps real
- `systemctl restart bind9`: Reinicia el Bind9.
- `host cryptosec.net`: Petició per resoldre la zona, **cryptosec.net**, obtindrem la IP.
- `nslookup cryptosec.net`: Petició per resoldre la zona, **cryptosec.net**, obtindrem la IP
- `dig cryptosec.net`: Petició per resoldre la zona, **cryptosec.net**, obtindrem la IP
- `systemd-resolve --status`: Verificació del status actual del DNS.
- `resolvectl query cryptosec.net`: Petició per resoldre la zona, **cryptosec.net**, obtindrem la IP

El client DNS

És el component que delega una consulta o consulta directament a servidors DNS, en la cerca d'un registre DNS a la qual vol accedir.

Utilitza el fitxer /etc/resolv.conf com a configuració del *resolver*.

La seva funció és millorar el rendiment de les resolucions mitjançant memòria cau. Quan una resolució provoca una fallada de memòria cau s'utilitzarà el DNS extern del qual probablement s'haurà obtingut la IP mitjançant una concessió DHCP.



>

Img Source: *https://603168-1953132-raikfcquaxqncofqfm.stackpathdns.com/wp-content/images/dns_process.jpg*

```
┌──(anonymous㉿osboxes)-[~]
└─$ host google.com
google.com has address 142.250.201.78
google.com has IPv6 address 2a00:1450:4003:80e::200e
google.com mail is handled by 10 smtp.google.com.

┌──(anonymous㉿osboxes)-[~]
└─$ host cryptosec.net
cryptosec.net has address 192.168.3.1

┌──(anonymous㉿osboxes)-[~]
└─$
```

> **Img Source**: *@Aaron & @Cristian 's GitHub*

Resolució de noms al client

Quan un client vol comunicarse amb una altra de la que només conéix el FQDN (*Fully Qualified Domain Name* = www.cryptosec.net), primer seria obtenir l'adreça IP amb el nom de domini. Després fa el request HTTP per poder accedir-hi.

Podem utilitzar el fitxer **/etc/hosts** com a resolver local o be als servidors DNS establertes en **/etc/resolv.conf**

Exemple de /etc/hosts

```
127.0.0.1 localhost
82.151.203.129 iespuigcastellar.xeill.net
145.97.39.155 es.wikipedia.org
192.168.3.1 cryptosec.net
```

Exemple de /etc/resolv.conf

Quan s'utilitza el client DNS per obtenir l'adreça IP d'un nom de domini, cal examinar el fitxer de configuració **/etc/resolv.conf** per obtenir:

- La llista de servidors DNS a utilitzar (un per línia precedit per la directiva nameserver)
- El domini a utilitzar per a les consultes que no són un FQDN indicat per la directiva search

```
# Recerca de cryptosec.net
nameserver 192.168.3.1
nameserver 10.200.244.10
search cryptosec.net
```

El servei systemd-resolved i la comanda resolvectl

La majoria de les distribucions actuals de GNU/Linux utilitzen systemdaixí que solen executar el servei systemd-resolvedcom a stub DNS local de la màquina. L'avantatge dutilitzar **systemd-resolved** és que les aplicacions trobaran un millor rendiment gràcies a la seva memòria cau.

El fitxer **/etc/resolv.conf** pot ser:

