

SERVIDOR DNS

Zones

Definició de zona

Les zones descriuen els equips que en formen part. Cada fitxer de zona és una base de dades que descriu els hosts que hi ha en la zona i la mateixa zona.

La configuració d'una zona s'emmagatzema en un conjunt de fitxers anomenat fitxers de zona.

Propòsit d'un DNS

Administrar una zona com per exemple una xarxa local amb tots els equips d'una organització, o un conjunt de zones d'una organització més complexa.

Objectius per aconseguir-ho

- Definir els fitxers de configuració del servei DNS.
- Definir cada una de les zones de què es compongui la xarxa.
- Crear els fitxers a la resolució inversa de la xarxa i del loopback.

Requisits per crear una zona

- Definir les zones en el fitxer de configuració del servei.
- Crear el fitxer de zona en què es defineix la resolució directa per a cada host de la zona i les característiques de la zona.
- Crear el fitxer de resolució inversa de la zona.

Fitxers de zona

En qualsevol zona hi haurà almenys els fitxers de zona següents:

- Un fitxer amb les associacions dels noms de domini a adreces IP. Aquest fitxer defineix la **resolució directa**.
- Un fitxer per a cada subxarxa amb l'associació de cada adreça IP al seu nom de domini canònic. Defineix la **resolució inversa**.
- Un fitxer amb la definició de la **resolució inversa del loopback**.
- Un fitxer amb la descripció dels **nodes arrel d'Internet**.

Registres de recurs (RR)

La informació de zona s'emmagatzema en forma de **registre de recurs** (RR (Resource Record)).

¿Què s'emmagatzema?

- Informació que permet identificar cada nom de domini amb l'adreça IP corresponent (**Resolució directa** o forward mapping).
- Informació per identificar cada adreça IP amb el nom de domini corresponent (**Resolució inversa** o reverse mapping)

Registres de recurs (RR)

El conjunt dels registres de recurs de totes les zones de l'espai de noms formen la base de dades distribuïda jeràrquica del sistema DNS.

L'especificació del DNS diuen com han de ser els fitxers de zona i com s'hi han de descriure els registres de recurs (descripció de cada element que pertany a la zona).

Registres de recurs (RR)

Registre SOA diu que el fitxer de zona on es troba és la millor font de dades per a la zona, que el servidor de noms és autoritari per a la zona. Només hi ha d'haver uno per zona.

Camps del registre SOA

- **nomDomini.** indica el nom del domini que s'està definint i pel qual el servidor de noms és autoritari. El punt final important posar-lo.
- **nsPrimari.** és el nom del host servidor de noms primari per a aquesta zona. Pareu atenció al punt final.

Registres de recurs (RR)

Camps del registre SOA (General)

- **admin.domini.** és l'adreça de correu electrònic de l'administrador del servidor de noms de domini, amb el format usuari.domini. El primer punt que separa el nom d'usuari i el nom del servidor cal interpretar-lo com una arrova (usuari@domini).
- **opcions-slaves** són paràmetres que s'indiquen entre parèntesis i que serveixen per definir com ha de ser la comunicació entre el servidor primari (o master) i els servidors secundaris (o slaves): serial, refresh, retry, expire, minimum

Registres de recurs (RR)

Camps del registre SOA (options-slaves)

- **Serial:** el número de sèrie de la versió de les dades. A cada canvi de les dades de la zona, el número s'incrementa.
- **Refresh:** temps a transcórrer entre cada refresc de dades del servidor secundari.
- **Retry:** temps d'espera per tornar a intentar un refresc quan el servidor secundari ha fallat en l'intent d'actualitzar les seves dades des del servidor primari.

Registres de recurs (RR)

Camps del registre SOA (options-slaves)

- **Expire:** temps a partir del qual les dades del servidor secundari es consideren sense autoritat si no s'han refrescat abans.
- **Minimum:** valor del TTL dels camps per defecte. Recordeu que a cada camp s'hi pot assignar un TTL específic. Segons la versió del servidor indicarà el TTL de les respostes negatives (negative caching), ja que el temps TTL es defineix per la directiva \$ttl.

Registres de recurs (RR)

Registre NS defineix un servidor de noms autoritatiu per a la zona. Hi haurà tantes entrades NS com servidors de noms autoritatius hi hagi en la zona. L'estàndard DNS en recomana almenys dos (un de primari o master i un de seguretat, secundari o slave).

Camps del registre NS

- **nomDomini.** indica el nom del domini que s'està definint.
- **nameServer.** és el nom del servidor de noms. Fixeu-vos un altre cop que tant nomDomini. com nameServer. acaben en punt per indicar que són noms de domini absolut o FQDN.

Registres de recurs (RR)

Registre A associa un nom de host a una adreça IP (resolució directa). Per cada nom de host de la xarxa caldrà disposar d'una entrada que associï el nom del host a la seva adreça IP.

Camps del registre A

- **nomHost.** indica el nom del host que s'està definint. Pot ser relatiu (sense punt final) o absolut (afegint el domini complert al final).
- **IP** és l'adreça IP assignada al host.

Registres de recurs (RR)

Registre A

nomHost acaba en punt per indicar que és un FQDN. Si no acabés en punt s'interpretaria com un nom relatiu al SOA que s'està definint actualment. Un host pot tenir més d'una IP assignada al mateix nom de host. Quan això passa s'anomena multi-homed. Simplement caldrà que hi hagi un registre A per a cada adreça IP. Constarà del mateix nom de host a l'esquerra de la definició i de la corresponent adreça IP a la dreta.

Registres de recurs (RR)

A tenir en compte

Els noms definits en els registres de tipus A són noms **canònics**. Un host es pot identificar per més d'un nom, però només un és el nom canònic (original), la resta són àlies. Els noms canònics es defineixen amb el tipus de registre A. Els àlies es defineixen amb el tipus de registre CNAME.

Registres de recurs (RR)

Registre CNAME (canonical name o nom canònic) associen un àlies a un nom canònic.

Camps del registre CNAME

- **nomHost.** indica el nom de l'àlies que s'està definint.
- **hostCanonicalName | IP** és el nom de host canònic al qual s'assigna l'àlies. És un FQDN i que acaba en punt. De vegades caldrà indicar-hi una adreça IP. En un host multi-homed amb múltiples adreces IP que a més té àlies, si la definició fos pel nom canònic del host, no se sabia quina de les adreces IP correspon a l'àlies. En aquests casos, el CNAME apunta a una adreça IP.

Registres de recurs (RR)

Resolució d'àlies

La resolució dels àlies s'obté buscant l'entrada de l'àlies en el fitxer de zona. Amb l'entrada CNAME s'obté el nom canònic corresponent a l'àlies. Un altre cop es torna a buscar en el fitxer de zona, ara el nom canònic. Una entrada de tipus A proporcionarà l'adreça IP corresponent (àlies → CNAME → nom canònic → A → adreça IP).

Registres de recurs (RR)

Registre PTR (pointer o punter) associa una adreça IP al nom de host corresponent (resolució inversa). Cal una entrada PTR per a cada interfície de xarxa de la zona, per a cada adreça IP.

Camps del registre PTR

- **ipInversa.in-addr.arpa.** indica l'adreça IP escrita en forma de domini in-addr.arpa per poder fer la resolució inversa. Les adreces IP s'escriuen al revés quan formen part del domini in-addr.arpa. Així, una IP 192.168.20.2 s'escriu
2.20.168.192.in-addr.arpa.
- **hostName.** és el nom de host FQDN assignat a l'adreça IP.