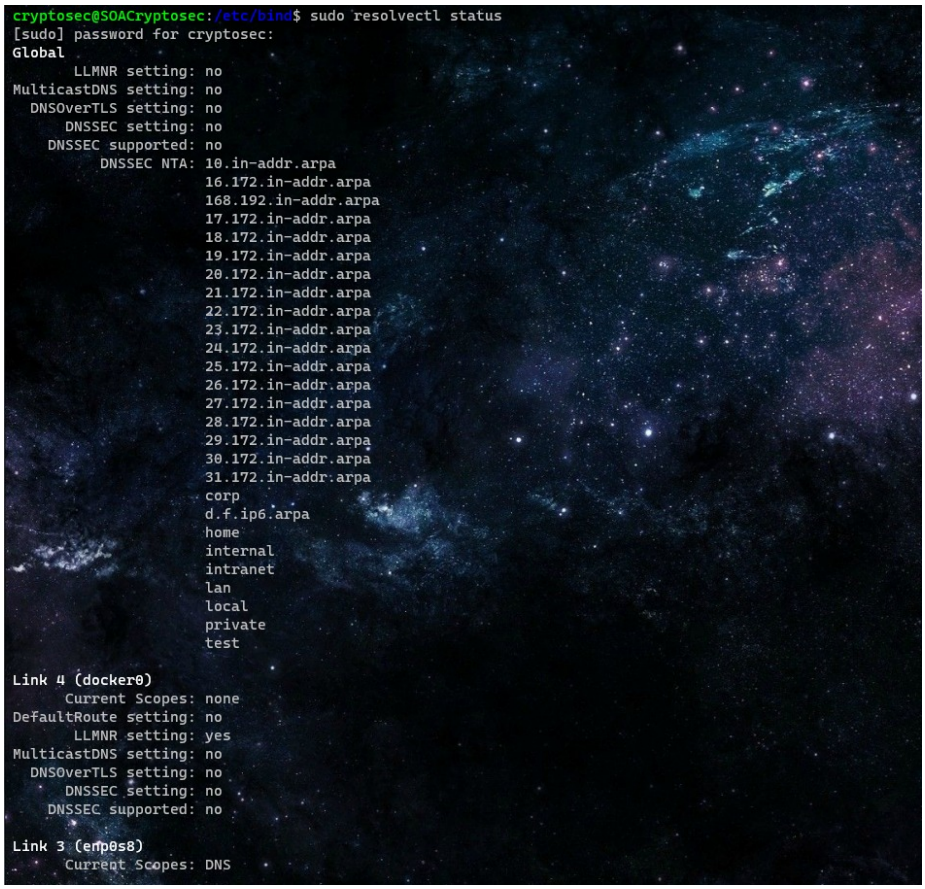
```
# See man:systemd-resolved.service(8) for details about the supported modes of
# operation for /etc/resolv.conf.

nameserver 127.0.0.53
options edns0 trust-ad
search cryptosec.net
```

Aquí es pot observar:

- El comentari adverteix que és un fitxer generat per **systemd-resolved**.
- Com a servidor DNS s'ha configurat l'adreça 127.0.0.53 que només és accessible des del propi equip.

L'ordre `resolvectl` permet:

- Mostrar informació sobre la configuració: **resolvectl status**
- Mostra estadístiques sobre els encerts de memòria cau: **resolvectl statistics**
- Mostra els DNS utilitzats: **resolvectl dns**
- Fer resolucions DNS: resolvectl query **cryptosec.net**

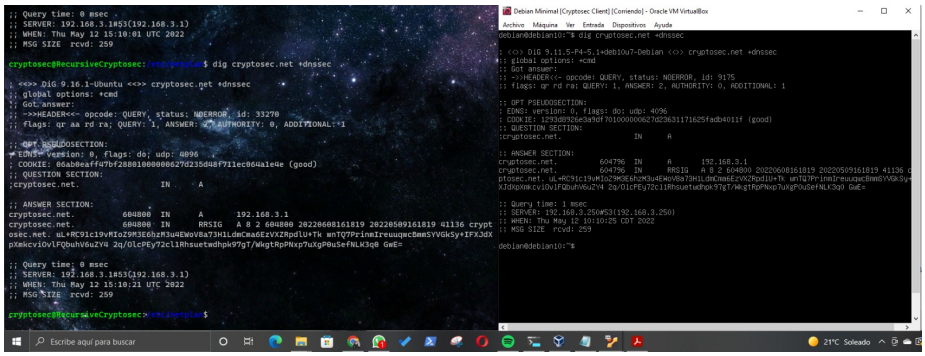


> **Img Source**: *@Aaron & @Cristian 's GitHub*

Com donar suport a consultes de DNS ràpides i segures

La solució es DNSSEC.

Consulteu la documentació més extensa i adherida de **DNSSEC**.



> **Img Source**: *@Aaron & @Cristian 's GitHub*

Glossari de termes de les configuracions de BIND9

`A` = stableix la correspondència d'un nom a una adreça IP.

`CNAME` = Estableix un àlies per a un nom.

`MX` = Especifica un servidor d'intercanvi de correu.

`NS` = Especifica un servidor de noms per al domini.

`PTR` = Estableix la correspondència d'una adreça IP a un nom.

`SOA` = Declara el servidor de noms que té més autoritat per a la zona.

Glossari de termes de tipus de servidors de BIND9

`Recursive` = El servidor que realitza diverses consultes fins a obtenir una resposta completa.

`Secondary` = El servidor DNS que rep la base de dades de zona d'un altre servidor.

`Forward` = El servidor que reenvia les consultes a altres servidors.

`Authoritative` = El servidor que proporciona respostes sobre les zones que té configurades.

`Primary` = El servidor DNS que conté els fitxers de zona (la base de dades original).

Glossari de termes seongs cada camp del SOA amb la seva funció (Bind9)

`time-to-retry` = Temps que un servidor secundari deixa passar abans de tornar a intentar una transferència de zona.

`serial-number` = Utilitzat pels servidors secundaris per a detectar els canvis a la base de dades.

`nxdomain-ttl` = El temps que els solucionadors han de guardar a la memòria cau una resposta de domini o host inexistent..

`time-to-expire` = Si passat aquest temps, un servidor secundari no aconsegueix realitzar la transferència de zona, ha de deixar de considerar-la vàlida.

Exemples BIND9 (Configuracions)

GLUE RECORD

```
# /etc/bind/named.conf.default-zones

zone "zone1.com" {
    type primary;
    file "/etc/bind/db.zone1.com";
};
```

```
# /etc/bind/db.zone1.com

@   SOA ns  admin   1700010100 20m 3m 2w 1h
    NS  ns
    A   1.1.1.1
```

Què respondrà el servidor a la següent consulta?

```
user@debian:~$ host zone1.com
```

No es pot carregar la Zona ja que falta el GLUE RECORD:

ns A 2.2.2.2

La resposta correcta és: `SERVFAIL`

$GENERATE

```
# /etc/bind/named.conf.default-zones

zone "server.tld" {
    type primary;
    file "/etc/bind/db.server.tld";
};
```

```
# /etc/bind/db.server.tld

@       SOA     ns    admin    1700010100 20m 3m 2w 1h
        NS      ns
ns      A       192.168.122.1
$GENERATE 1-4 database$ A 1.1.$.1
```

```
user@debian:~$ host database1.server.tld
database1.server.tld has address 1.1.1.1
user@debian:~$ host database2.server.tld
database2.server.tld has address 1.1.2.1
user@debian:~$ host database3.server.tld
database3.server.tld has address 1.1.3.1
user@debian:~$ host database4.server.tld
database4.server.tld has address 1.1.4.1
user@debian:~$ host database5.server.tld
Host database5.server.tld not found: 3(NXDOMAIN)
```

Resolució inversa

```
# /etc/bind/named.conf.default-zones

zone "5.43.IN-ADDR.ARPA" {
    type primary;
    file "/etc/bind/db.5.43.IN-ADDR.ARPA";
};
```

```
# /etc/bind/db.5.43.IN-ADDR.ARPA

@       SOA ns  admin   1700010100 20m 3m 2w 1h
        NS  ns
ns      A   192.168.122.1
78.202      PTR host.tld.
```

Quina adreça IP es resoldrà inversament al nom host.tld? `43.5.202.78`

–> [**Tornar a Ciberseguretat**] <–

Bibliografia

- https://www.cloudflare.com/learning/dns/dns-over-tls/
- https://www.cloudflare.com/es-es/learning/dns/what-is-dns/
- https://elpuig.xeill.net/Members/vcarceler/c1/didactica/apuntes/ud4/na8
- https://www.cloudflare.com/learning/dns/what-is-dns/
- https://www.digival.es/blog/que-son-las-dns-y-para-que-sirven/
- https://www.hostinger.es/tutoriales/que-es-dns
- https://www.webempresa.com/hosting/que-son-dns.html

- https://dinahosting.com/ayuda/que-es-un-servidor-dns/
- https://es.wikipedia.org/wiki/Sistema_de_nombres_de_dominio
- https://www.csuc.cat/ca/serveis/secundaris-i-repliques-de-dns
- https://ca.eyewated.com/que-es-dns-domain-name-system/
- https://ca.theastrologypage.com/dns-record
- http://acacha.org/mediawiki/Servidor_DNS#.Yoj9sKjP1PY